Musterlösungen zur
Hauptklausur
Kurs 01866 „Sicherheit im Internet I“

vom 16.09.2006

Aufgabe 1 (30 Punkte)

1P
a.) Was ist ein single point of failure?

Eine Architektur, bei der ein Fehler an einer einzelnen Stelle zum vollständigen Funktionsverlust führt.

4P
b) Nennen Sie vier der zu schützenden Eigenschaften aus dem Kurstext:

Vertraulichkeit: (engl. confidentiality) Daten sind nur für befugte Personen zugänglich.
Integrität: (engl. integrity) Daten sind korrekt und unverändert.
Authentizität: (engl. authenticity) Daten stammen vom vorgeblichen Erzeuger.
Verfügbarkeit: (engl. availability) Daten können von befugten Personen gelesen/bearbeitet werden.

2P
Wenn mit z.B. tcpdump der Netzwerkverkehr abgehört wird, welches Schutzziel wird gebrochen?

Vertraulichkeit.

2P
Wenn mit einer Paketinjektion Pakete injiziert werden, um z.B. aus Datenpaketen Schlüssel gewinnen zu können, welches Schutzziel wird gebrochen?

Integrität.

2P
Wenn Sie versuchen, z.B. einen Switch über MAC-Flooding in den Broadcast-Modus zu bekommen, welches Schutzziel wird gebrochen?

Authentizität, da die ARP-Pakete unterschiedliche MAC-Adressen enthalten müssen.

2P
Wenn Sie ein Laptop entwenden und das Passwort herausfinden, welches Schutzziel wird gebrochen?

Vertraulichkeit, Authentizität und Verfügbarkeit.

2P
Ein Denial of Service bricht welche Schutzziele?

Verfügbarkeit.

2P

Wenn IP-Adressen Rechner im Internet eindeutig identifizieren, wozu benötigt man noch ARP? Nennen Sie ein Beispiel!

IP-Adressen können dynamisch mit DHCP zugewiesen werden. ARP sorgt für eine (bijektive) Abbildung von MAC- auf IP-Adressen.

2P

Welche Information können Sie als Hacker über den anzugreifenden Zielrechner über ARP herausfinden?

Zumindest seine MAC und den Hersteller der Netzwerkkarte. Darüber – mit etwas Glück – die Information, ob sich diese in den „promiscuous“ Modus versetzen lässt.

1P

Verbreitung: wo liegt der Unterschied zwischen Viren und Würmern?

Viren verbreiten sich über Wirtsprogramme, Würmer verbreiten sich eigenständig.

Aufgabe 2 (34 Punkte)

6P

Was ist der Unterschied zwischen Leitungs- und Ende-zu-Ende-Verschlüsselung? Nennen Sie Vor- und Nachteile?

Leistungsverschlüsselung: auf dem Weg zum Zielrechner führt jeder passierte Rechner die Ver- und Entschlüsselung durch.
Hauptvorteil: nur die beiden direkten
”Nachbarn“ müssen sich auf einen Verschlüsselungsalgorithmus und einen Schlüssel einigen.
Nachteil: alle Computer auf dem Weg müssen sicher und vertrauenswürdig sein.

Ende-zu-Ende: nur Ziel- und Quellrechner ver- bzw. entschlüsseln.
Hauptvorteil: keiner der Computer auf dem Weg sieht die Nachricht im Klartext.
Nachteil: Der Absender muss sich jetzt mit jedem möglichen Empfänger auf ein Verschlüsselungsverfahren und einen Schlüssel einigen.

1P

Handelt es sich bei einer verschlüsselten E-Mail um eine Leitungs- oder Ende-zu-Ende-Verschlüsselung?

Ende-zu-Ende.

5P
Verschlüsseln Sie mit monoalphabetischer Verschlüsselung das Wort "kryptographie" unter Benutzung des Schlüssels: "xnyahpogzqwbtsflrcvmuekjdi"
Geben Sie das Ergebnis ebenfalls als Wort an.

Ergebnis: "wcdlmfocxlgzh"

2P
Wie viele mögliche Schlüssel besitzt ein Permutationskryptosystem wenn nur die ASCII-Zeichen 97-122 berücksichtigt werden sollen? (Geben Sie nur den mathematischen Ausdruck an, nicht ausrechnen).

Anzahl der möglichen Schlüssel: 26!

5P
Verschlüsseln Sie mit dem Feistel-Algorithmus die Nachricht: „FernUB“.

Die Funktion F (auf 24-Bit Zahlen) sei gegeben durch

```
F(x,y):=x or y;
```

S:=“FERNUNI“. S0:=“FER“.
Das Verfahren soll nur eine Runde laufen und das Ergebnis als Hexadezimalzahl angegeben werden.

1P S0=(70,69,82)=(0x46)(0x45)(0x52).
Aufteilen der Nachricht in 2 gleiche Teile:
1P: L0=“Fer“=(0x46)(0x65)(0x72). R0=“nUB“=(0x6E)(0x55)(0x42).
1P: R0’=S0 OR R0=(0x6E)(0x55)(0x52).
1P L0 XOR R0’=0x283020.
1P Vertauschen: L1=0x6E5552. R1=0x283020.

5P
Sie erhalten eine (dezimale) Folge von Bytes in ASCII-Codierung:

70 69 82 78 (=“FERN”).

Diese Bytefolge sei mit dem ROT13-Algorithmus entstanden.
Entschlüsseln Sie die erhaltene Bytefolge und geben Sie das Ergebnis als dezimale Folge von Bytes, sowie als Buchstabenfolge an.

<u>Hinweis:</u> „A“ hat den ASCII-Code 65 (dezimal)

ROT13 ist eine Cäsar-Chiffre auf den 26 Buchstaben des Alphabets: k_v=13.

Buchstabe	ASCII -Code	Offset	Offset+13 mod 26	ASCII -Code	Buchstabe verschlüsselt
F	70	5	18	83	S
E	69	4	17	82	R
R	82	17	4	69	E
N	78	13	0	65	A

Aufgabe 3 (36 Punkte)

2P

a) Was bedeutet es, wenn eine Primzahl g primitiv modulo p ist?

Zu jedem Element y aus Z_p außer der 0 existiert ein x aus Z_p mit $g^x \bmod p = y$.

1P

Beweisen oder widerlegen Sie, dass 7 primitiv modulo 3 ist!

7 ist primitiv modulo 3.
Beweis:
$Z_p=\{0,1,2\}$. $x \in Z_p$.
$7^0 \bmod 3=1$,
$7^1 \bmod 3=1$,
$7^2 \bmod 3=1$.

6P

Nennen Sie die drei Anforderungen an eine Hash-Funktion aus dem Kurstext und erläutern sie diese.

- **Einwegfunktion:** Zu einem gegebenen Hash-Wert h ist es praktisch unmöglich eine Nachricht M zu finden, für die H(M) = h gilt.
- **Schwache Kollisionsresistenz:** Zu einer gegebenen Nachricht M_1 ist es praktisch unmöglich, eine Nachricht $M_2 \neq M_1$ zu finden, für die $H(M_1) = H(M_2)$ gilt.
- **Starke Kollisionsresistenz:** Es ist praktisch unmöglich, zwei verschiedene Nachrichten M_1 und M_2 zu finden, für die $H(M_1) = H(M_2)$ gilt.

4P

Geburtstagsparadoxon:
Auf Ihrer Geburtstagsparty finden sich
12 30-40 jährige, 34 40-50 jährige und 12 60-70 jährige.

Wie hoch ist die Wahrscheinlichkeit, dass einer der Gäste zwischen 30 und 50 am gleichen Tag Geburtstag hat?
Geben Sie das Ergebnis als Formel an (nicht ausrechnen!).

$1-(364/365)^{46}$.

10P
Schildern Sie den Diffie-Hellmann Schlüsselaustausch zwischen zwei Parteien „A“ und „B“

Die Parteien A und B einigen sich zuerst auf eine große Primzahl p
und eine Zahl g die primitiv modulo p ist.
Diese Zahlen dürfen bekannt sein.
A wählt zufällig eine Zahl a_x und schickt $a_y = g^{a_x} \bmod p$ an B.

B wählt eine Zahl b_x und schickt $b_y = g^{b_x} \bmod p$ an A.

A berechnet aus b_y und seinem geheimen Wert a_x: $b_y^{a_x} \bmod p$.

B berechnet $a_y^{b_x} \bmod p$.

A und B haben nun beide denselben Wert berechnet.
Jemand der den Kommunikationskanal abhört, kennt nur g, p, a_y und b_y
und kann den berechneten Wert nicht rekonstruieren.

2P
Was ist ein Fingerprint, wozu wird dieser eingesetzt?

Ein Fingerprint ist mit einem Hash-Verfahren komprimierte Schlüsselinformation.
Er wird dazu eingesetzt, um eine einfache (visuelle) Prüfung zu gewährleisten.

2P
Kann SSL zusammen mit dem Telnet-Protokoll genutzt werden?

Begründen Sie Ihre Aussage!

Ja. SSL liegt oberhalb der Transport-Protokoll-Schicht unterhalb der Anwendungsebene und kann daher auch für Telnet benutzt werden.

2P
Wer kann ein Cookie setzen und über welches Protokoll?

Der Webserver über http.
Ein lokales Skript über http.

5P

Wie funktioniert der Verbindungsaufbau mit einem SSH-Server (KEIN Login)?

Client: Schickt Nachricht an Server.
Server: akzeptiert Anforderung, schickt ID-String an Client.
Prüfung durch Client, ob korrekter Daemon beim Server läuft.
Server: schickt öffentlichen Schlüssel (host key), einen Server-Schlüssel und Zufallszahl (cookie) an den Client.
Client: wählt symmetrisches Verschlüsselungsverfahren aus, generiert Sitzungsschlüssel, verschlüsselt diesen mit den Schlüsseln des Servers und schickt diese Informationen an den Server.

1P

Kann man X11-Verbindungen mit SSH tunneln?

Ja.

4P

Nennen Sie die im Kurs kennen gelernten Firewall-Architekturen!

- Packet filtering router
- Stateful inspection filter
- Application level gateway
- Screened subnet

Anhang: ASCII-Tabelle

Grossbuchstaben				Kleinbuchstaben			
Dec	**Hex**	**Z**	**Name**	**Dec**	**Hex**	**Z**	**Name**
064	0x40	@	COMMERCIAL AT	096	0x60	‘	GRAVE ACCENT
065	0x41	**A**	LATIN CAPITAL LETTER A	097	0x61	**a**	LATIN SMALL LETTER A
066	0x42	**B**	LATIN CAPITAL LETTER B	098	0x62	**b**	LATIN SMALL LETTER B
067	0x43	**C**	LATIN CAPITAL LETTER C	099	0x63	**c**	LATIN SMALL LETTER C
068	0x44	**D**	LATIN CAPITAL LETTER D	100	0x64	**d**	LATIN SMALL LETTER D
069	0x45	**E**	LATIN CAPITAL LETTER E	101	0x65	**e**	LATIN SMALL LETTER E
070	0x46	**F**	LATIN CAPITAL LETTER F	102	0x66	**f**	LATIN SMALL LETTER F
071	0x47	**G**	LATIN CAPITAL LETTER G	103	0x67	**g**	LATIN SMALL LETTER G
072	0x48	**H**	LATIN CAPITAL LETTER H	104	0x68	**h**	LATIN SMALL LETTER H
073	0x49	**I**	LATIN CAPITAL LETTER I	105	0x69	**i**	LATIN SMALL LETTER I
074	0x4a	**J**	LATIN CAPITAL LETTER J	106	0x6a	**j**	LATIN SMALL LETTER J
075	0x4b	**K**	LATIN CAPITAL LETTER K	107	0x6b	**k**	LATIN SMALL LETTER K
076	0x4c	**L**	LATIN CAPITAL LETTER L	108	0x6c	**l**	LATIN SMALL LETTER L
077	0x4d	**M**	LATIN CAPITAL LETTER M	109	0x6d	**m**	LATIN SMALL LETTER M
078	0x4e	**N**	LATIN CAPITAL LETTER N	110	0x6e	**n**	LATIN SMALL LETTER N
079	0x4f	**O**	LATIN CAPITAL LETTER O	111	0x6f	**o**	LATIN SMALL LETTER O
080	0x50	**P**	LATIN CAPITAL LETTER P	112	0x70	**p**	LATIN SMALL LETTER P
081	0x51	**Q**	LATIN CAPITAL LETTER Q	113	0x71	**q**	LATIN SMALL LETTER Q
082	0x52	**R**	LATIN CAPITAL LETTER R	114	0x72	**r**	LATIN SMALL LETTER R
083	0x53	**S**	LATIN CAPITAL LETTER S	115	0x73	**s**	LATIN SMALL LETTER S
084	0x54	**T**	LATIN CAPITAL LETTER T	116	0x74	**t**	LATIN SMALL LETTER T
085	0x55	**U**	LATIN CAPITAL LETTER U	117	0x75	**u**	LATIN SMALL LETTER U
086	0x56	**V**	LATIN CAPITAL LETTER V	118	0x76	**v**	LATIN SMALL LETTER V
087	0x57	**W**	LATIN CAPITAL LETTER W	119	0x77	**w**	LATIN SMALL LETTER W
088	0x58	**X**	LATIN CAPITAL LETTER X	120	0x78	**x**	LATIN SMALL LETTER X
089	0x59	**Y**	LATIN CAPITAL LETTER Y	121	0x79	**y**	LATIN SMALL LETTER Y
090	0x5a	**Z**	LATIN CAPITAL LETTER Z	122	0x7a	**z**	LATIN SMALL LETTER Z
091	0x5b	**[**	LEFT SQUARE BRACKET	123	0x7b	**{**	LEFT CURLY BRACKET
092	0x5c	****	REVERSE SOLIDUS	124	0x7c	**|**	VERTICAL LINE
093	0x5d	**]**	RIGHT SQUARE BRACKET	125	0x7d	**}**	RIGHT CURLY BRACKET
094	0x5e	**^**	CIRCUMFLEX ACCENT	126	0x7e	**~**	TILDE
095	0x5f	**_**	LOW LINE	127	0x7f		