

Übung zur Vorlesung ”Grundlagen Betriebssysteme und Systemsoftware”

(Prof. Dr. J. Schlichter, WS 2008 / 2009)

Übungsleitung: Dr. Georg Groh (grohg@in.tum.de)

Tutoren: Dipl. Inform. Vivian Prinz (prinzv@in.tum.de), Dr. Nils Kammenhuber (kammenhuber@net.in.tum.de), Dipl. Inform. Robert Schmohl (schmohl@in.tum.de), Dipl. Inform. Dipl. Geogr. Jan Herrmann (hermanj@in.tum.de), Dipl. Inform. Robert Eigner, David Brodski (brodski@in.tum.de), Yang Guo (yang.guo@gmx.de), Jan Finis (finis@in.tum.de), Martin Levihn (levihn@in.tum.de)

<http://www11.in.tum.de/Veranstaltungen/GrundlagenBetriebssystemeundSystemsoftware0809>

<http://www11.in.tum.de/Veranstaltungen/GrundlagenBetriebssystemeundSystemsoftware0809/uebung>

Blatt 12

- Abgabe: bis 02.02.2009 12:00 Uhr per E-Mail an den Tutor der eigenen Gruppe. Die Mail soll einen Zip-Ordner als attachment haben, der für jede Hausaufgabe einen Unterordner enthält, in dem die Lösung als .txt-File(s), als .c-File(s) o.ä. enthalten ist.
- Musterlösungen Hausaufgaben: ab 02.02.2009 12:00 Uhr auf der Übungswebseite zum Download.
- Musterlösungen Tutoraufgaben: ab 09.02.2009 12:00 Uhr auf der Übungswebseite zum Download.

Stoff

Es sei empfohlen folgende Literatur durchzuarbeiten:

- Skript Kapitel 9 Sicherheit in Rechensystemen
- Tanenbaum Kapitel 9 Security

1 Hausaufgabe (Sicherheit)

Lernziele

Vertiefung des Wissens zum Thema Sicherheit in Rechensystemen.

Aufgabe

In dieser Aufgabe werden Grundlagen zur Sicherheit in Verteilten Systemen behandelt. Asymmetrische Kryptosysteme spielen hier eine wesentliche Rolle.

1.1 Teilaufgabe

Beantworten Sie jeweils kurz:

1. Was ist der Unterschied zwischen Authentifizierung und Authorisierung?
2. Was ist der Unterschied zwischen Vertraulichkeit bzw. Geheimhaltung und Integrität?
3. Warum müssen Authentifizierung und Nachrichtenintegrität immer gemeinsam gewährleistet werden?

1.2 Teilaufgabe

Sie haben in der Vorlesung den RSA-Algorithmus kennengelernt, der nach seinen Erfindern Rivest, Shamir, Adleman benannt wurde. Zur Wiederholung: Es werden zunächst zwei sehr große Primzahlen, p und q , bestimmt. Aus diesen wird $n = p * q$ und $x = (p - 1) * (q - 1)$ berechnet. Anschließend wird eine Zahl e gewählt, so dass diese keinen gemeinsamen Teiler mit x besitzt. Darauf wird eine Zahl d ermittelt, die $\text{mod}(d * e, x) = 1$ erfüllt. Das Zahlenpaar (n, e) wird als öffentlicher Schlüssel verwendet, das Paar (n, d) dient als privater Schlüssel.

Führen Sie die folgenden Berechnungen durch:

1. Wählen Sie $p = 47$ und $q = 71$. Berechnen Sie daraus n und x . Nehmen Sie für e die Zahl 79 an. Über den erweiterten Euklidischen Algorithmus kann daraus d mit 1019 bestimmt werden.
2. Benutzen Sie e als privaten Schlüssel und kodieren Sie damit die Nachricht "6882326879666 68003". Dabei müssen Sie die Nachricht in Blöcke gleicher Länge zerteilen, die jeweils kleiner als n sind. Diese Blöcke transformieren Sie, indem Sie diese mit e exponentieren und Modulo n nehmen. Hängen Sie die Ergebnisse einfach aneinander, um die verschlüsselte Nachricht zu generieren. Für diese Rechnungen empfiehlt es sich, den "Basic Calculator" unter Unix zu verwenden, den Sie über den Befehl "bc" aufrufen können. (Modulo wird durch das Zeichen % repräsentiert.) Handelsübliche Taschenrechner sind durch die Größe der Ergebnisse überfordert und liefern falsche Ergebnisse.
3. Entschlüsseln Sie die Nachricht, indem Sie die verschlüsselten Blöcke mit d potenzieren und anschließend eine Modulo- n -Operation ausführen.

Abgabe

Antworten zu den Fragen als .doc, .pdf, oder .txt-Datei.

2 Hausaufgabe (Sicherheit II)

Lernziele

Vertiefung des Wissens zum Thema Sicherheit in Rechensystemen / Elementare Kryptographie. Trainieren des passiven und aktiven Umgangs mit Englisch als für die Informatik wichtigster Sprache in Zusammenhang mit Informatik-Problemen.

Aufgabe

Beantworten Sie die folgenden (auf Englisch formulierten) Fragen bzw. lösen Sie die folgenden kleineren Aufgaben aus dem Tanenbaum! Geben Sie die Antworten wenn möglich in englischer Sprache!

2.1 Teilaufgabe

Consider a secret-key cipher that has a 26×26 matrix with the columns headed by ABC ... Z and the rows are also ABC ... Z. Plaintext is encrypted two characters at a time. The first character is the column; the second is the row. The cell formed by the intersection of the row and column contains two ciphertext characters. What constraint must the matrix adhere to and how many keys are there?

2.2 Teilaufgabe

Break the following mono-alphabetic cipher (The plaintext consists of letters only and is a well known excerpt from a poem by L. Carroll

```
kfd ktbd fzm eubd pzyiom mztx tu kzyg ur bzha kfthcm
ur mfudm zhx mftnm zhx mdzythc pzq ur ezsszcdm zhx gthcm
zhx pfa kfd mdz tm sutythc fuk zhx pfdkfdi ncm fzld pthcm
sok pztk z stk kfd uamkdim eitdx sdruid pd fzld uoi efzk
rui mubd ur om zid uok ur sidzfk zhx zyy ur om zid rzk
hu foiaa mztx kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk
```

2.3 Teilaufgabe

Consider the following way to encrypt a file. The encryption algorithm uses two n -byte arrays, A and B. The first n -byte are read from the file into A. Then $A[0]$ is copied to $B[i]$, $A[1]$ is copied to $B[j]$, $A[2]$ is copied to $B[k]$, etc. After all n bytes copied to the B array, that array is written to the output file and n more bytes are read into A. This procedure continues until the entire file has been encrypted. Note that here encryption is not being done by replacing characters with other ones, but by changing their order. How many keys have to be tried to exhaustively search the key space? Give an advantage of this scheme over a monoalphabetic substitution cipher?

2.4 Teilaufgabe

Secret key cryptography is more efficient than public key cryptography but requires the sender and receiver to agree on a secret key in advance. Suppose that the sender and receiver have never met, but there exists a trusted third party that shares a secret key with the sender and also shares a (different) secret key with the receiver. How can the sender and receiver establish a new shared secret key under these circumstances?

2.5 Teilaufgabe

Not having the computer echo the password is safer than having it echo an asterisk for each character since the latter discloses the password length to anyone who can see the screen, Assuming that passwords consist of upper- and lower-case letters and digits only, and that passwords are between 5 and 8 characters long: How much safer is it not displaying anything (as in Unix)?

Abgabe

Antworten zu den Fragen als .doc, .pdf, oder .txt-Datei.

3 Hausaufgabe (freiwillig)(Wiederholung des Stoffes / Vorschläge für Prüfungsaufgaben)

Aufgabe/Hintergrund/Lernziele

Ein modernes Konzept aus dem Bereich Prüfungsmethodik ist es, Studenten selbst Prüfungsfragen vorschlagen zu lassen. Es hat sich gezeigt, dass die Aufgaben, die von Studenten vorgeschlagen werden, in der Regel recht gut dem geforderten Niveau der Prüfung entsprechen. Gleichzeitig vertieft das Erstellen einer Aufgabe zum Stoff diesen sehr effektiv.

Gehen Sie davon aus, dass Sie eine Klausur zu unserer Vorlesung erstellen müssen (5 Aufgaben a 8 Punkte, 90 Minuten Zeit, keine Hilfsmittel), die ein für unseren Fall adäquates Schwierigkeitsniveau besitzt.

Entwerfen Sie eine Aufgabe für diese Klausur! Geben Sie auch eine Musterlösung an!

Geeignete Aufgaben aus den von Ihnen vorgeschlagenen Aufgaben werden (ggf. leicht modifiziert) ggf. für die Klausur im Februar und die Klausur im April herangezogen!

Abgabe

Eine Klausuraufgabe mit Lösung als .doc, .pdf, oder .txt-Datei.

4 Tutoraufgabe (Sicherheit III)

Lernziele

Vertiefung des Wissens zum Thema Sicherheit in Rechner-Systemen / Elementare Kryptographie

Aufgabe

Beantworten Sie die folgenden Fragen bzw. lösen Sie die folgenden kleineren Aufgaben aus dem Tanenbaum!

4.1 Teilaufgabe

Name a C compiler feature that could eliminate a large number of security holes. Why is it not more widely implemented?

4.2 Teilaufgabe

Name one disadvantage of a polymorphic encrypting virus from the point of view of the virus writer!

4.3 Teilaufgabe

What is the difference between a virus and a worm? How do they each reproduce?

4.4 Teilaufgabe

Name three characteristics that a good biometric indicator must have for it to be useful as a login authenticator!

4.5 Teilaufgabe

How can a parasitic virus (a) ensure that it will be executed before its host program and (b) pass control back to its host after doing whatever it does?

4.6 Teilaufgabe

Often one sees the following instructions for recovering from a virus attack:

1. Boot the infected system
2. Back up all files to an external medium
3. Run fdisk to format the disk
4. Reinstall the OS from the original medium

5. Reload the files from the external medium

Name two serious errors in that procedure!

4.7 Teilaufgabe

To verify that an applet has been signed by a trusted vendor, the applet vendor may include a certificate signed by a trusted third party that contains its public key. However, to read the certificate, the user needs the trusted third party's public key. This could be provided by a trusted fourth party, but then the user needs that public key. It appears that there is no way to bootstrap the verification system, yet existing browsers use it. How could it work?

Abgabe

Die Fragen sollen gemeinsam in den Übungen erarbeitet werden. Sie brauchen nicht abgegeben zu werden.

5 Tutoraufgabe (Wiederholung)

Aufgabe / Lernziele

Klären Sie mit Hilfe des Tutors und mit Hilfe der anderen Studenten Ihrer Übungsgruppe Probleme und Fragen, die im Verlauf der Veranstaltung unklar geblieben sind!

Erklären Sie sich möglichst gegenseitig die Sachverhalte! Dies schult das Problembewusstsein und ermöglicht auch auf Seiten des Erklärenden oft ein vertieftes Verständnis.

Vorschlag zum Vorgehen (Zeitbedarf ca 45 Minuten)

1. Der Tutor gliedert den Stoff in 6 Themenblöcke zu je 2 Übungsblättern und bringt an 6 Stellen des Tutorraumes entsprechende Karten mit den Bezeichnungen der Themenblöcke an ("Stationen").
2. Die Teilnehmer bilden 6 Gruppen (wenn möglich).
3. Jede Gruppe verweilt 3 Minuten an jeder Station und wechselt dann an die nächste (im Uhrzeigersinn). Jede Gruppe beginnt an einer anderen Station.
4. Jede Gruppe sammelt ungeklärte Fragen zum jeweiligen Themenblock und klärt untereinander offene Fragen und Probleme zum jeweiligen Themenblock, soweit zeitlich möglich.
5. Nachdem jede Gruppe an jeder Station war, berichtet jede Gruppe nacheinander jeweils 2 Minuten (maximal) über die unklaren Punkte / offenen Fragen.
6. Die gesammelten unklaren Punkte / offenen Fragen werden anschliessend mit allen Teilnehmern und dem Tutor gemeinsam besprochen.