Kurs 1867 Sicherheit im Internet II

Hauptklausur am 19. Februar 2005

Lösungsvorschläge

Prof. Dr. J. Keller
LG Parallelität und VLSI

Aufgabe 1 (20 Punkte):

a) Beschreiben Sie den *Quadratic Sieve* Algorithmus. (10 Punkte)

Lösung: *Siehe Kurseinheit 1, Abschnitt 1.8.5, Seite 32*

b) Führen Sie die Faktorisierung der Zahl $n = 91$ mittels des Quadratic Sieve Algorithmus durch. (10 Punkte)

Lösung: *Man wählt* $x = 10$, *denn* $x^2 = 100$ *ist die kleinste Quadratzahl, die größer als* $n = 91$ *ist. Es gilt* $x^2 - n = 100 - 91 = 9$. *Da* 9 *eine Quadratzahl ist, erhalten wir* $y = \sqrt{9} = 3$. *Es gilt* $x - y = 7$ *und* $x + y = 13$. *Dies sind bereits Teiler von* n, *so dass die Bildung des größten gemeinsamen Teilers von* $x + y$ *bzw.* $x - y$ *und* n *entfallen kann.*

Aufgabe 2 (10 Punkte):

Beschreiben Sie die Schritte, die ein Kunde beim Kauf eines Artikels per Internet unter Nutzung des Paybox-Bezahlverfahrens ausführen muss.

Lösung: *Siehe Kurseinheit 2, Abschnitt 2.2.8, Seiten 57–58.*

Aufgabe 3 (20 Punkte):

a) Nennen Sie die Arten von Intrusion Detection Systemen (IDS), die im Kurs unterschieden werden? (5 Punkte)

Lösung: *Network-based IDS, Host-based IDS, Mischformen. Siehe Kurseinheit 3, Abschnitt 3.3.2, Seite 99.*

b) Welche Art IDS erkennt in der Regel nicht einen Angriff an sich, sondern nur seine Auswirkungen? (3 Punkte)

Lösung: *Das Host-based IDS, siehe Kurseinheit 3, Abschnitt 3.3.2, Seite 100.*

c) Ein Network-based IDS hängt an einem Netzwerklink mit der Bandbreite 80 MBit/s ($1\,M = 10^6$) und protokolliert von jedem IP-Paket die source address sowie die destination address (je 4 Byte). Alle IP-Pakete seien 80 Byte groß. Wieviele IP-Pakete pro Sekunde kann das IDS protokollieren, wenn die Bandbreite zur Protokoll-Festplatte 1 MByte/s beträgt? Wie hoch ist dann die prozentuale Auslastung des Netzwerklinks? Begründen Sie Ihre Antworten. (12 Punkte)

Lösung: *Wenn die Bandbreite zur Protokoll-Festplatte 1 MByte/s beträgt, und von jedem IP-Paket zwei Adressen der Größen 4 Byte protokolliert wird, dann können höchstens* $1\,M/8 = 125.000$ *IP-Pakete pro Sekunde protokolliert werden. Diese Pakete haben eine Gesamtgröße von* $125.000 \cdot 80 = 10.000.000$ *Byte. Die Bandbreite des Netzwerklinks beträgt 80 MBit/s, also* $80.000.000/8 = 10.000.000$ *Byte pro Sekunde. Mit den 125.000 IP-Paketen pro Sekunde ist der Netzwerklink also zu 100% ausgelastet.*

Aufgabe 4 (8 Punkte):

a) Nennen Sie die im System– bzw. Software-Entwurf üblichen Phasen. (5 Punkte)

Lösung: *Analyse, Design, Implementierung, Test, Betrieb. Siehe Kurseinheit 4, Abschnitt 4.3, Seite 141.*

b) In welcher Phase muss entschieden werden, ob ein System nur mit einer PIN zu Beginn der Sitzung oder mit PIN und TANs arbeitet, wobei bei jeder Transaktion eine TAN eingegeben werden muss. (3 Punkte)

Lösung: *Diese Entscheidung muss in der Design-Phase getroffen werden. Siehe Kurseinheit 4, Abschnitt 4.3.2, Seite 144.*

Aufgabe 5 (20 Punkte):

a) Beschreiben Sie kurz die Technik des Tunneling. (6 Punkte)

Lösung: *Siehe Kurseinheit 3, Abschnitt 3.2.2, Seite 86.*

b) Wird beim Einsatz von Encapsulation Security Payload (ESP) ein symmetrisches oder ein asymmetrisches Verschlüsselungsverfahren benutzt? Welche Möglichkeiten bestehen zum Schlüsseltausch? Bitte erläutern Sie die Durchführung bei den verschiedenen Möglichkeiten. (14 Punkte)

Lösung: *Es wird ein symmetrisches Verschlüsselungsverfahren benutzt. Der Schlüsseltausch kann entweder manuell oder automatisch nach dem Internet Key Exchange (IKE) erfolgen. Zur Erläuterung siehe Kurseinheit 3, Abschnitt 3.2.2, Seite 95–96.*

Aufgabe 6 (22 Punkte):

a) Was versteht man unter URL Hacking? Wozu wird URL Hacking außer zum Ausspähen von Passwörtern noch benutzt? (8 Punkte)

Lösung: *Siehe Kurseinheit 1, Abschnitt 1.6, Seite 13. Außer zum Ausspähen von Passwörtern kann man URL Hacking z.B. auch dazu benutzen, die Anzahl der Besuche auf der eigenen Seite zu erhöhen, um so die eigenen Werbeeinnahmen zu verbessern.*

b) Wie kann man im folgenden Programm einen Buffer-Overflow Angriff ausführen? (14 Punkte)

```
#include <stdio.h>

int main(int argc,char *argv[])
{ char strng1[8] = "TestWd\0"; /* Gespeichertes Passwort */
  char strng2[8];

  printf("Passwort eingeben!\n");
  gets(strng2);

  if(strncmp(strng1,strng2,8)){
    printf("Falsches Passwort!\n"); exit(-1);
  }else application();

  return 0;
}
```

Lösung: *In den meisten Rechnersystemen ist die Adresse von* `strng1` *gerade um 8 größer als die von* `strng2`*. Wird nun für* `strng2` *eine Zeichenkette der Länge 16 eingegeben, bei der die beiden Hälften gleich sind, so nimmt* `strncmp()` *Gleichheit an, da es nur 8 Zeichen überprüft, und es wird nach* `application()` *verzweigt, ohne dass ein korrektes Passwort vorliegt.*