Fachbereich Informatik

Lehrgebiet Technische Informatik II

Kurs 1866 „Sicherheit im Internet“

Lösungsvorschläge zur

Hauptklausur im SS 2003

am 20.09.2003

Aufgabe 1 (7 Punkte)

Warum sollen Passwörter auch dann nicht für Benutzer zugänglich abgespeichert sein, wenn die Passwörter durch eine Einwegfunktion verschlüsselt sind?

Viele Benutzer verwenden normale Worte oder Namen als Passwörter. Darum kann ein Programm, das von einem Lexikon gespeist wird und alle Wörter daraus verschlüsselt und mit den gespeicherten verschlüsselten Passwörtern vergleicht, viele Passwörter erfahren.

Aufgabe 2 (17 Punkte)

a) Zeichnen Sie das Prinzip der Berechnung eines Message Authentication Codes (MAC). (10 Punkte)

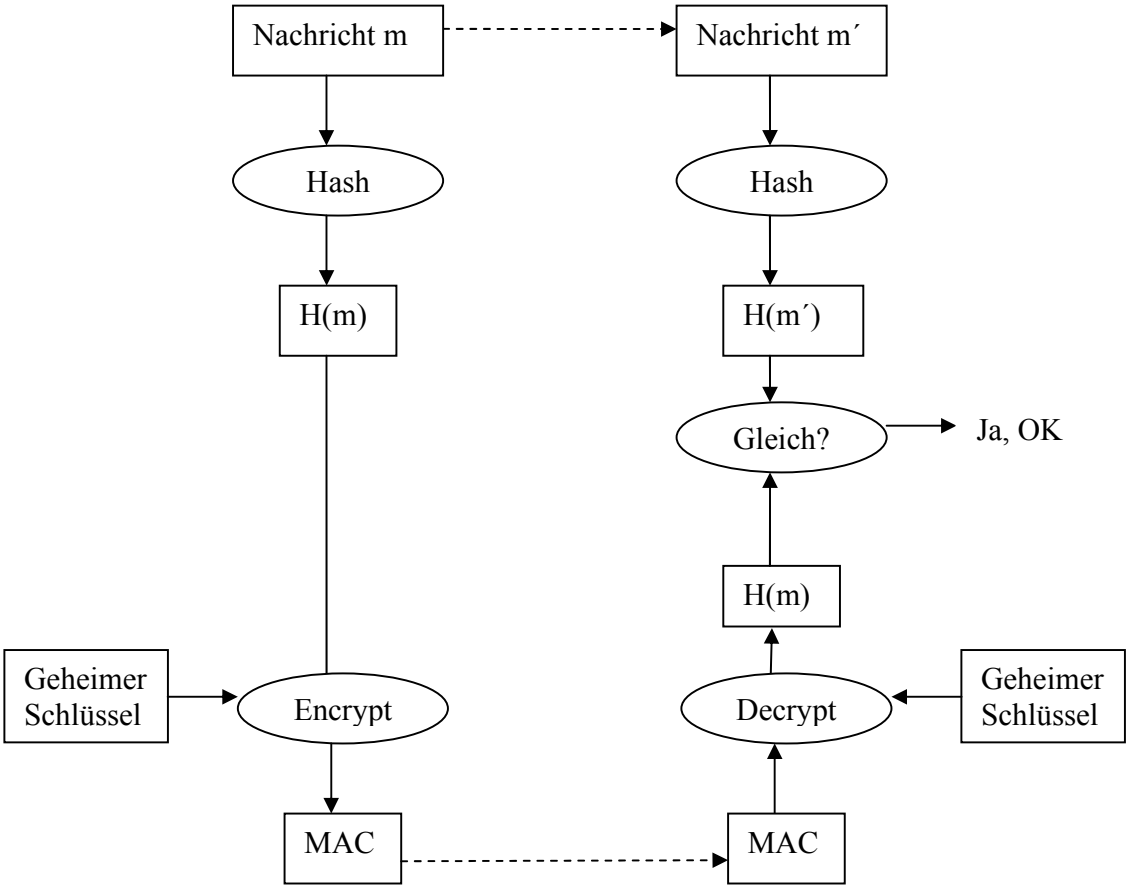

Abbildung: Prinzip der Message Authentication

b) Welches Verfahren erhält man, wenn man bei der Berechnung eines Message Authentication Code (MAC) den symmetrischen Verschlüsselungsalgorithmus gegen einen asymmetrischen Verschlüsselungsalgorithmus vertauscht? (7 Punkte)

Digitale Signatur, siehe Abschnitt 2.6.2

Aufgabe 3 (15 Punkte)

a) Nennen Sie 4 Maßnahmen zur Installation eines sicheren Webservers. (8 Punkte)

Nur benötigte Programme aufspielen.
Alle bekannten Patches aufspielen.
Nur benötigte Ports öffnen.
Nur benötigte, dienstspezifische Benutzer mit entsprechend eingeschränkten Rechten einrichten.
Prozesse unter diesen Benutzern und nicht unter Admin laufenlassen.
Installation mit Scanner o.ä. Tools auf Sicherheit testen.
Integritätstest vorsehen, d.h. Prüfsummen anlegen.

b) Warum sollte die Anzeige von Dateien in einem Verzeichnis des Webservers abgeschaltet sein? Warum kann man argumentieren, dass diese Vorgehensweise unter die Rubrik "Security by Obscurity" fällt? (7 Punkte)

Der zugreifende Benutzer erhält sonst auch Einblick in die Dateinamen, zu denen kein Link führt, und kann per URL darauf zugreifen.
Allerdings könnte auch auf anderem Wege die Kenntnis der Dateinamen gelingen. Enthält eine solche Datei schützenswerte Inhalte, so sollte sie in einem anderen Verzeichnis mit Zugangsbeschränkung liegen.

Aufgabe 4 (19 Punkte)

a) Nennen Sie die Aufgaben einer Firewall. (7 Punkte)

Die Aufgaben einer Firewall sind :

- Festlegung, welcher Internet-Nutzer auf welche interne Ressource bzw. Dienst zugreifen darf.
- Festlegung, welcher interne Nutzer/Prozess auf welchen Dienst bzw. Ressource des Internet zugreifen darf.
- Gegebenenfalls Adressumsetzung.

b) Definieren Sie Paketfilter-Regeln für folgende Anforderungen: (12 Punkte)

- 3 interne Rechner A,B,C mit IP-Adressen 132.176.72.1,2,3
- jeder Rechner darf per WWW ins Internet
- Nur zu Rechner A darf eine WWW-Verbindung aus dem Internet aufgebaut werden.
- telnet ist verboten,
- Nur zu Rechner C darf eine telnet-Verbindung aus dem Internet aufgebaut werden
- Nur Rechner B darf emails senden und empfangen
- ftp ist verboten in beiden Richtungen

Auf dem Paketfilter sollten die folgenden Regeln implementiert sein:

Nummer	Bedingung	Aktion
1	Port 80	Durchlassen
2	Port 80 UND IP-Adresse = 132.176.72.1	Durchlassen
3	Port 23	verwerfen
4	Port = 23 UND IP-Adresse = 132.176.72.3	Durchlassen
5	Port = 25 UND IP-Adresse = 132.176.72.2	Durchlassen
6	Port = 21	verwerfen

Aufgabe 5 (13 Punkte)

Beschreiben Sie die Authentisierung eines Clients, der mit einem Server kommunizieren will, mittels eines Kerberos Authentication-Servers. Unterscheiden Sie dabei die Varianten mit bzw. ohne Ticket-Granting-Server.

siehe Abschnitt 3.4.2

Aufgabe 6 (29 Punkte)

a) Beschreiben Sie die Tätigkeiten zur Erstellung eines Paares aus öffentlichem und geheimem Schlüssel für den RSA Algorithmus. (6 Punkte)

Um ein Schlüsselpaar zu erzeugen wählt man zunächst zwei große Primzahlen p und q. Dann wird das Produkt $n = p.q$ berechnet. Für jede Zahl $m \leq n$ gilt nun die folgende Gleichung: $m^{k(p-1)(q-1)+1} \bmod n = m.$

Anschließend wählt man eine natürliche Zahl e. Der öffentliche Schlüssel besteht aus e und n. Der geheime Schlüssel d wird so berechnet, daß
$e.d \bmod (p-1)(q-1) = 1$ gilt.

b) Beschreiben Sie die Berechnungen zur Ver- und Entschlüsselung mit dem RSA Algorithmus. (6 Punkte)

Eine Nachricht m wird mit dem öffentlichen Schlüssel wie folgt verschlüsselt: $Crypt(m) = m^e mod\ n$

Zur Entschlüsselung wird $c=Crypt(m)$ in folgende Formel eingesetzt: $DeCrypt(c) = c^d\ mod\ n$

c) Zeigen Sie, dass die Entschlüsselung eines Textes, der mit einem privaten Schlüssel verschlüsselt wurde, mit dem dazu gehörenden öffentlichen Schlüssel möglich ist. (6 Punkte)

Da die Multiplikation kommutativ ist kann man auch mit dem öffentlichen Schlüssel wieder entschlüsseln.

$$
\begin{aligned}
DeCrypt(Crypt(m)) &= Crypt(m)^e\ mod\ n \\
&= (m^d)^e\ mod\ n \\
&= m^{e.d}\ mod\ n \\
&= m^{k(p-1)(q-1)+1}\ mod\ n \\
&= m
\end{aligned}
$$

d) Person A hat als Primzahlen *p=23* und *q = 41* gewählt, sowie *e=7.* Person A teilt Person B ihren öffentlichen Schlüssel e, n mit. Person B verschlüsselt damit eine Nachricht M und erhält *C=545 .* Berechnen Sie für Person A den geheimen Schlüssel d und entschlüsseln Sie C. (11 Punkte)

Es gilt *(p-1)(q-1)=880* und *e=7*.
Es ist d zu berechnen so daß gilt

e.d=1 mod(p-1)(q-1)
7.d = 1 + k.880

Wir bestimmen *k.880 + 1* für *k=1, 2, 3....* bis das Ergebnis durch 7 teilbar ist.

Dies gilt für *k=4*
da *4.880 + 1= 3521 = 7.503*

Also ist *d=503*.

Es gilt $d=503=(11110111)_2$

Damit $M = C^d \bmod n = 545^{2^0} \cdot 545^{2^1} \cdot 545^{2^2} \cdot 545^{2^4} \cdot 545^{2^5} \cdot 545^{2^6} \cdot 545^{2^7} 545^{2^8} \bmod 943$

$= 545 \cdot 923 \cdot 400 \cdot 857 \cdot 795 \cdot 215 \cdot 18 \cdot 324 \bmod 943$

= 35

Damit die zwischen Ergebnisse nicht zu groß werden, sollte auch zwischendurch modulo 943 gerechnet werden.

Hinweis:

1. Um d zu finden, suchen Sie kleine Vielfache von (p-1)(q-1), die, wenn sie um 1 erhöht werden, durch e teilbar sind.

2. Um 545^d zu rechnen, bestimmen Sie die Binärdarstellung $d_8 d_7 ... d_0$ von d und benutzen

$$545^d \bmod n = 545^{\sum_{i=0}^{8} 2^i \cdot d_i} \bmod n = \prod_{i=0}^{8} 5^{2^i \cdot d_i} \bmod n$$

Hierbei gilt

i	$545^{2^i} \bmod n$
1	923
2	400
3	633
4	857
5	795
6	215
7	18