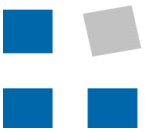


Prüfung IntSi2 Teil 2, 18.8.2008

Anzahl Zusatzblätter:

Name, Vorname:

- Prüfungsdauer: **60 Minuten**
- Die Prüfung setzt sich aus verschiedenen Fragetypen zusammen:
  ***Wis**sensfragen (Beschreibungswissen):* Abruf und Wiedergabe von Vorlesungsinhalten (z.B. Begriffe, Bezeichnungen, ...)
  ***Ver**ständnisfragen (Erklärungswissen):* Verständnis unter Beweis stellen (typische Fragen sind z.B. Erklären Sie ...).
  ***Ums**etzungsfragen (Transferleistung):* Gelernten Wissens auf andere Bereiche umsetzen, „Neue Fragen" d.h. Inhalte wurden nicht 1:1 in Vorlesung behandelt, eigene Ideen entwickeln (z.B. Wie würden Sie vorgehen wenn...)
- Es sind **keine Unterlagen** und auch **keine elektronische Hilfsmittel (Rechner, Mobile, etc.)** erlaubt.
- Die **Aufgabenblätter sind in zusammengehefteter Form zu belassen**.
- Die Lösungen sind direkt auf die Aufgabenblätter zu schreiben (nur wenn nötig auf Zusatzblätter).
- Sind Berechnungen anzustellen, so ist zusätzlich zum Endwert (*mit Dimensionen*) auch die Formel gefragt.
- **Alle Lösungen müssen nachvollziehbar sein** (Beschreibung und evtl. Hinweis auf Formelsammlung angeben).
- Bei Multiple-Choice-Fragen sind eventuell mehrere Antworten anzukreuzen. **Falsch angekreuzte Antworten ergeben Negativpunkte**. Kreuzen Sie besser nichts an, wenn Sie nicht sicher sind.
- Die pro Teilaufgabe erreichbare Punktzahl ist am Rand angegeben.
- Bei Unklarheiten sind sinnvolle Annahmen zu treffen (keine Fragen während der Prüfung stellen).
- Verwenden Sie keine rote Schriftfarbe für Ihre Lösungen; Bleistift ist erlaubt.

1) Information Security Management Einführung

a) Zählen Sie die in der Vorlesung vogestellten 5 grundsätzlichen Schutzmassnahmen auf und beschreiben Sie je eine Biespielmassnahme.

W			2
W			2
W			2
W			2
W			2

b) Zählen Sie die in der Vorlesung vorgestellten 3 grundsätzlichen Verletzlichkeitsbereiche auf und beschreiben Sie je ein Beispiel:

W			2
W			2
W			2

c) Geben Sie die sechs Massnahmen-Hauptbereiche an, welche das BSI unterscheidet:

W		1
W		1
W		1
W		1
W		1
W		1

d) Beschreiben Sie den in der Vorlesung behandelten Begriff „BCM”.

W		2

e) Geben Sie an, wofür die in der Vorlesung behandelte Abkürzung „PDCA” steht.

W		1

2) Verschiedene Organisationen veröffentlichen regelmässig Berichte über die „IT-Sicherheitslage".

a) Beschreiben Sie die Hauptmotivation der gegenwärtigen (2008) Angreifer und beschreiben Sie, wodurch sich die gegenwärtige (2008) Angriffsart von derjenigen der „klassischen Hacker" von vor einigen Jahren besonders unterscheidet. .

W		2
W		2

b) Beschreiben Sie, wieso die meisten Leute bei der „Teilnahme an einem Gewinnspiel" von einem „kleinen Risiko" sprechen.

U	Kosten		2
U	Erträge		2
U	Risiko		2

c) Sie sollten sich in einem Anstellungsgespräch zum Thema „Bot-Nets" und „IT-Sicherheit Trends" äussern. Beschreiben Sie, was Sie erzählen würden.

W	Bot-Nets		3
W	IT-Sicherheit Trends		3

3) Standards

a) Standardisierungsorganisationen

		ISO 27001 Specification fo an Information Security Management System (ISMS)	ISO 27002 Code of Practice for Information Security Management	Grundschutz-Handbuch (IT Grundschutz Kataloge) des Bundesamt für Sicherheit in der Informationstechnik	
W	Dieser Standard wurde von British Standardization Institution Standards abgeleitet.				1
W	Dieser Standard bildet die Grundlage für die unabhängige Sicherheitszertifizierung von Organisationen.				1
W	Dieser Standard enthält „Recommendations of good Security Things to do“.				1
W	Dieser Standard ist nicht gratis erhältlich sondern muss gekauft werden.				1

b) Beschreiben Sie die folgenden Begriffe und Vorteile von Audits nach dem Open Source Security Testing Methodology Manual (OSSTMM)

W	Was ist ein RAV		1
W	Konsistenz		1
W	Quantifizierbarkeit		1
W	False Positive		1

c) Welches Resultate liefere „Portscanning“ und „Fingerprinting“? Und welches bekannte Werkzeug wurde dazu im IntSec-Lab verwendet?

W	Portscanning		1
W	Fingerprinting		1
W	Tool		1

4) Sicherheitsanalyse: Als Student der HSR sind Sie mit der IT-Infrastruktur und den verschiedenen Anwendungen gut vertraut.

a) Notieren Sie die typischen Schritte, welche im Rahmen der Vorlesung für Risikoanalysen angegeben wurden.

W		1
W		1
W		1
W		1

b) Beschreiben Sie den Begriff Risiko anhand des Beispiels „Entwurf und Speicherung von Prüfungsaufgabenblättern auf der HSR IT-Infrastruktur” (geben Sie die englischen und die deutschen „Risikobegriffe” an).

V			3
V			3
V			3
V			3

c) Beurteilen Sie die „Passwort-Situation” an der HSR. Beschreiben Sie drei Aspekte der Passwort-Situation und geben Sie dazu je einen Vor- und einen Nachteil an. .

U		3
U		3
U		3

5) Im Artikel Psychology of Risk by Bruce Schneier werden diverse interessante Aussagen gemacht.

a) Er lieferte beispielsweise die Liste „Conventional Wisdom About People and Risk Perception“:

People exaggerate risks that are:	**People downplay risks that are:**
Spectacular	Pedestrian
Rare	Common
Personified	Anonymous
Beyond their control, or externally imposed	More under their control, or taken willingly
Talked about	Not discussed
Intentional or man-made	Natural
Immediate	Long-term or diffuse
Sudden	Evolving slowly over time
Affecting them personally	Affecting others
New and unfamiliar	Familiar
Uncertain	Well understood

Beschreiben Sie je drei Arten von Risiken, die von Menschen über- bzw. unterschätzt werden und geben Sie je ein konkretes Beispiel an:

V	diese Art Risiken wird überschätzt		1
V			1
V			1
V	diese Art Risiken wird unterschätzt		1
V			1
V			1

b) Es gibt etwa doppelt so viele englische Worte mit dem Buchstaben „k“ an dritter Stelle, als Worte, welche mit dem Buchsaben „K“ beginnen. Bruce Schneier beschreibt, dass bei einem Test rund 70% der Personen gesagt haben, dass es mehr Wörter gäbe, welche mit „K“ beginnen, als Worte, welche ein „k“ an dritter Stelle haben. Wie erklärt sich dies?

V		2

c) In einer Umfrage wurden Studenten die folgenden zwei Fragen in unterschiedlicher Reihenfolge gestellt:
1. How happy are you with your life in general?
2. How many dates did you have last month?
Was kam dabei heraus?

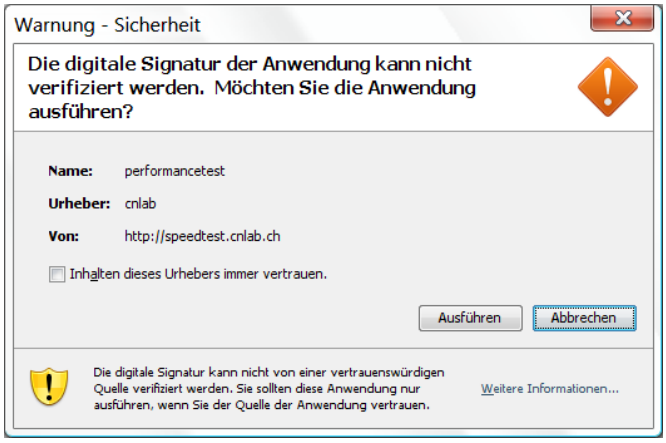
V		2

d) Welche Konsequenzen sollen aus den Ausführungen von Bruce Schneier in Bezug auf „Security Decisions“ gezogen werden? Nennen Sie drei wichtige Punkte, welche dem Bericht zu entnehmen sind.

U		1
U		1
U		1

6) Client Side Security

a) Beim Aufruf einer Web-Seite wird Ihnen der folgende Dialog angezeigt. Welche Komponente dieser Webseite hat diesen Dialog ausgelöst?



W		2

b) Welche Zugriffsrechte gewähren Sie dieser Anwendung auf Ihrem lokalen Rechner, wenn Sie auf „Ausführen" klicken?

W		2

c) Beschreiben Sie, was sich über den Urheber dieser Anwendung aussagen lässt.

V		2

d) Diverse Wissensfragen

		richtig	falsch	
W	Bei Signed und Unsigned ActiveX Controls werden unterschiedliche Rechte zur Nutzung von Ressourcen zugewiesen.			1
W	Die Unterschrift auf einem Signed Applet beweist, dass es sich nicht um ein „bösartiges" Applet handelt.			1
W	Es ist möglich, dass ein Cookie, welches von einem Web-Server „A" einer bestimmten Domain gesetzt wurde, auch von einem anderen Web-Server "B" der selben Domain gelesen werden kann.			1
W	„WebScarab" ist ein Werkzeug zur Analyse von HTTP-Verkehr, welches auch für HTTPS Man-in-the-Middle-Attacken genutzt werden könnte.			1

7) Phishing-Mail

a) Ein Phishing-Mail an stud.all@hsr.ch fordert alle Adressaten auf, sich bei ihrem HSR-Account anzumelden. Die Mail enthält folgenden Code:

```
<A href="https://unterricht.hsr.ch">
    <FORM action="http://unterricht.hsr.ch.vu/stealHsrLogin.php"
    method="get">
         <INPUT class="lookLikeLink" type="submit"
         value="https://unterricht.hsr.ch">
    </FORM>
</A>
```

W / V	Wie wird diese Attacke genannt und was wird mit diesen Codezeilen bezweckt?		2
V	Welche Adresse wird in der Statusleiste des Internet Explorers angezeigt? (url angeben)		2
V	Zu welcher Adresse wird man beim Klick auf den angezeigten Link geführt?		2

b) Wird dieser Angriff verunmöglicht, wenn im Internet Explorer die Sicherheitseinstellung „Active Scripting" deaktiviert wird? (Antwort mit Begründung.)

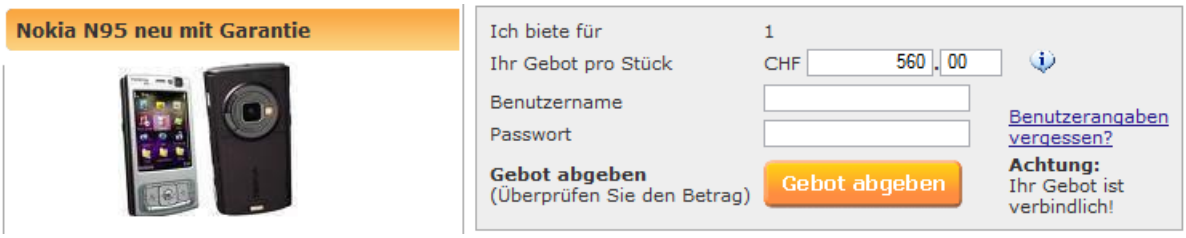
V		2

c) Ein unachtsamer Student hat den Link angeklickt und steht nun vor der Login-Seite. Wie könnte er nun den Betrug noch entdecken?

V		2

8) Cross-Site-Scripting / Cookies:

a) Auf einer Internet-Auktionsplatform gibt es für jeden Artikel eine Web-Seite. Diese besteht aus einer Artikelbeschreibung sowie einem Formular, über welches nach Angabe von Benutzername und Passwort an der Versteigerung teilgenommen werden kann (Gebote abgeben). Die Artikelbeschreibung kann beliebigen HTML- und Script-Code enthalten.



b) Natürlich möchten Sie mit Ihrer Auktion einen möglichst hohen Preis erzielen. Beschreiben Sie die nötigen Schritte, um mittels XSS den Betrag eines Gebots um den Faktor 100 zu erhöhen. (Ein Angebot von CHF 50, soll beispielsweise in ein Gebot über CHF 5‘000 gewandelt werden.)

V		2

c) Eine andere Auktion wurde so manipuliert, dass die Formulardaten an ein Skript auf einem privaten Server gesendet werden. Das Skript speichert die Formulardaten auf dem privaten Server ab.
Welche Funktionen muss dieses Skript zusätzlich aufweisen, damit der Betrug von den Bietern nicht entdeckt wird.

W		2

d) Welche Massnahmen muss der Betreiber der Auktionsplatform treffen um XSS zu unterbinden ?

W		2

9) OWASP Top 10

a) Beschreiben Sie, was das „OWASP-Projekt” ist. (Geben Sie drei Begriffe/Punkt dazu an.)

W		3

b) Ein Online-Multiplayer-Spiel besteht aus einem Server sowie einem Applet, welches im Browser jedes Teilnehmers läuft und via UDP mit dem Server kommuniziert.Geben Sie für jedes der untenstehenden Probleme an, welche Sicherheitsschwachstelle der OWASP Top Ten Liste diesem Problem zugeordnet werden kann.

V	Hat ein Hacker mit einem Sniffer das Login-Paket eines Benutzers abgefangen, so kann er sich selbst durch erneutes Senden dieses Pakets unter diesem Benutzer einloggen.		1
V	Spiel-Benutzer sind auf Datanbank-Ebene nicht bekannt. Sämtliche Transaktionen werden unter einem einzigen Datenbank-Benutzer mit Administrations-Rechten durchgeführt.		1
V	Da für jedes empfangene Paket wird auf dem Server ein grosser Buffer reserviert. Dadurch kann es bei übermässigem Verkehr sehr schnell zu einer OutOfMemoryException kommen. Dies bedeutet ein Absturz der gesamten Anwendung.		1
V	UDP Pakete, welche nicht, mehrfach oder in falscher Reihenfolge ankommen, können den aktuellen Spielstand in einen inkonsistenten Zustand überführen.		1

c) Nun entscheidet sich der Spiel-Betreiber, die auf UDP basierte Kommunikation zwischen dem Server und den Spieler-Applets durch eine TCP-Kommunikation mit SSL-Verschlüsselung zu ersetzen. Welche der oben angegeben Probleme können dadurch gelöst werden?

U		2

Formelsammlung

A1 - Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
A2 - Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 - Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
A4 - Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 - Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
A6 - Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
A7 - Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8 - Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9 - Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10 - Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

ISO-Standard (im Vergleich zu BSI UK)

EIN INSTITUT DER
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Institute for
Internet Technologies
and Applications

IntSi2 Prüfung vom 18.08.2008, Teil Steffen — 41 Punkte

Name:	Punkte:
Vorname:	

1 Contactless Proximity Cards — 2 Punkte

Warum funktionieren kontaktlose Chipkarten wie LEGIC oder MIFARE nur auf eine Entfernung von maximal ca. 10 cm?

2 Leistungsaufnahme von Chipkarten — 2 + 2 = 4 Punkte

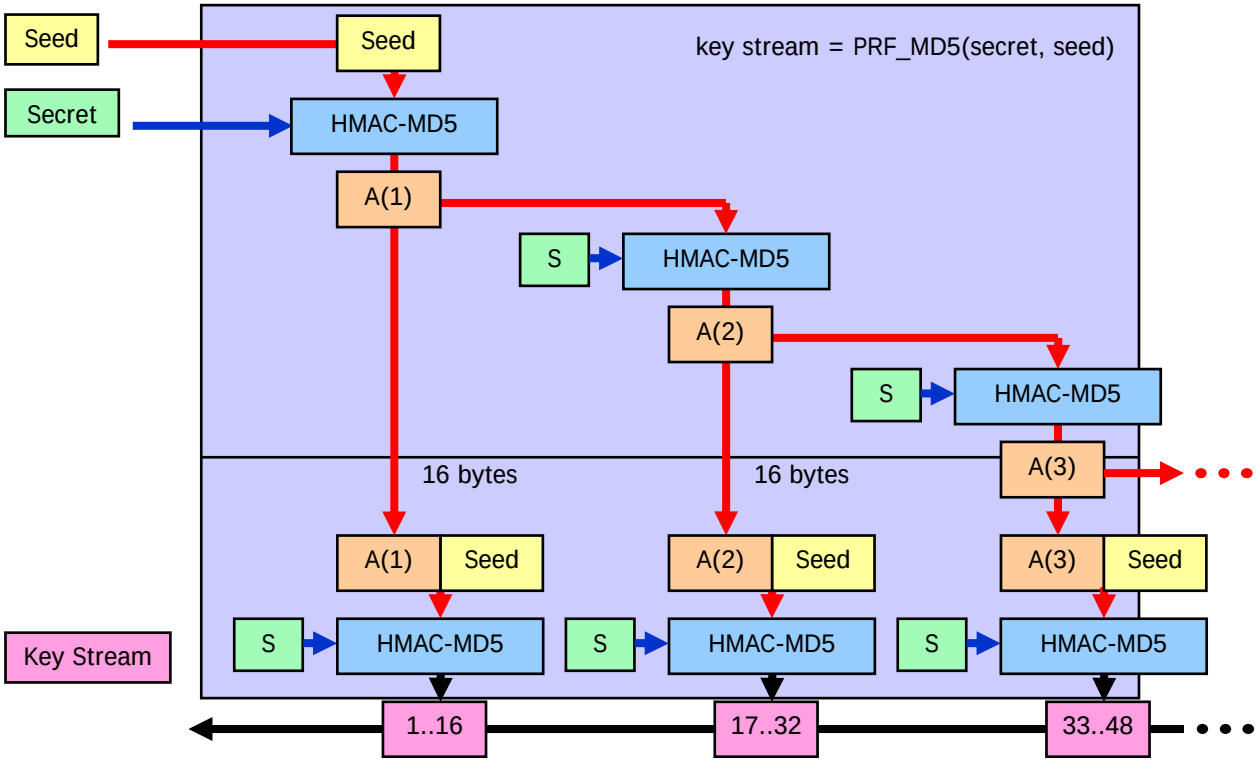
a) Warum werden im Zahlungswesen (EMV) nur Karten der Klasse A (5 V) eingesetzt, während es im Mobilfunkbereich (SIM) nur Karten der Klasse B (3 V) oder C (1.8 V) sind?

b) Warum achten die Chipkartenhersteller sehr darauf, dass der Stromverbrauch ihrer Karten im Betrieb über die Zeit möglichst konstant bleibt?

3 Generation von RSA Schlüsselpaaren auf der Chipkarte 3 Punkte

Alle Chipkarten mit einem Crypto Coprozessor bieten die Möglichkeit ein RSA Schlüsselpaar auf der Karte zu generieren. Beschreiben Sie je einen Vorteil und einen Nachteil dieses Features bei der Generierung von Signaturschlüssel.

4 HMAC als Pseudo Random Function (PRF) 2 Punkte



Warum werden im obenstehenden Blockdiagramm die HMAC Werte A(1), A(2), A(3), … nochmals gehasht, bevor sie als pseudo-zufälliger Schlüsselstrom verwendet werden?

5 True Random Numbers 2 + 2 + 2 = 6 Punkte

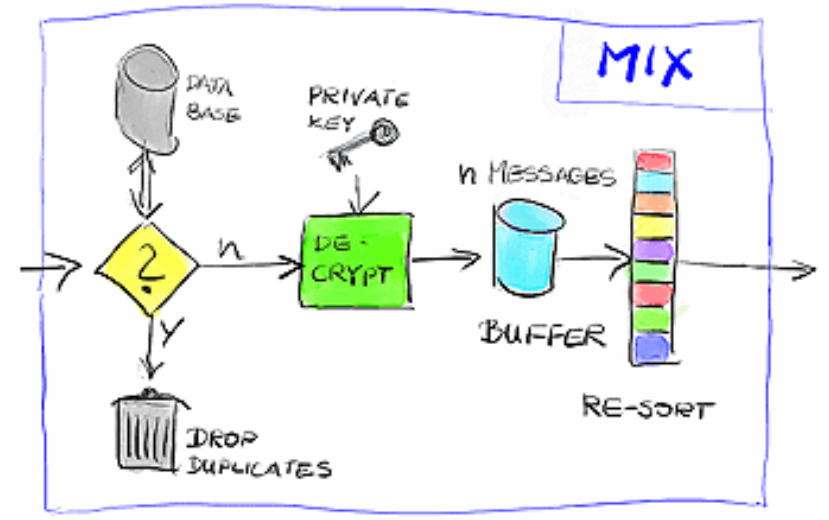
a) Was halten Sie vom Ansatz der Debian Distributoren, die OpenSSL PRF, die z.B. für die Generierung von RSA Schlüsselpaaren verwendet wird, mit der zufälligen 16 Bit langen Linux Prozess ID zu initialisieren? Hätte der verantwortliche Maintainer nicht besser noch die Serienummer des Intel oder AMD Prozessorchips dazugenommen?

b) Welche der beiden folgenden Zufallsquellen würden Sie zur Speisung des Entropie-Pools /dev/random auf einem Server verwenden: 1) Das Timing von ankommenden Netzwerkpaketen oder 2) die gesampelten LSBs der auf dem Motherboard vorhandenen 16 Bit Soundkarte? Begründen Sie Ihren Entscheid.

c) Unabhängig davon, ob Sie unter Frage b) die Entropiequelle 1) oder 2) gewählt haben: Worauf müssen Sie bei Verwendung von solchen Quellen unbedingt achten?

6 Anonymisierung 2 + 2 + 2 = 6 Punkte

Die untenstehende Figur zeigt den typischen Aufbau eines Mix-Knotens in einer Anonymisierungskette. Erläutern Sie den Effekt, der mit den einzelnen Komponenten erzielt werden soll.



a) DATABASE / DROP DUPLICATES

b) PRIVATE KEY / DECRYPT

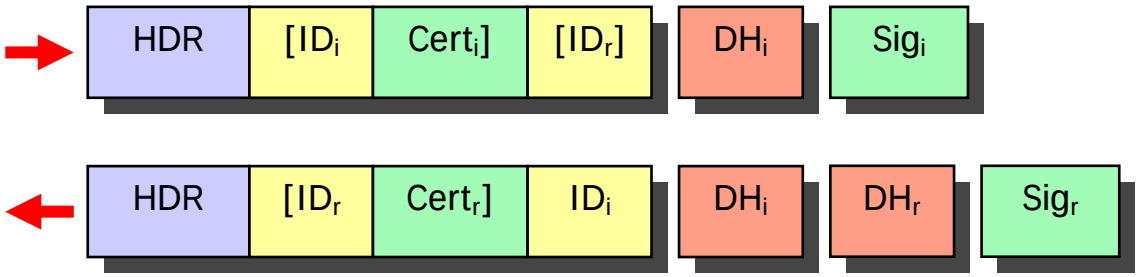
c) N MESSAGE BUFFER / RE-SORT

7 Tor — 2 + 2 = 4 Punkte

a) Warum bietet Tor den Exit Nodes die Möglichkeit eine Exit Policy zu definieren?

b) Wie können Exit Nodes ihre Position in einem Tor Netzwerk zu kriminellen Zwecken missbrauchen?

8 VoIP Security – Das MIKEY Protokoll — 2 + 2 = 4 Punkte



Das obenstehende MIKEY Protokoll erlaubt eine End-zu-End-Verschlüsselung von Multimedia Sessions (VoIP, Videokonferenzen, etc.) auf einer Peer-to-Peer Basis.

a) Wozu dienen die DH_i und DH_r Payloads in der oben dargestellten Variante des MIKEY Protokolls?

b) Wozu dienen die Sig_i und Sig_r Payloads in der oben dargestellten Variante des MIKEY Protokolls?

9 Buffer Overflows 2 + 2 = 4 Punkte

Ein Amateurhacker entwickelt auf seinem Linuxrechner einen Shellcode, der einen Bufferoverflow in einer bestimmten Zielsoftware ausnutzen soll, um dadurch die Kontrolle über fremde Hosts im Internet zu erlangen. Zuerst scheint die Attacke zu funktionieren. Aber nachdem der Hacker auf seinem Rechner manuell *googleearth* installiert und mit

```
PATH=$PATH:/opt/googleearth
```

die Pfadvariable erweitert hat, funktioniert der Bufferoverflow auf seinem Rechner plötzlich nicht mehr.

a) Was ist der Grund für das plötzliche Versagen der Bufferoverflow-Attacke?

b) Durch welchen Trick kann der Einfluss der Pfadvariable weitgehend eliminiert werden?

10 Software Security 2 + 2 + 2 = 6 Punkte

Im Buch „Software Security“ von Gary McGraw werden folgende drei Massnahmen zur Verbesserung der Softwaresicherheit mit abnehmender Effektivät aufgelistet:

① Code Review

② Architectural Risk Analysis

③ Penetration Testing

c) Weshalb sind Code Review und Architectural Risk Analysis fast gleich gestellt?

d) Was ist einfacher: Ein Code Review oder eine Architectural Risk Analysis? Begründen Sie Ihre Entscheidung.

e) Warum wird Penetration Testing, das heute die meistverbreitete Methode ist und gute Resultate liefert, relativ schlecht bewertet?