

FACHHOCHSCHULE WEDEL

SEMINARARBEIT

in der Fachrichtung

Wirtschaftsinformatik

Seminar über Mobile Computing

Thema Nr. 13:

Sicherheit in mobilen Netzen

Eingereicht von: Vaida Klimmek
Hohe Str. 4
25524 Itzehoe

Erarbeitet im: 4. Semester

Abgegeben am: 21. Dezember 2004

Referent FH Wedel: Dr. Sebastian Iwanowski
Fachhochschule Wedel
Feldstraße 143
22880 Wedel

Inhaltsverzeichnis

Inhaltsverzeichnis	II
Abbildungsverzeichnis.....	IV
Abkürzungsverzeichnis	V
1. Einleitung	1
1.1. Problemstellung.....	1
1.2. Vorgehensweise	1
2. Bedeutung der Sicherheit.....	2
3. Grundlagen der Kryptografie	4
3.1. Einführung in die Kryptografie.....	4
3.2. Symmetrische Verschlüsselung.....	6
3.2.1. DES	6
3.2.2. TDEA	7
3.2.3. AES	8
3.3. Public-Key-Verfahren	8
3.3.1. RSA.....	8
3.3.2. Der Diffie-Helman-Schlüsselaustausch	10
3.4. Hashfunktionen	11
3.5. Authentifizierung, Signierung und Zertifikate	12
4. Sicherheit in GSM-Netzen	15
4.1. Die Authentifizierung	16
4.2. Die Verschlüsselung	17
4.3. Sicherheit beim Roaming	18
4.4. Anonymität	18
4.5. Kritik am Sicherheitskonzept von GSM.....	18
5. Sicherheit in Wireless LANs.....	20
5.1. Die Authentifizierung	20
5.2. WEP	20
5.3. Kritik am WEP	22
6. Sicherheit in anderen mobilen Netzen	24
6.1. WAP	24

6.2. Bluetooth.....	27
6.3. Satellitensysteme	28
7. Fazit.....	30
Literaturverzeichnis	31

Abbildungsverzeichnis

Abbildung 1: Symmetrische Verschlüsselung.....	5
Abbildung 2: Asymmetrische Verschlüsselung.....	5
Abbildung 3: DES.....	6
Abbildung 4: TDEA.....	7
Abbildung 5: RSA	9
Abbildung 6: Diffie-Hellman-Schlüsselaustausch.....	10
Abbildung 7: Authentifizierung.....	12
Abbildung 8: Digitale Signatur.....	13
Abbildung 9: Authentifizierung in GSM-Netzen	16
Abbildung 10: Verschlüsselung in GSM-Netzen	17
Abbildung 11: Verschlüsselung in WEP	21
Abbildung 12: WAP	24

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AUC	Authentication Center
BSC	Base Station Controller
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DoS	Denial-of-Service-Angriff
GSM	Global System for Mobile Communications
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IMSI	International Mobile Subscriber Identity
IV	Initialisierungsvektor
Kap	Kapitel
LAI	Local Area Identity
LAN	Local Area Network
MAC	Message Authentication Code
PIN	Personal Identification Number
RAND	Random Number for Authentication
SIM	Subscriber Identification Module
SHA	Secure Hash Algorithm
TDEA	Triple Data Encryption Algorithm
TMSI	Temporary Mobile Subscriber Identity

VLR	Visitor Location Register
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WI	Wirtschaftsinformatik
WLAN	Wireless Local Area Network
WTLS	Wireless Transport Layer Security

1. Einleitung

1.1. Problemstellung

Es werden immer mehr verschiedene Kommunikationsgeräte eingesetzt, welche dem Mensch die Kommunikation einfacher und bequemer machen. Per Handy die aktuellste Information abfragen oder sogar einkaufen, mit dem tragbarem PC drahtlos online sein, oder die Daten ohne Speichermedien einfach per Signal übertragen usw. Viele Angebote, viele neue Techniken, die schnell verführen und nicht nur Privatpersonen, sondern auch Unternehmen zum Einsatz der neuen Techniken überzeugen. Damit vergißt man ganz schnell die Frage, was ist mit Sicherheit? Wird wirklich gewährleistet, dass die Informationen nicht von Fremden gelesen oder sogar manipuliert werden?

Im Rahmen der Seminararbeit versuche ich die neuen Techniken und Technologien, die in mobilen Netzen im Einsatz sind, bezüglich der Sicherheit auf den Prüfstand zu stellen. Der Schwerpunkt liegt in den GSM- und Wireless LAN-Netzen. Um das Verständnis zu erleichtern, lässt sich ein kurzer Exkurs in die Kryptografiegrundlagen nicht vermeiden.

1.2. Vorgehensweise

Da das Thema Sicherheit in mobilen Netzen ein sehr breites Thema ist, werden nur die wesentliche Aspekte und Techniken in ausgewählten mobilen Netzen vorgestellt. Nach der kurzen Erläuterung der Bedeutung der Sicherheit in mobilen Netzen Kapitel (Kap.) 2, werden die Grundlagen der Kryptografie im Kap. 3 erläutert. Im Kap. 4 wird ein tieferer Einblick in die Sicherheitskonzepte in GSM-Netzen gewährt. Mit der Sicherheit in Wireless LANs befasst sich das Kap. 5. Im Kap. 6 werden andere Mobile Netze kurz vorgestellt. Unter anderem Sicherheit in WAP-Technologie, Satellitensysteme und Bluetooth. Das Fazit wird in dem Kap. 7 gezogen.

2. Bedeutung der Sicherheit

Unter der Sicherheit in Kommunikationsnetzwerken versteht man die Erfüllung der Sicherheitsziele und Absicherung gegen typischen Gefährdungen, sowie Schutz der Privatsphäre. Man möchte als Nutzer sicher sein, dass die Informationen nicht manipuliert werden und den richtigen Kommunikationspartner erreichen, sowie, dass der Kommunikationspartner der Richtige ist. Bei der Übertragung der Information soll doch keiner mitbekommen, um was für eine Information es sich handelt.

Die Sicherheitsziele sind:

- Vertraulichkeit: Zugriff auf Information nur für gewünschte Kommunikationspartner.
- Authentifizierung: Feststellung und Zusicherung der Identität des Kommunikationspartners, sowie die Herkunft der Nachricht.
- Autorisierung: Den Zugriff auf Ressourcen für authentifizierte Benutzer beschränken oder verweigern.
- Integrität: Schutz vor Manipulation der Inhalte, Verdoppelung oder Löschen der Nachrichten bei der Übermittlung durch den Dritten.
- Nicht-Anfechtbarkeit: Sicherstellung, dass eine Nachricht von Sender versendet wurde und vom Empfänger empfangen wurde. Es entsteht ein Nachweis der Übertragung.
- Zugriffssteuerung: Zugriff von Außen auf das Netzwerk und dessen Komponenten nur für bestimmte Benutzerkreise.
- Verfügbarkeit: Sicherstellung, dass bei Bedarf das Netzwerk dem Benutzer zur Verfügung steht, sowie Schutz von Datenverlust.

Um die Sicherheitsziele genauer zu verstehen, folgendes Beispiel:

„Ein Bankkunde möchte eine Überweisung elektronisch über ein Mobiltelefon durchführen. Hierzu wird über das Telefon eine

Kommunikationsverbindung zur Bank aufgebaut. Als Erstes muss der Kunde sicher sein, dass der Kommunikationspartner wirklich seine Bank ist. Umgekehrt möchte die Bank sicher sein, dass es sich um den angegebenen Kunden handelt (Authentizität). Wird die Überweisung gesendet, muss gewährleistet werden, dass der Inhalt, z.B. der Geldbetrag, nicht bei der Übertragung verändert werden kann und dass die Überweisung nicht zweimal oder gar nicht bei der Bank eintrifft (Integrität). Schließlich sollte kein Dritter die Übertragung mithören können (Vertraulichkeit).

[...] Der Bankkunde muss sicher sein, dass die Bank später den Erhalt der Überweisung nicht leugnen kann (Nicht-Anfechtbarkeit). Personen, die nicht Kunden der Bank sind, sollten keinen Zugriff auf das Onlinebanking-System erhalten (Zugriffssteuerung). Letztlich sollte das System im vereinbarten zeitlichen Rahmen für Kunden zugreifbar sein (Verfügbarkeit).“¹

Die typischen Gefährdungen kann man in folgende Arten unterteilen:

- Menschliche Fehler, wie keine sichere Passwortaufbewahrung, Mitteilung von wichtigen Daten an Fremden usw.
- Programmen mit Schadfunktionen: Viren, Würmer, Trojaner.
- Spoofing: Angriff auf Authentifizierung durch vortäuschen falscher Identität.
- Denial-of-Service-Angriffe (DoS): Angriff auf Verfügbarkeit durch Einspielen von Nachrichten mit dem Ziel serverseitige Überlastung zu erzeugen.

¹ Roth, Jörg: Mobile Computing, 2002, S. 292f

3. Grundlagen der Kryptografie

3.1. Einführung in die Kryptografie

Die Begriffe Kryptologie und Kryptographie kommen aus dem Griechischen und bedeuten „geheim“, „das Wort“ und „schreiben“.

„Beide bezeichnen die Kunst und die Wissenschaft, die sich damit beschäftigt, Methoden zur Verheimlichung von Nachrichten zu entwickeln.“ Man unterscheidet „[...] zwischen **Kryptographie**, der Wissenschaft von der Entwicklung von Kryptosysteme, **Kryptoanalyse**, der Kunst diese zu brechen und [...] **Kryptologie** die Gesamtheit dieser Wissenschaften.“²

Die Sicherheitsziele wie Authentifizierung, Vertraulichkeit, Integrität und Verbindlichkeit werden mit Hilfe von kryptografischen Verfahren erreicht. Leider nicht absolut. Wichtigste Angriffsarten bei Verschlüsselung sind:

- Man-in-the-Middle-Angriff: Durch direkte Beteiligung an der Kommunikation die Information zu gewinnen und zu manipulieren.
- Brute-force-Angriff: Durch einfaches Ausprobieren den Schlüssel zu erraten und Information zu gewinnen.

Verschlüsselung ist der wesentliche Teil der Kryptographie. Der Inhalt von Informationen wird unleserlich gemacht, um über die unsicheren Kommunikationswege zu übertragen, wie z.B. Luftschicht und Vertraulichkeit zu ermöglichen. Der Klartext (Inhalt, was übertragen werden soll) wird mit Verschlüsselungsalgorithmus chiffriert (Chiffretext) und über einen unsicheren Kanal wie Internet übertragen. Empfänger dechiffriert den verschlüsselten Text mit dem Entschlüsselungsalgorithmus und kann den Klartext bearbeiten.

Im Bezug auf Schlüssel unterscheidet man zwischen der symmetrischen und asymmetrischen Verschlüsselung. Bei der symmetrischen Verschlüsselung (auch secret key Verfahren genannt) ist der Schlüssel zum Chiffrieren und Dechiffrieren

gleich. Der geheime Schlüssel soll für beide Seiten (Sender und Empfänger) bekannt sein, somit durch einen sicheren Kanal davor übermittelt worden sein.

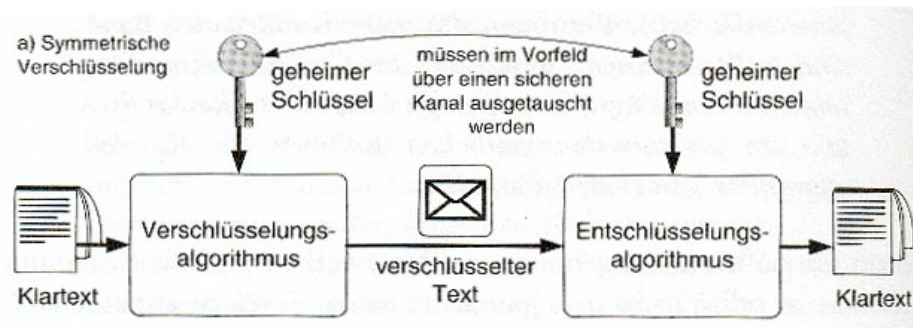


Abbildung 1: Symmetrische Verschlüsselung³

Bei dem asymmetrischen Verfahren (public key Verfahren) unterscheidet sich der Chiffrierschlüssel vom Dechiffrierschlüssel.

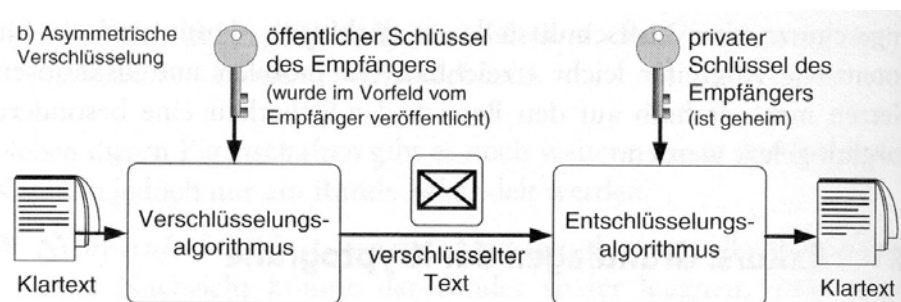


Abbildung 2: Asymmetrische Verschlüsselung⁴

Der Dechiffrierschlüssel ist geheim (privat) und ist nur dem Empfänger bekannt. Nur mit ihm kann die Nachricht entschlüsselt werden. Der Chiffrierschlüssel ist öffentlich (public) und kann über unsicheren Kanal übertragen werden. Zur Entschlüsselung vom Chiffriertext ist der Schlüssel nutzlos. Somit ist kein geheimer Austausch der Schlüssel notwendig, was als Hauptproblem beim symmetrischen Verfahren anzusehen ist. Man kann „spontan“ und mit neuen Teilnehmern ohne Probleme kommunizieren.

² Beutelspacher, Albrecht: Kryptologie, 1996, S. 10

³ Roth, Jörg: Mobile Computing, 2002, S. 294

⁴ Roth, Jörg: Mobile Computing, 2002, S. 294

Authentizität und Integrität wird durch Hashfunktionen sichergestellt. Hashfunktionen bilden lange Daten auf einen Wert fester Länge ab. Damit kann die Information aus dem Hashwert nicht mehr errechnet werden, die Daten nach der Bitkodierung sind nicht mehr intakt.

3.2. Symmetrische Verschlüsselung

3.2.1. DES

Symmetrische Verschlüsselungsverfahren werden häufiger eingesetzt als asymmetrische Verfahren und haben lange Tradition.⁵ Die bekannteste Chiffrierung ist der DES, Data Encryption Standard, wurde von IBM 1977 entwickelt und standardisiert. Es ist der erste Algorithmus, der von Anfang an publiziert wurde.⁶

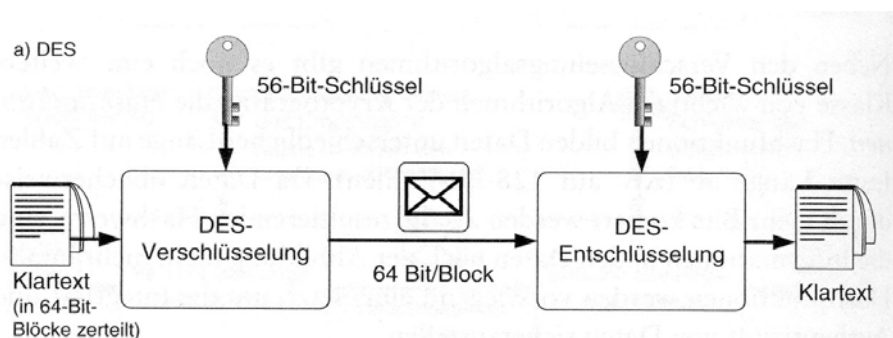


Abbildung 3: DES⁷

Es ist eine Blockchiffrierung (Klartext wird in Blöcke fester Länge unterteilt) mit 64 Bit Blocklänge und einem 56 Bit Schlüssel.

Kurze Beschreibung des Prinzips:

- Schlüssel und Klartext werden in Bitfolge übersetzt.
- Verfahren besteht aus 16 Runden. Bei jeder Runde rotiert der Schlüssel und der Klartext bzw. Zwischenergebnis bitweise. Zusätzlich werden die Teile des Zwischenergebnisses über S-Boxes (Ersetzungstabellen) transformiert.

⁵ Roth, Jörg: Mobile Computing, 2002, S. 295

⁶ Vgl. Beutelspacher, Albrecht: Kryptologie, 1996, S. 26

- Am Ende wird noch Schlusspermutation (Veränderung der Position der Zeichen) auf das Ergebnis angewandt.

Obwohl es $2^{56} \approx 7 \cdot 10^{16}$ verschiedene Schlüssel geben kann, ist die Sicherheit durch Brute-Force-Angriff eingeschränkt. „Unterstellt man einem Angreifer, dass genug Rechenleistung zur Verfügung steht, um 10^{12} Entschlüsselungen pro Sekunde durchzuführen, sind alle Schlüssel in weniger als einem Tag ausgetestet.“⁸ Aber man muss auch feststellen, ob dechiffrierter Klartext der richtige Klartext ist.

3.2.2. TDEA

1979 wurde Triple Data Encryption Algorithmus entwickelt, um die Brute-Force-Angriffe bei DES auszuschließen (wie bereits oben beschrieben, bei 10^{12} Entschlüsselungen pro Sekunde braucht man um die 10^{31} Jahre).

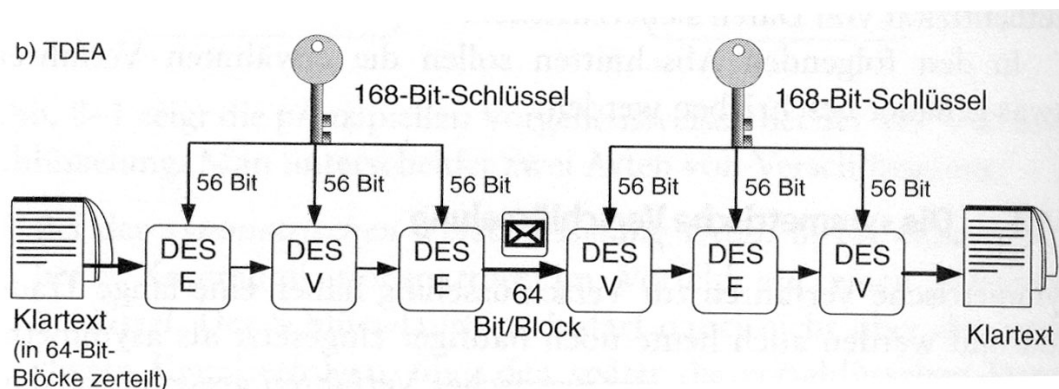


Abbildung 4: TDEA⁹

Kurze Beschreibung des Prinzips:

- Innerhalb des Algorithmus dreifache Anwendung des DES-Algorithmus zur Ver- und Entschlüsselung.
- Verläuft in drei Teilschritten: Ver-, Ent- und Verschlüsselung.
- Entsteht eine Schlüssellänge von 168 Bits.

⁷ Roth, Jörg: Mobile Computing, 2002, S. 296

⁸ Roth, Jörg: Mobile Computing, 2002, S. 297

- TDEA ist abwärtskompatibel zu DES.

3.2.3. AES

Unter Advanced Encryption Standard verbirgt sich ein Algorithmus Rijndael, der vom belgischen Wissenschaftler entwickelt worden ist. Er ist als Sieger aus einer Ausschreibung hervorgegangen, die im Jahr 2000 stattgefunden hat. Diese Ausschreibung, die seit Januar 1997 lief, sollten folgende Kriterien erfüllt werden: mindestens für die nächste 20 Jahre sicher sein, mindestens 128 Bit Schlüssel verwenden, einfach implementierbar in Hard- und Software und kostenfrei für alle nutzbar.

Kurze Beschreibung des Prinzips:

- Feste Transformation auf Klartext
- XOR-Verknüpfung (Exklusiv-Oder) des Ergebnisses mit dem Schlüssel
- 10 Runden aus Transformation und XOR-Verknüpfung

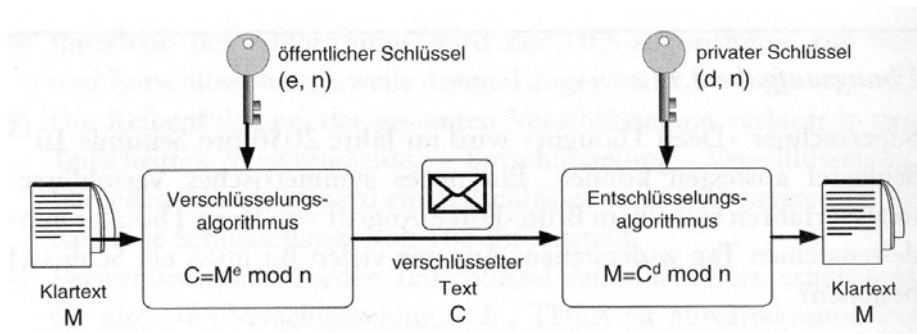
Rijndael ver- und entschlüsselt Blöcke der Länge 128, 160, 192, 224 und 256 Bit. Schlüssellänge von 128, 192 und 256 Bit möglich.

3.3. Public-Key-Verfahren

3.3.1. RSA

RSA ist eine asymmetrische Verschlüsselung, die 1978 entwickelt und nach den Erfindern Rivest, Shamir und Adleman benannt wurde.

⁹ Roth, Jörg: Mobile Computing, 2002, S. 296

Abbildung 5: RSA¹⁰

Kurze Beschreibung des Prinzips:

- Öffentlicher Schlüssel besteht aus (e, n)
- Privater Schlüssel besteht aus (d, n)
- M ist Klartext als ganze Zahl kodiert und liegt zwischen 0 und $n-1$
- C als chiffrierter Text als ganze Zahl
- Verschlüsselt durch $C = M^e \bmod n$
- Entschlüsselung durch $M = C^d \bmod n$
- Es muss gelten $M = C^d \bmod n = (M^e)^d \bmod n$
- $n = p \cdot q$ mit p und q als beliebige Primzahlen, wobei gilt $\Phi(n) = (p-1) \cdot (q-1)$
- Wähle d , so dass $d \cdot e \bmod \Phi(n) = 1$ ist
- e und n werden an Sender veröffentlicht

Der Brute-Force-Angriff kann bei der RSA-Verschlüsselung vermieden werden, wenn große Primzahlen p und q gewählt werden. Die Schlüssellänge von 1024 Bit gilt als sicher. Aber große Schlüssellängen bei Schlüsselgenerierung, Ver- und Entschlüsselung brauchen viel Rechenzeit, somit ist die asymmetrische

¹⁰ Roth, Jörg: Mobile Computing, 2002, S. 300

Verschlüsselung im Vergleich mit symmetrischem Verfahren langsamer. Meistens wird für Schlüsselverwaltung und Signaturen verwendet.

3.3.2. Der Diffie-Hellman-Schlüsselaustausch

Der im Jahre 1976 veröffentlichte Diffie-Hellman-Algorithmus war der erste Public-Key-Algorithmus, der veröffentlicht wurde. Er verbindet symmetrischer und asymmetrischer Algorithmen und nutzt die Vorteile von beiden Algorithmen aus. Asymmetrisches Verfahren wird nur zum Schlüsselaustausch benutzt und für Verschlüsselung selbst wird ein beliebiges symmetrisches Verfahren angewendet.

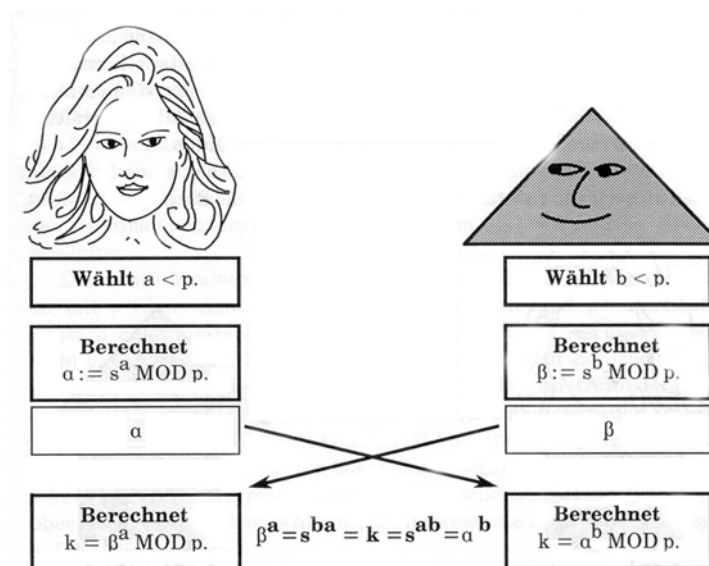


Abbildung 6: Diffie-Hellman-Schlüsselaustausch¹¹

Kurze Beschreibung des Prinzips:

- Beide Kommunikationspartner A und B sollen eine Primzahl p und eine natürliche Zahl $s < p$ vereinbaren. Sie können öffentlich sein.
- A und B wählen eine natürliche Zahl a bzw. b , wobei gilt $a, b < p - 1$. a und b sind geheim.

¹¹ Beutelspacher, Albrecht: Kryptologie, 1996, S. 139

- A berechnet $\alpha = s^a \bmod p$ und B berechnet $\beta = s^b \bmod p$. α und β werden verschickt.
- A bildet $k = \beta^a \bmod p$ und B berechnet $k = \alpha^b \bmod p$.
- Es gilt: $\alpha^b \bmod p = (s^a)^b \bmod p = s^{ab} \bmod p$
- Und es gilt: $\beta^a \bmod p = (s^b)^a \bmod p = s^{ba} \bmod p = s^{ab} \bmod p$
- Beide Teilnehmer erhalten denselben Wert $k = s^{ab} \bmod p$.

Vorteile gegenüber dem Angriff vom Dritten Person: es ist außerordentlich schwer von $\alpha = s^a$ auf a zu schließen, wobei α bekannt ist und bei genug großen Zahlen p und s ist es praktisch unmöglich auf k zu schließen.

3.4. Hashfunktionen

Wie bereits in Kapitel 3.1 erwähnt wurde, Hashfunktionen bilden beliebig lange Daten auf einen vorgegebenen kurzen Wert ab. Hashfunktionen müssen folgende Anforderungen erfüllen:

- Einfache Hashwertberechnung $h = H(x)$.
- Aus dem Hashwert h ist es praktisch unmöglich die ursprüngliche Nachricht zu berechnen.
- Es ist praktisch unmöglich aus mehreren Eingaben den gleichen Hashwert zu berechnen, für die gilt $H(x) = H(y)$, wo $x \neq y$

Die Hashfunktionen sind nicht umkehrbar, sodass es dem Dritten nicht möglich ist auf die eigentliche Information zu schließen.

Bekannteste Verfahren:

- SHA-1: Secure Hash Algorithm, entwickelt von der NSA, bildet Daten von 2^{64} Bit auf 160 Bit ab. Nachricht wird in 516 Bit-Blöcke unterteilt (falls nicht Teilbar, wird mit Füllbits auf notwendige Länge gebracht), auf jeden Block eine bestimmte Funktion angewandt und Zwischenergebnisse werden in weitere

Teilberechnung übernommen. Somit ist jedes Hashwertbit von dem Eingabebit abhängig.¹²

- MD5: von Rivest entwickelt, teilt die Nachricht in 512 Bit Blöcke auf und erzeugt einen Hashwert von 128 Bit Länge, was die Schwäche des Verfahrens darstellt.¹³

3.5. Authentifizierung, Signierung und Zertifikate

Asymmetrische Verfahren werden nicht nur zur Verschlüsselung, sondern auch zur Authentifizierung eingesetzt.

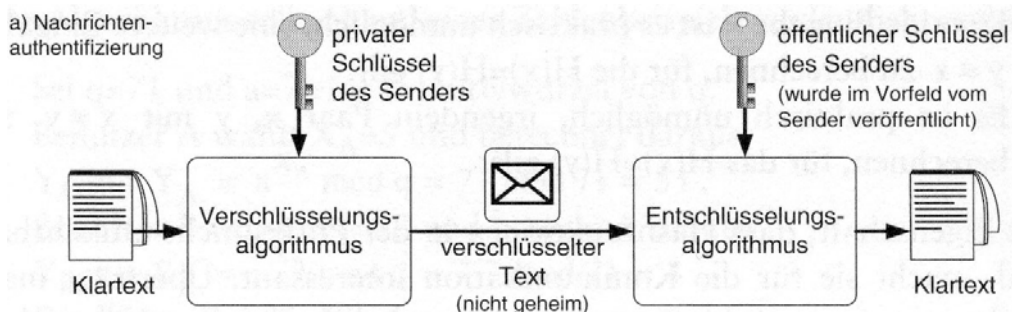


Abbildung 7: Authentifizierung¹⁴

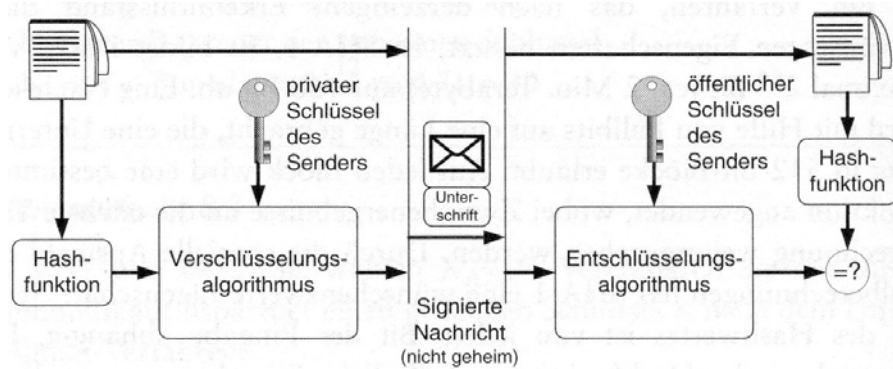
Der Klartext wird mit dem privaten Schlüssel des Absenders verschlüsselt. Der verschlüsselte Text kann von jedem mit dem öffentlichen Schlüssel des Senders entschlüsselt und gelesen werden. Diese Nachricht wird damit eindeutig einem bestimmten Absender zugeordnet.

Dieselbe Variante des Verfahrens wird auch für die digitale Unterschrift angewendet. Der Unterschied besteht darin, dass der Schlüssel nicht auf gesamte Nachricht, sondern nur auf dem Hashwert des Dokumentes angewendet wird.

¹² Vgl. Roth, Jörg: Mobile Computing, 2002, S. 305

¹³ Vgl. Roth, Jörg: Mobile Computing, 2002, S. 305

¹⁴ Roth, Jörg: Mobile Computing, 2002, S. 306

Abbildung 8: Digitale Signatur¹⁵

Der Sender berechnet den Hashwert seines Dokuments. Der Hashwert wird mit dem privaten Schlüssel des Senders chiffriert. Dieser verschlüsselte Hashwert wird als Message Authentication Code MAC, oder kryptografischer Fingerabdruck, oder kryptografische Prüfsumme genannt.¹⁶ Es wird die signierte Nachricht, die aus dem nicht verschlüsseltem Dokument und der chiffrierten Hashwert besteht, versendet. Der Empfänger entschlüsselt den Hashwert mit dem öffentlichen Schlüssel des Senders. Zusätzlich wird aus dem Dokument ein neuer Hashwert gebildet und beide Hashwerte werden mit einander verglichen. Wenn sie übereinstimmen, dann ist die Nachricht vom Sender. Wenn nicht, dann ist die Nachricht nicht vom Sender, oder sie wurde manipuliert.

Durch digitale Signatur werden die Authentizität und die Integrität der Nachricht gewährleistet. Die Kombination aus Signierung und Verschlüsselung stellt sicher, dass kein Dritter die Nachricht abhört, verändert oder sogar sich als an Stelle des Senders ausgibt.¹⁷

Natürlich muss der öffentliche Schlüssel eindeutig und jeder einzelnen Person zugeordnet werden. Das Problem wird durch die Zertifizierungsstelle, die vertrauenswürdig sein sollten und meistens Behörden oder große Organisationen sind, gelöst. Zertifikat enthält folgende Daten:

¹⁵ Roth, Jörg: Mobile Computing, 2002, S. 306

¹⁶ Vgl. Beutelspacher, Albrecht: Kryptologie, 1996, S. 83

¹⁷ Vg. Roth, Jörg: Mobile Computing, 2002, S. 307

- Identität der Person,
- Identität der Zertifizierungsstelle,
- Datumbereich der Gültigkeit,
- öffentlichen Schlüssel der Person und
- digitale Unterschrift der Zertifizierungsstelle (gewährleistet, dass der Inhalt des Zertifikats Nachhinein nicht geändert wurde und, dass der öffentliche Schlüssel der Person gehört).

Die Aufgaben der Zertifizierungsstellen und die Inhalte der Zertifikate werden im Signaturgesetz SigG geregelt, das im Jahr 2001 beschlossen wurde. Leider liegt noch keine Gleichsetzung zur gesetzlich vorgeschriebenen Schriftform vor.

4. Sicherheit in GSM-Netzen

Mit dem Sicherheitskonzept von GSM „[...]“ wurden folgende Sicherheitsziele verfolgt:

- Schutz vor nicht autorisiertem Telefonieren,
- Schutz vor dem Anhören einer Sprach- oder Datenverbindung,
- Schutz davor, den Aufenthaltsort eines Teilnehmers zu bestimmen.“¹⁸

Wichtige Bestandteile zur Erfüllung des Sicherheitskonzepts:

- Kryptografische Funktionen A3, A5 und A8.
- Schlüssel K_i , der zur Authentifikation verwendet wird.
- Schlüssel K_c , der zur Verschlüsselung verwendet wird.
- SIM-Karte, die den Schlüssel K_i , die Implementierungen der Funktionen A3 und A8 und International Mobile Subscriber Identity IMSI enthält.
- Das Mobiltelefon, das die Implementierung der Funktion A5 enthält.
- Datenbanken des Mobilfunkbetreibers, mit dem Authentication Center AUC, in dem die Liste aller IMSIs mit zugehörigen K_i feststeht.

Leider deckt das Sicherheitskonzept nur die Luftschnittstelle zwischen dem Mobiltelefon und der Basisstation ab. Wenn die Daten über die Luftschnittstelle im Netz des Betreibers weitergeleitet werden, liegen sie unverschlüsselt vor, weil sie bereits durch Base Station Controller (BSC) entschlüsselt wurden. Das Problem kann behoben werden, wenn der Betreiber eigenes Verschlüsselungsverfahren einsetzt.

¹⁸ Roth, Jörg: Mobile Computing, 2002, S. 319

4.1. Die Authentifizierung

Authentifizierung verläuft grundsätzlich in einer Richtung, wo der Netzbetreiber sicherstellen will, dass der Mobilfunkteilnehmer derjenige ist, für wen er sich ausgibt.

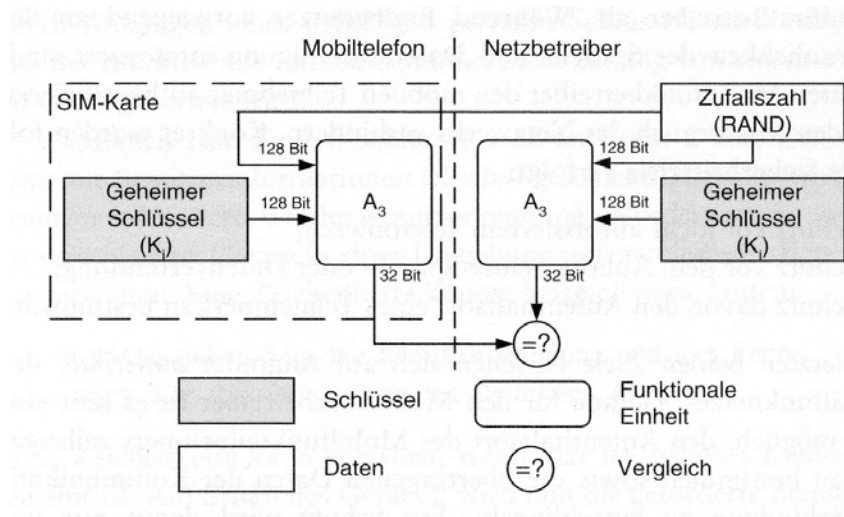


Abbildung 9: Authentifizierung in GSM-Netzen¹⁹

Kurze Beschreibung des Prinzips:

Die Zugangsberechtigungsprüfung verläuft in zwei Schritten. Im ersten Schritt muss der Nutzer einen 4-stelligen PIN eingeben und somit sich gegenüber der SIM-Karte auszuweisen. Bei drei Mal falscher PIN-Eingabe wird das Mobiltelefon gesperrt. Die Sperre kann nur mit dem 8-stelligen Super-PIN aufgehoben werden. Der zweite Schritt der Authentifizierung erfolgt nach Challenge-Response-Verfahren. Es wird geprüft, ob der Netzzugriff über eine berechtigte SIM-Karte erfolgt.²⁰ Bei Challenge-Response-Verfahren wird eine Zufallszahl von dem Netzbetreiber erzeugt und an den Teilnehmer gesendet. Dann erfragt der Netzbetreiber den geheimen Schlüssel K_i des Teilnehmers anhand des IMSI von dem AUC. Mit dem geheimen Schlüssel und der Zufallszahl wird Funktion A_3 angewendet. Das Ergebnis wird an den Betreiber

¹⁹ Roth, Jörg: Mobile Computing, 2002, S. 320

²⁰ Vgl. Lüders, Christian: Mobilfunksysteme, 2001, S. 140

übermittelt und verglichen. Wenn die Ergebnisse nicht identisch sind, wird der Zugriff auf das Mobilfunknetz nicht gewährt.

Bei dem Mobilfunkteilnehmer läuft die ganze Authentifizierungsberechnung auf der SIM-Karte, weil der geheime Schlüssel K_i auf der SIM-Karte gespeichert ist und die Funktion A_3 nur auf der Karte laufen kann. Nur das Ergebnis kann aus der SIM-Karte ausgelesen werden.

4.2. Die Verschlüsselung

Verschlüsselte Übertragung wird nur bei gelungener Authentifizierung eingerichtet.

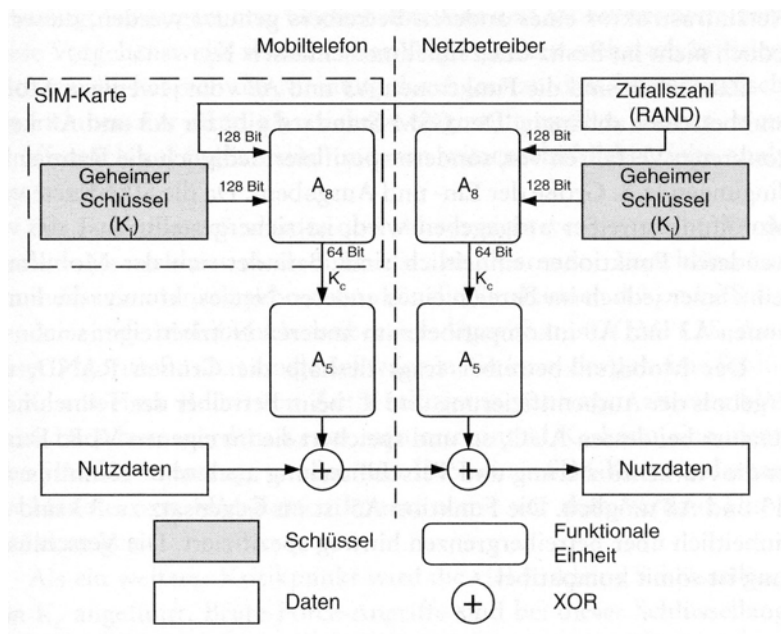


Abbildung 10: Verschlüsselung in GSM-Netzen²¹

Kurze Beschreibung des Prinzips:

Das Ablaufprinzip ist mit dem Authentifizierungsprinzip gleich, nur dass auf dem geheimen Schlüssel K_i und der Zufallszahl die Funktion A_8 ausgeführt wird, die auch auf der SIM-Karte implementiert ist. Der als Ergebnis erzeugte Schlüssel K_c wird mit der Funktion A_5 , die durch das Mobiltelefon abgearbeitet wird und Pseudo-Bits erzeugt, bearbeitet. Jeder Bit der Nutzdaten wird Exclusive-Oder mit jedem

Pseudo-Bit (Stromchiffre - ein Bit des Klartextes wird der Reihe nach mit einem Bit des Schlüssels verknüpft) verknüpft.

4.3. Sicherheit beim Roaming

Auch wenn der Mobilfunknetzteilnehmer durch Roaming-Abkommen den Netzbetreiber wechselt, kann die Authentizität und Verschlüsselung gewährleistet werden. Da die Funktionen A3 und A8 bei verschiedenen Betreibern nicht kompatibel sein können, wird das Problem damit gelöst, dass der Mobilfunkbetreiber die Zufallszahl RAND, das Ergebnis der Authentifizierung und Kc beim Betreiber des Teilnehmers (AUC) erfragt. Die Informationen werden in eigenem VLR (Visitors Location Register) gespeichert. Die Funktion A5 ist spezifiziert und somit ist die Verschlüsselung kompatibel.

4.4. Anonymität

Um die Bewegungsprofile, die leicht über das Abhören von IMSI feststellbar sind, zu unterbieten, werden die Temporary Mobile Subscriber Identity TMSI statt der IMSI benutzt. Nach der Authentifikation bekommt der Mobilfunkteilnehmer den TMSI, was zusammen mit der Location Area Identity LAI die eindeutige Zuordnung des Teilnehmers ermöglicht, zugeordnet. Die Zuordnung wird bei dem Betreiber gespeichert. Bei dem Wechsel in den Bereich eines neuen VLS, wird ein neues TMSI/LAI-Paar dem Teilnehmer zugeordnet.²²

4.5. Kritik am Sicherheitskonzept von GSM

Die Funktionen A3 und A8, die für Authentifikation und Verschlüsselung eingesetzt werden, wurden geheim gehalten, jedoch besitzen sie offene und standardisierte Schnittstellen. Im Jahr 1998 wurden sie in Internet veröffentlicht. Damit wurde bestätigt, dass die Algorithmen nicht besonders stark sind.²³ Einige Mobilfunkbetreiber verwenden für die Funktionen A3 und A8 den Algorithmus

²¹ Roth, Jörg: Mobile Computing, 2002, S. 320

²² Roth, Jörg: Mobile Computing, 2002, S. 322

²³ Vgl. Schiller, Jochen: Mobilkommunikation, 2003, S. 156

COMP128, der einige Schwäche hat. Nach einer Reihe von Authentifikationsanfragen an die SIM-Karte kann der K_i Schlüssel berechnet werden. Damit ist die Möglichkeit für die Erstellung der gleichen SIM-Karte geschaffen, weil die IMSI von der SIM-Karte gelesen werden kann.

Durch den Bruce-Force-Angriff kann der Schlüssel K_c erraten werden, weil er eine zu kleine Länge besitzt.

Bei der Authentifikation muss sich der Mobilfunkteilnehmer beim Mobilfunkbetreiber authentifizieren und nicht umgekehrt, was eine gute Voraussetzung für den Man-in-the-Middle-Angriff ausmacht. Die so genannten IMSI-Catcher, nutzen die Möglichkeit aus, um sich als Basisstation gegenüber dem Teilnehmer und als Mobilfunkteilnehmer gegenüber der Basisstation auszugeben. Um das Gespräch abzuhören, verlangt der IMSI-Catcher vom Mobiltelefon bei dem Aufbau der Verbindung die Verschlüsselung auszuschalten.²⁴

²⁴ Vgl. Roth, Jörg: Mobile Computing, 2002, S. 323

5. Sicherheit in Wireless LANs

Die Betreiber der drahtlosen Netze streben nach dem gleichen Sicherheitsniveau, das bei den drahtgebundenen Netzwerken besteht. Die Sicherheitsziele Authentizität und Verschlüsselung werden bei Wireless LAN nach IEEE 802.11 durch folgende Sicherheitskonzepte umgesetzt:

- Bei einem Access Point werden Zugriffslisten hinterlegt, die die Pakete vom Sender akzeptieren, die in der Liste hinterlegt sind.
- Ein gemeinsames Kennwort bei allen Access Points und Stationen. Eine Station kann jede Station authentifizieren.
- Alle Pakete werden mit einem gemeinsamen Kennwort durch die Stationen und Access Points verschlüsselt.²⁵

5.1. Die Authentifizierung

Die Authentifizierung in WLAN wurde sehr einfach gelöst. Jedes Access Point im Netz verfügt über die Zugriffsliste mit allen MAC-Adressen von zugelassenen Stationen. Wenn ein Paket von einer anderen Adresse empfangen wird, wird diese einfach verworfen.

Das Konzept ist einfach und gut zu realisieren, aber bekommt enormen Verwaltungsaufwand, wenn das Netz größer wird. Die MAC-Adresse kann auch bei modernen Karten geändert werden. Dies eröffnet dem Angreifer den Zugang in das Netz.

5.2. WEP

WEP bedeutet Wired Equivalent Privacy und ist verfügbar im Standard IEEE 802.11. Dieses Sicherheitskonzept dient zur Verschlüsselung und Authentifizierung. Das soll die o.g. Nachteile bei der Authentifizierung beheben.

²⁵ Vgl. Roth, Jörg: Mobile Computing, 2002, S. 324

Prinzip des WEPs:

- Jedem Teilnehmer im Netz wird ein geheimer Schlüssel, der durch einen sicheren Kanal übertragen werden muss, mitgeteilt (meistens durch den Systemadministrator).
- Jedes Paket wird mit dem geheimen Schlüssel symmetrisch verschlüsselt (Symmetrische Verschlüsselung: aus dem geheimen Schlüssel wird eine Pseudo-Bitfolge generiert und mit den Daten XOR verknüpft. Empfänger hat den gleichen geheimen Schlüssel und durch zweimal Anwenden des XOR erhält die ursprüngliche Daten).
- Die geheimen Schlüssel werden selten geändert. Zu der Verschlüsselung wird zusätzlich eine Bitfolge Initialisierungsvektor IV verwendet. Er wird bei jedem Paket verändert und als Klartext dem Paket beigelegt.

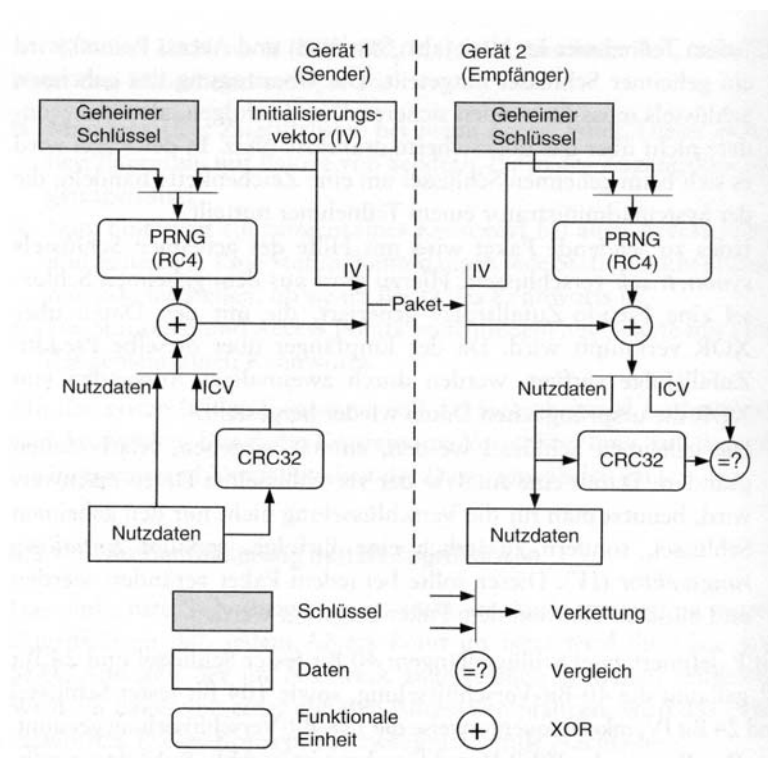


Abbildung 11: Verschlüsselung in WEP²⁶

²⁶ Roth, Jörg: Mobile Computing, 2002, S. 326

Kurze Beschreibung des WEP Verschlüsselungsprinzips:

Der geheime Schlüssel wird mit dem IV verkettet und durch den Pseudo-Zufallszahlgenerator Pseudo Random Number Generator PRNG in eine feste Zufallsbitfolge umgewandelt. Es wird das RC4 Verfahren verwendet, was sehr einfach und gut durch Einsatz von Hardware zu berechnen ist. Bevor aber die Daten verschlüsselt werden, wird ein Integrity Check Value ICV beigefügt, der für die Integrität der Daten sorgt. Die generierte Bitfolge wird mit den Nutzdaten mit Hilfe der Stromchiffrierung verschlüsselt und versendet. Der Empfänger entschlüsselt die Nachricht und bildet den neuen ICV. Der Wert wird mit dem übertragenen verglichen. Wenn die Werte ungleich sind, wird das Paket verworfen.

Die Authentifikation mit WEP wird folgendermaßen gelöst: es können nur diejenige die Prüfsumme gemäß Cyclic Redundancy Check CRC vor der Verschlüsselung berechnen, die das Kennwort besitzen. Zusätzlich bietet WEP eine explizite Authentifizierung des Kommunikationspartners. 128 Bit lange Zufallsfolge wird an den Teilnehmer unverschlüsselt versendet. Der Teilnehmer muss die Zufallsfolge mit WEP-Verschlüsselung verschlüsseln und zurücksenden. Ist der Wert nach der Entschlüsselung gleich dem versendeten Wert, so ist der Teilnehmer authentifiziert.

Mit WEP können zwei Schlüssellängen angewendet werden:

- 40-Bit-Verschlüsselung: 40 Bit fester Schlüssel und 24 Bit IV,
- 128-Bit-Verschlüsselung: 104 Bit fester Schlüssel und 24 Bit IV.

5.3. Kritik am WEP

Wireless LAN wird immer mehr verbreitet. Nicht nur in der privaten Wirtschaft, sondern auch an öffentlichen Stellen, wie Cafes, Flughafen und Hotels. Das bedeutet, dass die Teilnehmer sich nicht kennen und potentielle Angreifer in dem gleichen Netz sind. WEP bietet dabei keinen Schutz.

Durch einfaches Ausprobieren kann der 40-Bit Schlüssel erraten werden. Hier sollte nur der 104 Bit Schlüssel verwendet werden.

Initialisierungsvektor wird von einigen WLAN-Karten nicht oder zu selten geändert. Er ist aber der Hauptteil bei der Modifizierung der Pseudo-Zufallsfolge, weil der geheime Schlüssel nicht geändert wird.

Der Algorithmus RC4 hat einige Schwachstellen. „So erlauben es bestimmte schwache Schlüsselkombinationen, bei der Kenntnis nur weniger Schlüsselbits auf die gesamte Ausgabe zu schließen.“²⁷ Bei dem IV besteht der variable Anteil nur aus 24 Bits. Somit werden die IV wiederholt. Bei einer hohen Netzlast können Pakete abgefangen werden, die mit gleicher Zufallsfolge verschlüsselt wurde. Kennt der Angreifer einige Bits der ersten Nachricht, so kennt er automatisch die Folgebites und kann entsprechende Bits des zweiten Paketes entschlüsseln. Somit kann der Angreifer ein „Wörterbuch“ für alle IV Werte erstellen.

Access Point verschlüsselt die von außen kommenden Pakete und leitet sie drahtlos an den Empfänger. Der Lauscher kann damit den Access Point mit den Paketen versorgen und die verschlüsselten Pakete abfangen. Somit hat er den verschlüsselten Text und den Klartext.

Integrität mit CRC-Verfahren kann auch nicht gewährleistet werden. Ohne den kompletten Text der Nachricht zu kennen, kann der Angreifer einige Bits eines abgefangenen Pakets verändern und eine neue CRC-Summe berechnen.

WEP2 unterstützt die Schlüssel von 128 Bit. Aber es wird genau das gleiche RC4 Verfahren verwendet, das die o.g. Schwachstellen enthält.

²⁷ Roth, Jörg: Mobile Computing, 2002, S. 327

6. Sicherheit in anderen mobilen Netzen

6.1. WAP

Das Sicherheitskonzept von Wireless Application Protocol WAP ist in der Abbildung 12 dargestellt.

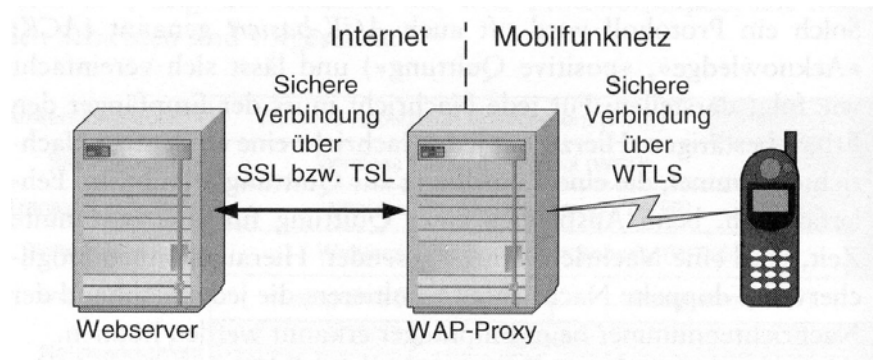


Abbildung 12: WAP²⁸

Die Verbindung zwischen dem Webserver und WAP-Proxy wird über die Protokolle des Internets gesichert. Die Luftverbindung zwischen dem WAP-Proxy und Mobiltelefon wird über das WTLS gesichert.

Spezielle Protokollschicht WTLS stammt aus Transport Layer Security TLS, die wiederum von dem Protokoll Secure Socket Layer SSL stammt. Sie wurde für drahtlose Netze optimiert.

WTLS²⁹ übernimmt folgende Aufgaben:

- Sicherung der Datenintegrität.
- Schutz gegen Mithören.
- Authentifikation.
- Schutz gegen Denial-of-Service-Angriffe.

²⁸ Roth, Jörg: Mobile Computing, 2002, S. 396

²⁹ Vgl. Roth, Jörg: Mobile Computing, 2002, S. 308ff

Anwendungen je nach Sicherheitsanforderungen können diese Funktionen ein- oder ausschalten.

Damit die Anwendungen sicher über das drahtlose Netzwerk kommunizieren können, vereinbaren die Teilnehmer einen Satz von kryptografischen Verfahren und die zugehörigen Schlüssel. Ist die Vereinbarung abgeschlossen, werden auf alle Nachrichten diese Verfahren angewendet, ein Abhören der Nachrichten ist nicht mehr möglich und Veränderungen können aufgedeckt werden. Verletzungen werden nach oben gemeldet.

Folgendes Sicherheitskonzept ist entwickelt worden:

- Asymmetrisches Verschlüsselungsverfahren zur Vereinbarung des gemeinsamen Schlüssels.
- Symmetrische Verschlüsselung für Anwendungsnachrichten.
- Hashfunktionen zur Authentifizierung.

Die symmetrische Verschlüsselung wurde deshalb gewählt, weil asymmetrische Verschlüsselung viel Rechenzeit kostet. Für die symmetrische Verschlüsselungen und Hashfunktionen liegen Implementierungen vor, die selbst auf kleinen Geräten effizient laufen.

Damit die Kommunikationspartner sichere Verbindung aufbauen können, hält jeder einen Sitzungszustand, der folgende Daten enthält:

- Sitzungserkennung
- Zertifikat des Kommunikationspartners
- gemeinsame Komprimierungsmethode
- symmetrischer Verschlüsselungsalgorithmus
- Hashfunktion für authentifizierte Nachrichten
- Master Secret (gemeinsames Geheimnis) für Schlüsselbildung

Um diesen Zustand auf beiden Seiten einzurichten und zu verwalten, verfügt WTLS über drei Protokolle:

- Handshake-Protokoll
- Change-Cipher-Protokoll
- Alert-Protokoll

Das Handshake-Protokoll dient zur Einrichtung der sicheren Verbindung und der Vereinbarung der Verfahren sowie des Schlüssels zwischen dem Client und Server.

Es wird vereinbart:

- Schlüsselaustauschverfahren. Mögliche Verfahren sind RSA und Diffie-Hellmann.
- symmetrisches Verschlüsselungsverfahren. Mögliche Verfahren sind DES, TDES und RC5.
- Hashfunktionen. Mögliche Verfahren sind MD5 und SHA-1.
- Eine Liste von unterstützten Komprimierungsverfahren
- Festlegung der Häufigkeit von neuen Vereinbarungen für kryptografische Informationen

Das Change-Cipher-Protokoll definiert die Vereinbarungen als gültig und besteht nur aus einer Nachricht. Diese Nachricht wird innerhalb des Handshake-Protokolls versendet, aber nach WTLS-Spezifikation gehört sie nicht zum Handshake-Protokoll.

Wenn während der Sitzung sicherheitsrelevante Fehler auftreten, werden sie dem Kommunikationspartner mit dem Alert-Protokoll mitgeteilt. Bei schwerwiegender Sicherheitsverletzung wird die Verbindung nach dem die Alert-Nachricht gesendet wurde, beendet. Alert-Nachrichten werden bei ungültigem Zertifikat oder bei Veränderung der Nachricht während des Transports verschickt.

Da die Datagramme auf Transportebene benutzt werden, die sehr schnell vom Dritten in eine existierende Verbindung eingeschleust werden können, ist man dem Denial-of-Service-Angriff ausgeliefert. WTLS bietet einen Schutz gegen solche Angriffe. Nach dem Aufbau der sicheren Verbindung können die fremden Nachrichten mit Hilfe von zusätzlichen Informationen, wie Nachrichtennummern leicht erkannt und verworfen werden. Damit soll aber die existierende Verbindung nicht beeinträchtigt werden. Problematisch sind die Angriffe, die auf Handshake-Nachrichten sind. Hello-Nachrichten sind nicht verschlüsselt, somit können nicht sofort als fremde Nachricht identifiziert werden. Als Lösung wurde festgelegt, dass die Änderungen von kryptografischen Parametern erst nach Finish-Nachricht erlaubt sind. Kommen aber die Aufforderungen zum Schlüsselabgleich sehr oft, ist man nur mit der Behandlung des Protokolls beschäftigt, obwohl der Abgleich später als fehlerhaft erkannt wird. Client ist besonders anfällig, weil er nur über geringe Rechenkapazität verfügt. Deswegen kann der Client Schlüsselabgleichsanfragen ignorieren, wenn sie zu häufig auftreten.

6.2. Bluetooth³⁰

Das Sicherheitskonzept von Bluetooth basiert auf Authentifikation und Verschlüsselung. Die Authentifikation, mit der die Zugangsberechtigungsprüfung erfolgt, basiert auf den Cahlange-Response-Verfahren. Leider wurden keine Anforderungen für den Zufallszahlgenerator gestellt. Somit können die Zufallszahlgeneratoren mit den vorhersehbaren Zufallszahlen die Verschlüsselung und Authentifizierung schwächen.

PINs von Bluetooth-Geräten sind meistens nur 4-stellige Nummern. Sie sind kurz und können durch einfaches Ausprobieren erraten werden. Einige Geräte haben keine Möglichkeit die PIN zu ändern oder einzugeben, was das Problem ausmacht, weil die meisten PINs von Geräten von den Herstellern mit Nullen belegt sind. Auch die Frequenz der Benutzung der PINs macht das Sicherheitskonzept fragwürdig. Die PINs werden nur einmal beim Pairing von Geräten benutzt.

³⁰ Vgl. Roth, Jörg: Mobile Computing, 2002, S. 328ff

Anonymität wird mit Hilfe vom Non Discoverable Mode Zustand gewährleistet. Wenn das Gerät auf diesem Status ist, reagiert es nicht auf Suchanfragen, ist aber auch nicht mehr erreichbar. Andersfalls kann das Bewegungsprofil leicht erstellt werden.

6.3. Satellitensysteme

„Forschern der Ruhr-Universität Bochum ist es bei der Untersuchung der Satelliten-Internet-Zugänge (DSL über Satellit) der Telekom[1], Megasys und Netsystems gelungen, umfangreiche Informationen über einzelne Personen zu ermitteln. So konnten sie in einem Zeitraum von 24 Stunden in den Datenströmen eines Astra-Transponders Name, Adresse, Geburtsdatum, Einkommen und EC-Kartenummer eines Opfers mitlesen. Auch war es möglich, die E-Mail-Kommunikationen zwischen kommerziellen Nutzern abzuhören. Dazu benutzten sie nur einen handelsüblichen PC, eine DVB-S-Karte und eine Satellitenschüssel.“³¹

Die Zeitschrift c't (in Ausgabe 24/03) hat auf die grundsätzlichen Sicherheitsmängel bei der Nutzung des Internet über Satellitenverbindungen hingewiesen. Jeder Satellitennutzer kann dort prinzipiell die Daten aller anderen mitlesen, sofern diese nicht die Sicherheitsfunktionen aktiviert haben. Satellitengestützte Internetzugänge arbeiten meist asymmetrisch: die Anfrage eines Clients geht über die Telefon- oder ISDN-Leitung, die Antwort eines Servers kommt in der Regel über Satellit zurück. Die Anbieter stellen die Sicherheitsmechanismen bereit. Dazu muss aber der in der Betriebssoftware mitgelieferte Proxy aktiviert sein. Dieser so genannte Performance Enhancement Proxy (PEP) dient eigentlich der Verbesserung des Datendurchsatzes. Zusätzlich verschlüsselt er den Verkehr. Einige Anwender scheinen diese Funktion aber wieder zu deaktivieren. Ein Grund dafür ist, dass auf IPSec-basierende VPN-Software mit PEP nicht richtig funktioniert.

Bereits früher haben die Nachrichten über die Satelliten die Welt erschüttert. Von Nachrichtenagentur Reuters im Jahr 1999 veröffentlichte Nachricht „**LONDON** –

³¹ Heise Zeitschrift Verlag: Forscher spähnen Satelliten-Internet-Zugänge aus, 2004

Hackers have reportedly seized control of one of Britain's military communication satellites and issued blackmail threats.”³² hat für Aufsehen gesorgt. Dabei haben, laut Reuters, "Hacker" die Flugbahn des Satelliten manipuliert und anschließend in einem Erpresserschreiben Geld gefordert, wenn sie mit der Manipulation des Satelliten aufhören sollen. Um eine solche Manipulation durchzuführen, benötigt man außer Fachwissen ein Ausrüstungsbudget von unter 10000 DM. Ausgemusterte professionelle Ausrüstung ist mitunter sehr preiswert zu erhalten.

GPS Systeme wurden von Angreifern nicht verschont. Es wurde ein Störgerät entwickelt (militärischer Fachbegriff: Jammer), das in einem definierten Bereich beim GPS-Empfänger keine zuverlässige Daten zur Navigation liefert. „[...] Ein solches Gerät wurde auf der Moscow Air Show 98 von einem Russen erstmals der Öffentlichkeit vorgestellt und versetzte die dort anwesenden Militärs vieler Länder in hektische Aufregung.”³³ Das tragbare Gerät in der Größe einer Damenhandtasche kann den Empfang von GPS-Signalen (und dem russischen Pendant GLONASS) in größerem Umkreis unterbinden. Die genaue Leistungsfähigkeit und der Preis des Geräts sind nicht bekannt, der Erfinder stellte aber klar, dass das Gerät für jeden käuflich zu erwerben sei.

³² Fuchs, Howard: Sicherheit bei Sattelitenkommunikation, 1999

³³ Fuchs, Howard: Sicherheit bei Sattelitenkommunikation, 1999

7. Fazit

Sicherheit bei drahtlosen Netzen hinkt der Sicherheit bei den drahtgebundenen Netzen noch meilenweit hinterher. Wie die Untersuchungen ergeben, haben die meisten Betreiber von WLANs offensichtlich keinen blassen Schimmer davon, was sie tun, und wie leicht es ist, den Datenschutz von WLANs aufzuheben. So hat die Wirtschaftsprüfungsgesellschaft Ernst & Young festgestellt, dass bei 80% der stichprobenartig in Wien gefundenen 200 WLANs noch nicht einmal die einfache WEP-Verschlüsselung aktiviert war.³⁴

Wie wir gesehen haben, werden die Anforderungen der Sicherheitsmechanismen nicht erfüllt. Man muss genau davor überlegen für welche Daten welche Verbindung gewählt wird. Bei besonders sensitiven Daten ist Beachtung der Sicherheit unumgänglich.

Das bedeutet aber nicht, dass man auf Mobilkommunikation verzichten muss. Mit geeigneten zusätzlichen Absicherungsmaßnahmen, wie z.B. Firewall bei WLAN können die mobilen Netze bequem benutzt werden.

Satellitensysteme sind genauso störanfällig und unsicher. Und es ist besonders gefährlich, weil sie immer mehr für kommerzielle Zwecke eingesetzt werden, wie z.B. Satelliten-Internet-Zugänge.

Trotz der bestehenden Sicherheitsmängel wird das mobile Computing sich Beweisen und zukünftig eine große Rolle in alltäglichen Leben spielen.

³⁴ Vgl. Kauffels, Franz-Joachim: Wireless LANs, 2002, S. 329

Literaturverzeichnis

Literaturverzeichnis

Beutelspacher, Albrecht, 1996: [Kryptologie], Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 5., leicht verbesserte Auflage, Braunschweig, Vieweg, 1996

Kauffels, Franz-Joachim, 2002: [Wireless LANs], 1. Auflage, Bonn, mitp-Verlag, 2002

Roth, Jörg, 2002: [Mobile Computing], Grundlagen, Technik, Konzepte, 1. Auflage, Heidelberg, dpunkt.verlag, 2002

Schiller, Jochen, 2003: [Mobilkommunikation], 2., überarbeitete Auflage, München, Pearson Studium, 2003

Quellen im Internet

Fuchs, Howard: [Sicherheit bei Sattelitenkommunikation], 1999, Internet http://www.fuhs.de/de/fachartikel/artikel_de/sathack99.shtml, Abruf 2004-11-26

Heise Zeitschrift Verlag: [Forscher spähen Satelliten-Internet-Zugänge aus], 2004, Internet <http://www.heise.de/newsticker/meldung/53676>, Abruf 2004-11-26