Kryptographie – Eine Einführung

Jan Tobias Mühlberg
<muehlber@fh-brandenburg.de>

Brandenburg, den 9. Dezember 2003

There's security that really makes us safer and security that only lets us feel safer, with no reality behind it.

— Bruce Schneier in „Beyond Fear“

Gliederung

1. Motivation
2. Die Ziele der Kryptographie
3. Kryptographische Verfahren
   - Symmetrische Verfahren
   - Asymmetrische Verfahren
   - Verschlüsseln und Signieren
   - Die Praxis: Hybride Verfahren
4. Zur Sicherheit kryptographischer Verfahren

Motivation – Problemstellung

- E-Mails werden heute meist ungeschützt über das Internet von Server zu Server geschickt.
- Sie werden dabei mehrfach zwischengespeichert und können von Administratoren oder Angreifern gelesen und manipuliert werden.
- Teilweise geltende gesetzliche Regelungen zwingen Dienstanbieter, die elektronische Korrespondenz ihrer Kunden über Monate zu archivieren.
- Weder Absender noch Adressat einer E-Mail wissen, wieviele Kopien ihrer Nachricht erstellt wurden, wo diese lagern und ob sie dort genügend geschützt sind.

Motivation – Lösungsansatz

- Einen auf den ersten Blick vielversprechenden Lösungsansatz bietet die Kryptographie:
  - Absender und Adressat tauschen ein Geheimnis, einen Schlüssel aus.
  - Der Absender verschlüsselt eine Nachricht mit diesem Schlüssel und sendet sie über das unsichere Internet.
  - Der Empfänger kann sie entschlüsseln und lesen.

Motivation – Warum es nicht so einfach ist!

- Was gewinnen wir tatsächlich dadurch?
- Kann ein Angreifer nicht einfach alle denkbaren Schlüssel durchprobieren?
- Wie sicher ist das alles? Oder: Ist Sicherheit meßbar?
- Wie kann man in einer unsicheren Welt ein so wichtiges Geheimnis wie den Schlüssel austauschen?

Die Ziele der Kryptographie

- Grundsätzlich werden mit kryptographischen Verfahren die folgenden Ziele verfolgt:
  - **Vertraulichkeit** – Eine Nachricht soll nur von den Adressaten, nicht von Dritten gelesen werden können.
  - **Authentizität** – Der Ursprung einer Nachricht soll zweifelsfrei nachgewiesen werden können, der Absender soll das Abschicken der Nachricht später nicht leugnen können.
  - **Integrität** – Die Nachricht soll den Empfänger nachweisbar korrekt und unmanipuliert erreichen.

Kryptographische Verfahren

- Verschlüsselungsverfahren transformieren einen allgemein lesbaren **Klartext** in einen, für nicht Eingeweihte unlesbaren **Geheimtext**.

- Da Computer intern alles, auch Text, als eine Folge von Zahlen darstellen, sind moderne kryptographische Verfahren nicht mehr als **Rechenvorschriften**.

- Die Verfahren benutzt für die Umwandlung von Klar- in Geheimtext und wieder zurück ein **Schlüssel**, der wiederum auch nur eine Menge von Zeichen ist.

Kryptographische Verfahren

- In Abhängigkeit davon, wie in einem Verfahren mit dem Schlüsselmaterial umgegangen wird, unterscheidet man zwischen
  - **symmetrischen** Verschlüsselungsverfahren und
  - **asymmetrischen** Verschlüsselungsverfahren.

Symmetrische Verfahren

- Symmetrische Verschlüsselungsverfahren verwenden zum Ver- wie auch zum Entschlüsseln einer Nachricht den gleichen Schlüssel.
- Dieser muß zwischen den Kommunikationspartnern vor dem Austausch der geschützten Nachricht ausgetauscht werden.
- Prinzipiell ist bei der Verwendung symmetrischer Kryptographie für jede Kommunikationsverbindung zwischen zwei Partnern ein eigener Schlüssel nötig.
- Bei nur 10 Kommunikationspartnern sind das bereits 45 Schlüssel, wenn jeder mit jedem vertrauliche Informationen austauschen möchte.

Symmetrische Verfahren – Caesar Chiffre

- Ein gutes Beispiel für ein sehr einfaches symmetrisches Verschlüsselungsverfahren ist die bereits ca. 2000 Jahre alte Caesar-Chiffre.
- Hierbei werden alle Buchstaben des verwendeten Alphabetes durch andere Buchstaben desselben ersetzt.
- Caesar ersetzte angeblich jeden Buchstaben des lateinischen Alphabetes durch den dritten, auf ihn folgenden Buchstaben.
- Man bezeichnet diese Art von Verschlüsselungsverfahren als „Rotationschiffren“.

Symmetrische Verfahren – Caesar Chiffre

- Klar- und Geheimtextalphabete für die Caesar-Chiffre:

Klartext:	a	b	c	d	e	f	g	h	i	j	k	l	m
Geheimtext:	D	E	F	G	H	I	J	K	L	M	N	O	P
Klartext:	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtext:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Ein Beispiel:

DQJULIILPPRUJHQJUDXHQ $\approx$ angriffimmorgengrauen

Symmetrische Verfahren

- Moderne symmetrische Chiffren funktionieren immernoch nach dem gleichen Prinzip.
- Es wird nicht mehr mit ganzen Buchstaben sondern mit einzelnen Bits gerechnet.
- Symmetrische Schlüssel haben heute eine Länge von bis zu 256 Bit, das macht $2^{256} =$<eine 79stellige Zahl> mögliche Schlüssel, was ein einfaches „Durchprobieren“ aussichtslos macht.
- Ungelöst bleibt das **Problem der Schlüsselverteilung.**

Asymmetrische Verfahren

- Asymmetrische Verschlüsselungsverfahren sind eine sehr junge Gruppe kryptographischer Verfahren, die erste Veröffentlichung hierzu gab es 1976. Seit etwa 20 Jahren werden sie praktisch eingesetzt.

- Jeder Teilnehmer besitzt ein Schlüsselpaar, einen **öffentlichen** und einen **privaten Schlüssel**.

Asymmetrische Verfahren

- Die beiden Teile des Schlüsselpaares sind derart miteinander verknüpft, daß Nachrichten, verschlüsselt mit dem öffentlichen Schlüssel nur mit dem privaten Schlüssel entschlüsselt werden können und umgekehrt.

- Der öffentliche Schlüssel eines Teilnehmers wird für alle zugänglich hinterlegt, wärend der private Schlüssel um jeden Preis geheimgehalten wird.

Asymmetrische Verfahren: Verschlüsseln

- Soll eine Nachricht für einen bestimmten Teilnehmer verschlüsselt werden, benutzt der Absender den öffentlichen Schlüssel des Adressaten.

- Die Nachricht kann damit nur vom Adressaten, der den zugehörigen privaten Schlüssel besitzt, gelesen werden. Auch der Absender eine keinen Enblick mehr in die von ihm gesendete Nachricht.

- Soll eine Nachricht von einer Gruppe von Personen lesbar sein, muß sie für jeden Teilnehmer explizit verschlüsselt werden.

Asymmetrische Verfahren: Signieren

- Elektronische Signaturen sollen, ebenso wie konventionelle Unterschriften die Authentizität und die Integrität einer Nachricht sicherstellen.

- Zum Erstellen einer elektronischen Signatur muß der Absender einer Nachricht diese lediglich mit seinem privaten Schlüssel verschlüsseln.

Asymmetrische Verfahren: Signieren

- Ein Empfänger kann die Nachricht dann mit dem zugehörigen und frei verfügbaren öffentlichen Schlüssel lesen.

- Vertraut der Empfänger darauf, daß der Sender seinen privaten Schlüssel niemals und niemandem aushändigen wird, wird er auch darauf vertrauen, daß die Nachricht authentisch und integer ist.

Die Praxis: Hybride Verfahren

- In der Praxis haben sich asymmetrische Chiffren zwar als *die* Lösung für das Problem der Schlüsselverteilung erwiesen, jedoch sind sie sehr rechenaufwendig.

- Hinzu kommt, daß sich beim Anschreiben mehrerer Adressaten die Nachricht massiv vergrößert, weil sie ja für jeden Empfänger getrennt verschlüsselt wird.

- Aus diesen Gründen ging man dazu über, symmetrische und asymmetrische Chiffren in hybriden Verfahren zu kombinieren.

Hybride Verfahren – Verschlüsseln

- Hybride Verfahren erzeugen zum verschlüsseln einer Nachricht zuerst einen zufälligen Schlüssel.
- Mittels eines symmetrischen Verfahrens und dieses Schlüssels wird die Nachricht verschlüsselt.
- Der Schlüssel wiederum wird nun für jeden Adressaten mittels eines asymmetrischen Verfahrens geschützt.

Hybride Verfahren – Signieren

- Zum Signieren wird zuerst mittels einer Einweg-Funktion eine „Prüfsumme“ über der Nachricht gebildet.
- Der Absender verschlüsselt nun lediglich diese Zahl mit seinem privaten Schlüssel und schickt das Ergebnis zusammen mit der Nachricht an die Adressaten.
- Diese können nun selbst die Prüfsumme über der empfangenen Nachricht errechnen und mit dem entschlüsselten Wert vergleichen.

Zur Sicherheit kryptographischer Verfahren

- Heute verwendeten kryptographische Verfahren sind nach aktuellem Stand der Erkentnisse nur sehr schwer zu brechen.

- Das Durchprobieren aller möglichen Schlüssel übersteigt selbst mit den schnellsten denkbaren Computern die Lebenserwartung unseres Universums – aber vielleicht können wir ja morgen schon weiterdenken.

Zur Sicherheit kryptographischer Verfahren

- Verfahren wie AES, Blowfish oder RSA wurden hundertfach analysiert, es wurden Schwachstellen gefunden, diese auszunutzen erfordert immernoch
  - einige Jahrtausende Rechenzeit – bis dahin ist das Geheimnis längst unwichtig oder
  - sehr viel, nach Möglichkeit auswählbaren Klar- und Geheimtext – besonders bei E-Mails ist das kritisch, weil viele Leute beispielsweise falsch zitieren

Zur Sicherheit kryptographischer Verfahren

- Leider gibt es noch einfachere Möglichkeiten, an Daten zu bekommen:
  - Die stärkste Kryptographie nutzt nichts, wenn Schlüssel bekannt werden oder ein einfach zu erratendes Passwort verwendet wird.
  - Daten, die auf Transportwegen durch tolle Kryptographie geschützt werden, auf Workstations und Datenträgern jedoch im Klartext auf Angreifer warten, wüssen auch nicht sein.

Zur Sicherheit kryptographischer Verfahren

- Kryptographie wird eingesetzt um Geheimnisse oder die eigene Privatsphäre zu schützen.

- Sie dient dazu, einem Angreifer das Herankommen an vertrauliche Daten zu erschweren. Sie wird es ihm nie völlig unmöglich machen.

- Wer bereit ist, gewisse Preise zu zahlen und Risiken auf sich zu nehmen, wird auch die stärkste Kryptographie umgehen können.