

\_\_\_\_\_

--	--	--	--	--	--	--	--	--	--

**Bitte hier unbedingt Matrikelnummer und Adresse eintragen, sonst keine Bearbeitung möglich.**

Postanschrift: FernUniversität, D-58084 Hagen \_\_\_\_\_

Name, Vorname \_\_\_\_\_

\_\_\_\_\_

Straße, Nr. \_\_\_\_\_

PLZ, Wohnort \_\_\_\_\_



**Fakultät für**

**Mathematik und Informatik**

**Kurs: 01867 „Sicherheit im Internet II“**

Klausur am 05.02.2011

Hörerstatus:

Klausurort:

- Vollzeitstudent
- Teilzeitstudent
- Zweithörer
- Gasthörer
- Bachelor
- Lehramt
- .....

- Berlin
- Bochum
- Frankfurt
- Hamburg
- Karlsruhe
- Köln
- München
- Bregenz
- Wien
- Bern
- .....

Zutreffendes unbedingt

Aufgabe	1	2	3	4	5	6	7	8	9	10	Summe
erreichbare Punktzahl	14	9	10	8	8	10	12	11	10	8	100
bearbeitet											
erreichte Punktzahl											

Note: \_\_\_\_\_

Hagen, den \_\_\_\_\_

Betreuer: \_\_\_\_\_

## Bescheinigung zur Vorlage beim Finanzamt

Herr/Frau \_\_\_\_\_

geb. am \_\_\_\_\_, Matr.-Nr.: \_\_\_\_\_,

hat am 05.02.2011 von 10:00 - 12:00 Uhr an der Klausur zum Kurs

**01867 „Sicherheit im Internet II“**

in \_\_\_\_\_ teilgenommen.

\_\_\_\_\_  
(Stempel)

\_\_\_\_\_  
(Prof. Dr. J. Keller)

## Leistungsnachweis / Zertifikat

Herr/Frau \_\_\_\_\_

geb. am \_\_\_\_\_, Matr.-Nr.: \_\_\_\_\_,

hat im WS 2010/2011 mit Erfolg an der Klausur zum Kurs

**01867 „Sicherheit im Internet II“**

teilgenommen.

Note: \_\_\_\_\_

\_\_\_\_\_  
(Siegel)

\_\_\_\_\_  
(Prof. Dr. J. Keller)

## **Hinweise zur Klausur des Kurses 01867 am 05.02.2011**

---

- Die Klausurdauer beträgt: zwei Stunden (10:00 bis 12:00 Uhr)
- **Es sind keine Hilfsmittel erlaubt.**
- Legen Sie Ihren Studenten- und Personalausweis zur Überprüfung durch die Aufsicht bereit.
- Füllen Sie vor Beginn der Klausur unbedingt das Deckblatt aus - und zwar in leserlicher Druckschrift.
- Füllen Sie bitte vor Inangriffnahme der Klausuraufgaben die Bescheinigung und den/das Leistungsnachweis/Zertifikat leserlich aus (natürlich bis auf die Note und Unterschrift). **Andernfalls wird kein Leistungsnachweis erstellt.**
- Die Bescheinigung für das Finanzamt ist nur mit Unterschrift und Stempel gültig.  
Nur vollständig ausgefüllte Bescheinigungen werden von uns abgestempelt, unterschrieben und Ihnen zugestellt.
- Überprüfen Sie die Vollständigkeit der Aufgabenstellungen!  
Die Klausur umfasst einschließlich der drei Deckblätter insgesamt 10 Seiten mit 10 Aufgaben.
- Schreiben Sie auf alle Lösungsbögen Ihren Namen und Ihre Matrikelnummer !
- Tragen Sie Ihre Lösungen in die dafür vorgegebenen Felder ein. Falls Sie damit nicht auskommen, benutzen Sie bitte die Rückseite der vorhergehenden Aufgabe. Verweisen Sie in diesem Fall darauf, dass diese Rückseite beschrieben ist.
- Bei Abgabe Ihrer Arbeit heften Sie bitte die ersten Seiten des übergebenen Klausur-exemplares (Deckblatt, Bescheinigungen und Hinweise zur Klausur) vor Ihre Lösungsblätter. Kontrollieren Sie zum Schluss, dass Sie Ihre gesamte Arbeit geheftet abgeben. Nachträglich eingereichte Lösungen werden von uns nicht akzeptiert.
- Die Korrektur der Klausur wird voraussichtlich bis Mitte März 2011 erfolgt sein. Wir bitten, von vorzeitigen Nachfragen abzusehen.

Bei der Bearbeitung der Klausur wünschen wir Ihnen viel Erfolg!

**Ihre Kursbetreuer**

**Aufgabe 1:****(14 Punkte)**

- a) Ein Wörterbuch enthält  $10^6$  Wörter. Ein Benutzer generiert nun sein Passwort wie folgt: er nimmt eine Ziffer von 0 bis 9, daran hängt er ein Wort  $w_1$  aus dem Wörterbuch, und daran hängt er ein Wort  $w_2$  aus dem Wörterbuch. Sind allerdings die Wörter  $w_1$  und  $w_2$  identisch, so ersetzt er  $w_2$  im Passwort durch ein Semikolon. Wie viele Passwörter muss ein Angreifer, der diese Erzeugungsroutine kennt, bei einem Wörterbuchangriff maximal probieren, bis er das Passwort des Benutzers ermittelt hat. Geben Sie die Zahl als Zehnerpotenz an.

**(6 Punkte)**

Zunächst ermitteln wir die Anzahl verschiedener Passwörter:

$$10 * 10^6 * 10^6 = 10^{13}$$

Die Anzahl verschiedener Passwörter ändert sich nicht durch die Extra-Regel, dass  $w_2$  durch ein Semikolon ersetzt wird, wenn  $w_1$  und  $w_2$  gleich sind.

Der Angreifer muss daher auch maximal (er findet es zuletzt) alle  $10^{13}$  Passwörter ausprobieren.

Quelle: keine, einfache Kombinatorik

- b) Klassifizieren Sie Angriffe auf Verschlüsselung nach der Menge an verschlüsselter bzw. unverschlüsselter Information, die dem Angreifer zur Verfügung steht. Geben Sie jeweils an, wie die Angriffsklasse heißt, und welche Information zur Verfügung steht. Nennen Sie auch die drei weiteren Angriffstypen nach Schneier. Die erste Klasse (ciphertext only Angriffe) brauchen Sie nicht zu beschreiben. **(8 Punkte)**

Erste Klasse: ciphertext only Angriffe (sollen nicht beschrieben werden)

Zweite Klasse: known plaintext Angriffe

Der Angreifer ist im Besitz von Paaren von plain text und cipher text und kann durch lineare Kryptoanalyse Rückschlüsse auf den Schlüssel anstellen.

Dritte Klasse: chosen plaintext Angriffe

Der Angreifer kann plain text zu cipher text verschlüsseln lassen und dabei den plain text so wählen, dass er Rückschlüsse auf den Schlüssel durch die Verwendung von bestimmten Mustern zulässt.

Bei der Erweiterung dieser Methode, der adaptive chosen plaintext Angriffe, basiert die Veränderung des plain text auf das Ergebnis der vorangehenden Verschlüsselung. Dadurch kann man sich interessanten Mustern annähern.

Die chosen plaintext Angriffe basieren auf der differentiellen Kryptoanalyse.

Nach Schneier gibt es ausserdem noch diese drei Angriffsarten:

- 1) Chosen Ciphertext: Wahl des cipher text und Analyse des plain text nach Entschlüsselung
- 2) Chosen Key: Analyse über die Auswirkungen der Wahl verschiedener Schlüssel
- 3) Kryptoanalyse mit Gewalt: Erzwingen des Schlüssels von einer Person durch Gewalt.

Quelle: Seiten 33 - 35 KE 1

**Aufgabe 2:****(9 Punkte)**

Gegeben sei eine SQL-Datenbank mit einer Tabelle user, die eine Spalte kennung enthält. In einem Java-Programm kann ein Benutzer eine Tastatureingabe vornehmen, die in einer Variablen Eingabe vom Typ String abgelegt wird. Mittels des Kommandos



```
String anw = new String("select * from user where kennung = " + eingabe + " ;");
```

erzeugt das Programm eine SQL-Anweisung in der Variablen anw und führt diese Anweisung auf obiger Datenbank-Tabelle aus.

Schildern Sie den in Kurseinheit 1 beschriebenen Angriff, der zur Löschung der Tabelle user führt, und beschreiben Sie Gegenmaßnahmen, um diesen Angriff zu verhindern.

Der Angreifer könnte folgenden String eingeben:

```
";drop table user;--
```

Dadurch wird der Befehl "drop table user;" ausgeführt, wodurch die Tabelle gelöscht wird. Durch die Eingabe des einfachen Gänsefüßchens mit Semikolon wird die Select-Anweisung syntaktisch beendet. Sie wird ausgeführt. Danach kommt der eingefügte, schädliche Teil des Angreifers. Ausserdem deaktiviert er durch das Kommentarzeichen "--" sämtliches SQL, das danach kommt. So erzeugt er eine Zeile mit 2 Anweisungen, wobei die erste verkürzt aber ausführbar bleibt, die zweite eingefügt ist und alle weiteren Zeichen entschärft wurden, um Fehler zu verhindern.

Als Gegenmaßnahme kann man durchführen:

- 1) Ersetzen von gefährlichen Zeichen durch ungefährliche. Hier ist das Problem, alle Zeichen zu erkennen, auch zukünftige.
- 2) Das Zulassen von eingeschränkten Zeichenräumen. Dies ist die sicherere Methode.

Bei Java und JDBC gibt es auch eine spezielle Anweisung für SQL-Abfragen. Dies geschieht über das spezielle Objekt PreparedStatement. Dieses Objekt kann feststellen, ob ein an ein SQL-Statement zu übergebender String die Struktur des SQL-Statements verändert, und falls ja, dieses nicht ausführt.

Quelle: Seiten 18 - 21 der KE 1

**Aufgabe 3:****(10 Punkte)**

- a) Wie erkennt beim Konzept der blinden Signatur die Bank den Wert einer von einem Benutzer erstellten Münze, wenn die Bank die Münze selbst nicht lesen kann, da sie vom Benutzer verändert wurde? **(5 Punkte)**

Zunächst erklären wir den Hintergrund. Damit das digitale Geld sicher vor Vervielfältigung und Fälschung ist, gehen wir davon aus, dass ein Bezahlvorgang so aussieht:  
Ein Käufer überträgt digitale Münzen in Höhe des Kaufpreises an den Verkäufer. Der Verkäufer lässt diese Münzen bei der zentralen Bank digital prüfen. Die Bank gibt die Münzen aber nicht mehr aus. Zum Schutze der Anonymität und der Fälschungssicherheit kann jede Münze nur einmal verwendet werden. Dies wird anhand der Seriennummer durchgeführt. Die Bank wird also eine große Liste von verbrauchten Seriennummern pflegen.  
Damit der Verkäufer nun anonym den Kaufbetrag in Form digitaler Münzen gutgeschrieben bekommt, erzeugt er seine eigenen Münzen. Damit diese nun gültig werden muss die Bank diese signieren. Die Bank darf die Seriennummern der Münzen nicht sehen, um die Anonymität zu wahren. Dies wird durch die blinde Signatur erreicht.  
Für jede neue zu signierende Münze erwartet die Bank nun mehrere, z.B. 100 Stück. Sie fordert vom Verkäufer 100 verschlüsselte Münzen. Der Verkäufer nutzt zur Verschlüsselung den öffentlichen Schlüssel der Bank plus je eine Zufallszahl pro Münze. Die Bank kann nun keine der 100 Münzen lesen, auch nicht die (zufällig erzeugten Seriennummern). Sie verlangt vom Verkäufer nun, 99 Münzen zu entschlüsseln. Dies geschieht anhand der Zufallszahlen, die der Verkäufer für die 99 Münzen auch an die Bank übergeben kann. Die Bank prüft nun den Wert der 99 Münzen. Sind die Münzen OK, so signiert sie blind die verbleibende Münze. Der Verkäufer kann mittels der Zufallszahl die Münze zu einer normalen Münze entschlüsseln. Dies ist technisch möglich, da gilt:  
$$\text{SignierteMünze} \bmod n = (\dots) = \text{Münze}^{\text{GeheimerSchlüssel}} * \text{Zufallszahl} \bmod n$$
  
wobei  $n$  der Modulo ist, der zu den RSA-Schlüsseln der Bank gehört.  
Quelle: Seiten 66 - 69 KE 2

- b) Wie erzeugt der Benutzer beim Konzept der blinden Signatur die Seriennummern seiner Münzen? **(5 Punkte)**

Um die Anonymität zu wahren, darf die Bank die Seriennummer der neuen Münzen nicht lesen dürfen. Die Lösung ist, dass die Seriennummer eine große Zufallszahl ist, die mit sehr niedriger Wahrscheinlichkeit schon einmal erzeugt wurde. Damit dies praktikabel ist, muss der Zufallszahlenraum natürlich sehr groß gewählt werden.  
Quelle: Seiten 69 - 70 KE 2

**Aufgabe 4:****(8 Punkte)**

Beschreiben Sie den Miller-Rabin-Primzahltest. Ist dieser Test ein Monte-Carlo- oder ein Las-Vegas-Verfahren?

Der Miller-Rabin-Primzahltest gehört zu den Probabilistischen Primzahltests. Dies bedeutet, dass er zu einer gewissen Wahrscheinlichkeit eine Primzahl erkennen kann. Ist das Ergebnis jedoch negativ, so ist dies sicher. Ist es positiv, kann die Fehlerwahrscheinlichkeit durch mehrmaliges Anwenden des Tests mit unterschiedlichen Parametern noch verringert werden.

Genau diese Wahrscheinlichkeitseigenschaften zeichnen ein Monte-Carlo-Verfahren aus.

Ein Las-Vegas-Verfahren zeichnet sich hingegen dadurch aus, dass seine Laufzeit (bzw. Ressourcenaufwand) abhängig von der Menge der Eingabe ist. Dazu gehören Sortierverfahren, deren Laufzeit gerne mittels der O-Notation beschrieben werden -  $O(n)$ .

Funktionsweise Miller-Rabin:

$x$  ist die potenzielle Primzahl, natürlich ungerade.

Man ermittelt nun  $d$  und  $j$ , für die gilt:  $x-1 = d \cdot 2^j$  und  $d$  ist ungerade.

Dann prüft man beliebig viele  $a$  (je mehr desto geringer die Fehlerwahrscheinlichkeit), für die gilt:

$a^d = 1 \pmod{x}$  oder  $a^{d \cdot 2^r} = -1 \pmod{x}$ , wobei  $0 < r < j-1$  und  $j = \text{Anzahl von Folge 0 am Ende der Binärdarstellung der Zahl } x-1$ .

Trifft eine der beiden Gleichungen zu, so ist für das jeweilige  $a$  das  $x$  als Primzahl bestätigt.

Der Miller-Rabin Test basiert auf dem kleinen Fermatschen Satz:

Wenn  $x$  eine Primzahl ist, dann gilt für jede natürliche Zahl  $a$ :

$$a^{x-1} = 1 \pmod{x}$$

Quelle: Seiten 72 - 74 KE 2

Anmerkung:

Der Anteil der Primzahlen in einer Menge natürlicher Zahlen von 1 bis (großen)  $n$  ist:  $1 / \ln(n)$

Bei kleinen  $n$  sollte man lieber nachzählen.

**Aufgabe 5:****(8 Punkte)**

- a) Welche Kreislänge (=Periodenlänge) können Sie erwarten, wenn Sie einen Pseudozufallszahlengenerator mit  $k$ -Bit Zuständen benutzen und die Zustandsübergangsfunktion zufällig aus der Menge aller möglichen Zustandsübergangsfunktionen gewählt ist? Geben Sie die Periodenlänge mithilfe von  $k$  und der O-Notation an. **(4 Punkte)**


Bei einem PZZG mit einer scheinbar zufälligen Zustandsübergangsfunktion handelt es sich um einen sogenannten Deg1-Graph. Ein solcher PZZG nutzt in der Regel ein Bit mehr, um den inneren Zustand zu speichern als die Anzahl Bit, um die Ausgabe zu machen. Damit kann er nämlich doppelt so viele Zustände speichern wie die, die er ausgibt.

Der PZZG benötigt also  $k$ -Bit für den inneren Zustand, um eine  $k-1$  Bit Ausgabe zu generieren. Bei  $k-1$  Bit Zuständen gibt es  $2^{k-1}$  Varianten, oder ausgegebene Zufallszahlen.

Die erwartete Kreislänge liegt bei der Wurzel aus der Anzahl der möglichen Zufallszahlen, also hier bei  $\sqrt{2^{k-1}}$ , in O-Notation  $O(\sqrt{2^{k-1}})$ .

Quelle: Seiten 78 - 79 KE 2

- b) Welche Kreislänge kann maximal bei einem solchen Pseudozufallszahlen-generator auftreten? Geben Sie die Kreislänge mithilfe von  $k$  an. **(4 Punkte)**

Wenn man davon ausgeht, dass alle Übergangsfunktionen möglich sind, so sollte auch die des linearen Kongruenzgenerators möglich sein, und zwar in der Form, wo die Zahlen einfach durchgezählt werden. 

In dieser Hinsicht wäre die größtmögliche Kreislänge die Anzahl an Varianten, also vom obigen Beispiel abgeleitet,  $2^{(k-1)}$

Quelle: Seiten 76 - 79 KE 2

**Aufgabe 6:** **(10 Punkte)**

- a) Beschreiben Sie kurz das 3-Wege Challenge/Response Verfahren beim Challenge Handshake Authentication Protocol (CHAP). **(5 Punkte)**

CHAP und das nicht zu empfehlende PAP sind Authentifizierungsprotokolle des Layer 2 Point to Point Protocoll (PPP).

Funktionsweise CHAP:

Es ist ein 3-Wege Challenge / Response Verfahren. Ein Client will sich an einem Server anmelden. Der Client hat eine Benutzerkennung und ein Passwort. Dem Server ist das Passwort bekannt. Der Client sendet seine Benutzerkennung. Der Server antwortet mit einem Challenge, indem er eine Zufallszahl sendet und eine Antwort erwartet. Der Client erzeugt einen Hashwert aus Benutzerkennung, Zufallszahl und Passwort, und sendet dieses als Antwort. Der Server kann nun durch nachrechnen prüfen, ob der Client das richtige Passwort benutzt, und falls ja, eine Verbindung gewähren.

Quelle: Seite 98 KE 3

Anmerkung:

PAP sendet Benutzerkennung und Passwort im Klartext an den Server, daher sollte es nur genutzt werden, wenn die Bekanntgabe des Passwortes kein Problem ist. So haben Internetanbieter z.B. die Kennung und das Passwort freigegeben, weil die Internetnutzung über den Telefonanschluss zugeordnet und über die Telefonrechnung abgerechnet werden konnte.



- b) Beschreiben Sie kurz die benötigte Infrastruktur, wenn man bei einem OpenVPN eine Authentisierung des VPN-Servers mittels Zertifikat vornehmen will. **(5 Punkte)**

Die OpenVPN-Server-Software ist frei verfügbar und kann z.B. im Userspace von Linux installiert werden. Für den OpenVPN-Client gilt dasselbe. Die Authentifizierung über Zertifikat läuft dann folgendermaßen ab:  
Auf Serverseite wird eine Certification Authority eingerichtet. Dies bedeutet, dass hier das Root-Zertifikat (ein X.509-Zertifikat), das CA-Zertifikat erzeugt wird. Dann werden das Zertifikat des Servers erstellt und die der Clients. Diese werden mittels des CA-Zertifikats signiert. Außerdem werden private Schlüssel erzeugt. Der Server, und jeder Client, müssen also folgende Dinge haben:  
1) Das CA-Zertifikat um die Signatur zu überprüfen  
2) Den privaten Schlüssel  
3) Das eigene Zertifikat  
Nach Verteilen dieser Dinge kann sich jeder beteiligte Client am Server authentifizieren und sicher kommunizieren. Der Server wird mittels des dem Client vorliegenden CA-Zertifikats authentifiziert.  
Quelle: Seite 109 KE 3

### Aufgabe 7:

**(12 Punkte)**

Ein Sensor eines network-based Intrusion Detection Systems (IDS) soll die Paketköpfe (Header) aller IP-Pakete speichern, die innerhalb von 1 Minute und 40 Sekunden durch die Leitung transportiert werden, an die der Sensor angeschlossen ist.

Welche der folgenden Aussagen treffen zu? (Hinweis: 8 MBit = 1 MByte)

- Bei einer Fast Ethernet Leitung (100 MBit/s), bei der 80% der Kapazität durch IP-Pakete belegt sind, fällt im genannten Zeitraum, wenn die Header 10% der Paketgröße ausmachen und keine weiteren Overheads betrachtet werden, eine zu speichernde Datenmenge von 100 MByte an.
- Bei einer Fast Ethernet Leitung (100 MBit/s), bei der 80% der Kapazität durch IP-Pakete belegt sind, fällt im genannten Zeitraum, wenn die Header 10% der Paketgröße ausmachen und keine weiteren Overheads betrachtet werden, eine zu speichernde Datenmenge von 10 MByte an.
- Bei einer Ethernet-Leitung (10 MBit/s), bei der 80% der Kapazität durch IP-Pakete belegt sind, fällt im genannten Zeitraum, wenn die Header 5% der Paketgröße ausmachen und keine weiteren Overheads betrachtet werden, eine zu speichernde Datenmenge von 5 MByte an.
- Bei einer Ethernet-Leitung (10 MBit/s), bei der 80% der Kapazität durch IP-Pakete belegt sind, fällt im genannten Zeitraum, wenn die Header 5% der Paketgröße ausmachen und keine weiteren Overheads betrachtet werden, eine zu speichernde Datenmenge von 1 MByte an.
- Bei einer Ethernet-Leitung (10 MBit/s), bei der keine IP-Pakete übertragen werden, fällt eine zu speichernde Datenmenge von 0 Bytes an.

**Aufgabe 8:****(11 Punkte)**

Welche der folgenden Aussagen treffen zu?

- S.147** In der Telekommunikations-Überwachungsverordnung (TKÜV) ist festgelegt, welche Möglichkeiten den Überwachungsbehörden wie Polizei und Nachrichtendiensten durch die Provider eingeräumt werden müssen.
- S.148** Die Vergabe von Domänen-Namen wird von der Internet Corporation for Assigned Names and Numbers (ICANN) gesteuert, die Vergabe von Domänen innerhalb der Domäne .de ist aber an das Deutsche Network Information Center (DENIC) delegiert.
- S.146** Ein Zugangsanbieter muss immer auch Inhaltenanbieter sein.
- S.149** Das Einbinden einer Grafik in eine HTML-Seite mittels `` kann in keinem Fall eine Urheberrechtsverletzung darstellen.
- S.148** Bei der Domänen-Registrierung prüfen die Verwaltungsorganisationen der DNS-Namen, ob die zu registrierende Domäne als Marke geschützt ist.
- S.148** Ein Diensteanbieter braucht ein Impressum (von wem werden Daten gespeichert/verarbeitet) und eine Unterrichtung (welche Daten werden zu welchem Zweck gespeichert/verarbeitet) für seine Nutzer.

**Aufgabe 9:****(10 Punkte)**

- a) Nennen Sie die drei Phasen, in denen sich verschiedene Versionen einer komplexen, 3-Schichten Web-Anwendung befinden können, so dass die Anforderungen an die verschiedenen Umgebungen maximal werden. **(3 Punkte)**

Die Webanwendung wird in 3 Versionen entwickelt. Jede Version durchläuft dabei die Phasen: Anforderung, Design, Implementierung, Test und Betrieb.  
Die erste Version beinhaltet die Grundfunktionalitäten, die zweite dann weitergehende Funktionalitäten und die dritte alle Funktionalitäten. Die 3 Versionen werden gleichzeitig entwickelt und stehen in erkenntnistheoretischer Wechselwirkung, im besten Fall von einer früheren zu der späteren. Die erste Version startet zuerst, die nachfolgenden um eine Phase versetzt.  
Die Anforderungen an die verschiedenen Umgebungen (Versionen) wird in der letzten Phase der ersten Version maximal. Denn zu diesem Zeitpunkt befinden sich die Versionen in den Phasen:

1. Version: Betrieb
2. Version: Test
3. Version: Implementierung

Quelle: Seite 164 KE 4

- b) Nennen Sie die Software-Komponenten, die auf den Rechnern für die verschiedenen Phasen installiert sein sollten. **(7 Punkte)**

Die verschiedenen Phasen sind:

Version 1: Betrieb => Produktionsumgebung

Version 2: Test => Testumgebung

Version 3: Implementierung => Entwicklungsumgebung

Produktionsumgebung:

Server Betriebssystem, Web-Server, Application-Server, Datenbank-Server, Monitoring

Testumgebung:

Identisch wie Produktionsumgebung, aber im eigenen Netz und mit eigenen Testdaten

Entwicklungsumgebung:

Server Betriebssystem, Web-Server, Application-Server,

Datenbank-Entwicklung,

Entwicklungsumgebung (Tools)

Kommunikations- und Textverarbeitungstools etc.

Quelle: Seiten 164, 165 KE 4

#### Aufgabe 10:

**(8 Punkte)**

Erklären Sie die Techniken Interposition und Compartmentalization.

Bei der Interposition wird ein System zwischen zwei andere Systeme oder zwischen Benutzer und System gesetzt, um den Datenfluss zu kontrollieren. Ein Beispiel hierfür ist ein Proxy.

Der Proxy hat die Aufgabe, nur bestimmte Daten (z.B. Web-Daten über http) durchzulassen und kann auch zu Filterzwecken eingesetzt werden, um gefährliche Inhalte zu entschärfen oder zu entfernen.

Compartmentalization ist eine Technik, um Systembereiche voneinander abzuschotten, sodass Gefahren in einer Zone nicht auf die andere übergreifen.

Ein Beispiel hierfür ist das chroot Kommando in Unix, welches eine Laufzeitumgebung für ein Programm auf einen Teil der Dateistruktur begrenzen kann.

Ein Screened subnet (DMZ) ist ein anderes Beispiel aus der Netzwerktechnik. Es ist ein abgeschottetes Teilnetz, das besonders kontrolliert wird.

Quelle Seite 158 KE 4