Lösungsvorschläge

Kurs 1866
Sicherheit im Internet I
Hauptklausur am 31. Juli 2010

Prof. Dr. J. Keller
LG Parallelität & VLSI

Aufgabe 1 (20 Punkte)

1.1. Geben Sie drei Klassifizierungsmerkmale für den Begriff "Bedrohung" an. (3 Punkte)

Man unterscheidet technische und nicht-technische Bedrohungen. (1.2.4)
Diese können wieder in beabsichtigt und unbeabsichtigt sowie aktiv und passiv unterschieden werden.

1.2 Was ist Steganographie? (1 Punkt)

Versteckt man eine Nachricht in einer anderen, unverfänglichen und i. d. R. größeren Nachricht, so spricht man von Steganographie.

1.3. Wozu benötigt man einen Repeater? Geben Sie genau an, welche Signale der Repeater weiterleitet. (2 Punkte)

Ein Repeater ist ein Gerät, das zwei gleichartige lokale Netze miteinander verbindet und zu einem Gesamt-Netz macht. Dazu verstärkt und übertragt der Repeater alle Signale (also auch Störungen) zwischen den beiden Netzen.

1.4. Kennzeichnen Sie die folgenden Behauptungen mit wahr oder falsch. (2 Punkte)

a) Um zwei Netze unterschiedlicher Technologien (z.B: Ethernet und Token Ring) zu verbinden, benötigt man eine Bridge.
b) TCP bedeutet: Transmission Control Protocol (TCP).
c) DNS bedeutet: Domain Name System.
d) http bedeutet: host transfer protocol.

a) Falsch
b) Richtig
c) Richtig
d) Falsch (Transfer)

1.5. Wie viele mögliche IP(v4)-Adressen gibt es? Geben Sie Ihre Lösung als Zweierpotenz an. (1 Punkt)

2^32

1.6 Geben Sie drei der im Kurstext beschriebenen Virentypen an. (3 Punkte)

1. Bootsektor-Viren (BSV)
2. Dateiviren
3. Makroviren

1.7. Was ist der Hauptunterschied zwischen Viren und Würmern? (2 Punkte)

Während Viren sich mit Hilfe anderer Programme, sog. Wirtsprogramme, verbreiten, verbreiten sich Würmer eigenständig. Sie müssen also vom Benutzer mindestens einmal explizit gestartet werden. Die Schadensfunktion kann nun auch darin bestehen, dass der Wurm dafür sorgt, dass er später automatisch immer wieder gestartet wird.

1.8 Was ist ein Trojanisches Pferd? (1 Punkt)

Ein Programm, das neben seiner eigentlichen Funktion auch weitere Funktionen ausführt.

1.9. Wie viele Kombinationen müssen Sie im schlechtesten Fall bei einer Brute-Force-Attacke auf das in /etc/passwd eingetragene Passwort eines Ihnen bekannten Benutzers ausprobieren, wenn Sie wissen dass das Passwort n Zeichen lang ist, dass jedes Zeichen ein Groß- oder Kleinbuchstabe (ohne Umlaute) oder eine Ziffer von 0 bis 4 sein kann, und dass das Salt m Bit umfasst? Geben Sie die Anzahl als Formel an. (5 Punkte)

Kombinationen: (2*26+5)^n * 2^m

Aufgabe 2 (32 Punkte)

2.1. Wie funktioniert ein hybrides Verschlüsselungsverfahren? (2 Punkte)

Zunächst wird ein geheimer Schlüssel generiert und diesen Schlüssel mit einem public key Verfahren verschlüsselt an den Empfänger übertragen. Anschließend verschlüsselt man die Nachricht selbst symmetrisch mit dem gerade übertragenen geheimen Schlüssel.

2.2. Wenn Sie eine VoIP-Verbindung verschlüsseln wollen, welchen Verschlüsselungsmodus würden Sie wählen? Warum? (2 Punkte)

Stromverschlüsselung: Ein Vorteil dieser Methode ist es, dass eine Klartextnachricht nicht aufgefüllt werden muss, so dass tatsächlich nur Nutzdaten übertragen werden. Die Leitungskapazität wird besser ausgenutzt.

2.3. Verschlüsseln Sie den Text „ANFANG“ mit der
Chiffre(x) = (x + 4) mod 26, wenn die Buchstaben A bis Z mit 0 bis 25 codiert sind.
(3 Punkte)

„ERJERK“

2.4. Was ist das Kennzeichen einer polyalphabetischen Chiffre? (2 Punkte)

Klartextzeichen werden nicht immer durch das selbe Chiffrezeichen ersetzt.

2.5 Gegeben sei der Schlüssel „ABCD“, verschlüsseln Sie den Text „ANFANGAN“ mit der Vigenère-Chiffre. Die Buchstaben A bis Z sollen mit 1 bis 26 codiert sein.
(2 Punkte)

ANFANGAN
ABCDABCD (1,2,3,4)+
BPIEOIDR

2.6. Schildern Sie eine Runde des Feistel-Verfahrens in pseudo-algorithmischer Notation
(Zuweisung „<=“,
logische Operationen (<<< [linkszirkuläres Shiften],
AND, NOT, OR, XOR, z.B: a AND b, a <<< b),
Funktionen „F(x,y,…)“,
eine arithmetische Funktion „+“). Als Eingaben haben Sie L0, R0, sowie S0.
Ausgaben sind L1 und R1 (3 Punkte)

R0‘<=F(S0,R0);
R1<=R0‘ XOR L0;
L1<=R0;

2.7. Wie funktioniert der electronic code book-Mode? (1 Punkt)

Aus einem Klartextblock wird immer derselbe Geheimtextblock. Die Klartextblöcke werden unabhängig voneinander verschlüsselt. Damit wird aus einem bestimmten Klartextblock immer der gleiche Geheimtextblock.

2.8. Wie funktioniert der cipher block chaining? (1 Punkt)

Jeder Klartextblock wird vor seiner Verschlüsselung mit dem vorhergehenden Geheimtextblock verknüpft. Dazu benutzt man die Funktion XOR.

2.9. Welchen Schlüssel benutzt man für die Entschlüsselung einer Nachricht bei einer asymmetrischen Verschlüsselung? (1 Punkt)

Man benutzt seinen eigenen privaten Schlüssel.

2.10 Auf welchem schwierigen mathematischen Problem beruht die Sicherheit der El-Gamal Verschlüsselung? (1 Punkt)

Der Berechnung von diskreten Logarithmen über endliche Körper.

2.11. Schildern Sie das Verfahren von Diffie-Hellmann zur Übermittlung eines geheimen Schlüssels? (5 Punkte)

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 nun zufällig eine geheime Zahl ax und schickt $ay = g^{ax} \bmod p$ an B.
B wählt eine Zahl bx und schickt $by = g^{bx} \bmod p$ an A.

Jetzt berechnet A aus dem empfangenen by und seinem geheimen zufällig gewählten Wert ax den Wert: $by^{ax} \bmod p$. Genauso berechnet B den Wert $ay^{bx} \bmod p$.

A und B haben nun beide denselben Wert berechnet, da die folgende Umformung (immer mod p) gilt:
$by^{ax} = (g^{bx})^{ax} = g^{ax * bx} = (g^{ax})^{bx} = ay^{bx}$

Jemand der den Kommunikationskanal abhört kennt aber nur g, p, ay und by und kann den berechneten Wert nicht rekonstruieren.

2.12. Was ist eine Kollision bei Hash-Werten und wieso gibt es überhaupt Kollisionen? (2 Punkte)

Die Abbildung einiger Elemente der Ursprungsmenge auf denselben Hash-Wert.

Kollisionen gibt es, da die Zielmenge kleiner ist als die Ursprungsmenge. Daher müssen einige Elemente der Ursprungsmenge auf denselben Hash-Wert abgebildet werden.

2.13. Gegeben sei eine Hash-Funktion, die 1 000 000 unterschiedliche Hash-Werte erzeugen kann, z. B. Zahlen aus dem Intervall von 0 bis 999 999.

a) Weiterhin sei eine Nachricht N mit Hash-Wert H(N) gegeben. Wie viele Nachrichten müssen Sie erzeugen, um mit einer Wahrscheinlichkeit größer als 1/2 eine Nachricht mit demselben Hash-Wert H(N) zu erhalten? (2 Punkte)

b) Wie viele zufällige verschiedene Nachrichten müssen Sie erzeugen, damit mit einer Wahrscheinlichkeit größer als 1/2 mindestens zwei (beliebige) dieser Nachrichten denselben Hash-Wert haben? (3 Punkte)

Antwort, s. Übungsaufgabe 2.5

2.14. Was ist der prinzipielle Unterschied in der Berechnung zwischen Message Authentication Codes (MACs) und Digitalen Signaturen? (1 Punkt)

Bei MACs verwendet man einen geheimen Schlüssel, bei Digitalen Signaturen einen privaten und einen öffentlichen Schlüssel.

2.15. Was macht eine Bridge-CA? (1 Punkt)

Eine Bridge-CA signiert Zertifikate von CAs, die zwar nicht den Standards des Signaturgesetzes entsprechen, die dafür aber trotzdem bestimmte pragmatisch orientierte Standards erfüllen.

Aufgabe 3 (10 Punkte)

3.1. Wie funktioniert RSA Authentisierung bei SSH-Verbindungen (Client/ Server) bei der erstmaligen Verbindung des Client mit dem Server? (6 Punkte)

Der Client erzeugt ein eigenes Schlüsselpaar aus privatem und öffentlichem Schlüssel. Er kopiert seinen öffentlichen Schlüssel auf den Server. Wenn der Benutzer das erste Mal eine SSH-Verbindung zum Server aufbaut, kann der öffentliche Schlüssel des Servers automatisch (und erst einmal nicht verschlüsselt) zum Client übertragen werden. SSH zeigt dem Benutzer auf der Client-Seite den Fingerprint des öffentlichen Schlüssels des Servers an. Der Client sollte den Fingerprint prüfen und dann die Korrektheit bestätigen. Nun wird der öffentliche Schlüssel des Servers auf dem Client gespeichert.

3.2. Schildern Sie die Grundidee der User Account Control (ab Windows Vista) (4 Punkte)

Die Grundidee von UAC ist es, dass der Benutzer gefragt wird, wenn eines der Programme das er gestartet hat eine sicherheitskritische Funktion ausführen will. Dabei werden alle Funktionen die Administratorrechte brauchen als sicherheitskritisch angesehen. Auch wenn der Benutzer mit einer Kennung aus der Administratorengruppe angemeldet ist, wird die kritische Funktion nicht einfach ausgeführt, sondern es erscheint ein Dialogfenster in dem der Benutzer die Ausführung explizit bestätigen muss.

Aufgabe 4 (14 Punkte)

4.1. Wozu dient caching beim Proxy? (1 Punkt)

Hat der erste interne Benutzer eine bestimmte Seite geladen, so können nachfolgende Anforderungen für dieselbe Seite aus dem proxy (cache) bedient werden. Dies senkt die Netzlast und führt zu kürzeren Antwortzeiten.

4.2. Warum anonymisiert ein Proxy, wenn http-requests von innen nach außen über den Proxy gehen? (1 Punkt)

Jeder http-request von innen wird vom proxy nach außen weitergegeben. Für einen Web-Server im Internet kommt der http-request also vom proxy und nicht mehr von einem einzelnen Benutzer.

4.3. Was ist der Unterschied zwischen Screened Subnet und DMZ? (1 Punkt)

Es gibt keinen.

4.4. Was ist der Unterschied in Bezug auf die Hardware zwischen single- und dual homed application level gateways (ALG)? (1 Punkt)

Ein dual-homed ALG hat zwei, ein single-homed ALG einen Netzwerkanschluss.

4.5. Was sind mangle Regeln bei iptables? (1 Punkt)

Mangle-Regeln erlauben beliebige Veränderungen an Paketen vorzunehmen, z. B. den TTL-Zähler zu ändern.

4.6. Was bedeutet die Abkürzung ITIL und wie hängt ITIL mit IT-Sicherheit zusammen? (3 Punkte)

IT Infrastructure Library (ITIL) .

In der ITIL werden best practises, also bewährte Vorgehensweisen, vorgestellt. Sie bestehen zum einen darin, wie man IT-Dienste vernünftig (zuverlässig, kosteneffizient, usw.) anbietet und zum anderen auch darin, wie die Prozesse zur Änderung der IT-Dienste aussehen sollten. Da sich Geschäftsprozesse immer schneller verändern, muss auch die IT sich immer schneller anpassen und evtl. veränderte oder neue Dienste anbieten.

Das Thema IT-Sicherheit wird insofern berührt, als Sicherheitsprobleme immer zu Beeinträchtigungen führen und damit zu Geschäftsproblemen.

4.7. Ordnen Sie die folgenden Risiken in die angegebene probability impact Matrix ein:

1. Ein Hacker manipuliert die Homepage derart, dass dort dumme Witze und Links zu zwielichtigen Web-Servern installiert werden.
2. Der Administrator-Zugang zum Web-Server ist eine telnet Verbindung über das Internet.
3. Durch Probleme in der internen Ablauforganisation werden die HTML Seiten auf dem Server nicht rechtzeitig aktualisiert, sondern mit 1 Stunde Verzögerung. (6 Punkte)

Auswirkung	Hoher Schaden			
	Niedriger Schaden			
		Niedrig		Hoch
		Eintrittswahrscheinlichkeit		

Lösung, s. Übungsaufgabe 4.5