Sicherheit in mobiler Kommunikation

Sabine Keuser

ETH Zürich

Seminar “Mobile Computing”

Professor: F. Mattern

Betreuerin: M. Moschgath

1 Sicherheitsprobleme mobiler Netze

In verkabelten Netzen bieten die Kabel, welche die Geräte miteinander verbinden einen gewissen physischen Schutz gegen Manipulationen: Die Kabel selbst befinden sich normalerweise innerhalb eines Gebäudes, welches durch gewisse Zugangskontrollen geschützt ist. Dort ist das Kabel innerhalb der Räume, wo sich die Geräte befinden, frei zugänglich. Um die Kabel selbst zu erreichen muss ein Angreifer also in das Gebäude und den entsprechenden Raum einbrechen, und um an die Daten zu gelangen, muss er das Kabel anzapfen, ohne dass dies für den Benutzer sichtbar ist.

In mobilen, kabellosen Netzen werden die Daten nun nicht mehr über Kabel, sondern offen über die Luft übertragen und sind somit in einem gewissen räumlichen Umkreis einfach zu empfangen. Es kann sogar sein, dass die Übertragungen ausserhalb des Gebäudes empfangbar sind. Die Datenübertragung ist sehr viel leichter zugänglich, als bei einem verkabelten Netz. Dieser Umstand erfordern den Einsatz von Authentisierung und Verschlüsselung.

Bei Adhoc-Netzwerken besteht zusätzlich die Herausforderung, dass sich die Teilnehmer beim Aufbau des Netzwerkes noch nicht "kennen", es also ist nicht möglich auf gemeinsamen Informationen beispielsweise eine geheimer Schlüssel, aufzubauen. Möglicherweise realisieren sie auch verschiedene Sicherheitsstandards.

Eine Attacke, die speziell auf mobile Netzwerke zielt, ist die location attack. Das Ziel dieses Angriffs ist es, den Standort eines Geräts zu bestimmen und damit Aussagen über den Standort einer Person zu machen. Des weiteren kann diese Person auch in Beziehung zu anderen Geräten und somit Personen gebracht werden. Diese Attacke ist besonders problematisch, da eine Person rund um die Uhr, auch im privaten Bereich, ohne grossen (finanziellen) Aufwand überwacht und der Standort mit hoher Genauigkeit bestimmt werden kann. Diese Informationen könnten für vielerlei Angriffe verwendet werden: Erpressung, Kontrolle des Lebenspartners, Aufbauen eines Profils einer bestimmten Person etc. Auf jeden Fall bedeutet eine unerwünschte Überwachung für das Opfer einen Verlust der Privatsphäre.

Als Vertreter für mobile Netze werden in den folgenden Kapiteln Bluetooth und Wireless LAN (IEEE 802.11) genauer betrachtet.

2 Sicherheit bei Bluetooth

2.1 Eigenschaften

Bluetooth bietet gegenseitige und einseitige Authentisierung sowie Verschlüsselung auf Basis eines gemeinsamen geheimen Schlüssels dem sogenannten link key. Zur Verschlüsselung wird für jede Session aus dem link key ein neuer Schlüssel, der encryption key, generiert. Das Schlüsselmanagement ist Teil des Standards und wird in der Initialisierungsphase realisiert.

Verschlüsselung und Authentisierung sind optional, jedoch ist die Authentisierung Voraussetzung für die Verschlüsselung.

2.2 Initialisierung

Begegnen sich zwei Geräte zum erstenmal, müssen sie zunächst einen gemeinsamen Schlüssel vereinbaren, falls eine verschlüsselte Übertragung gewünscht ist:

Als erstes wird ein init key generiert. Dieser wird von beiden Geräten mittels der Funktion f aus einem geheimen PIN, der Device Adresse des Geräts und einer Zufallzahl berechnet und anschliessend überprüft (siehe Abb. 1 und Abb. 2). Der PIN ist eine Zahl, die in beide Geräte „out of band“ (z B. über Tastaturen) eingegeben wird und zwischen 8 und 128 Bits lang sein muss. Wird kein PIN gewählt, wird der default PIN 0 verwendet. Die Zufallszahl wird unverschlüsselt über die Luft übertragen, die Device Address ist durch vorangehende, unverschlüsselte Kommunikation bekannt.

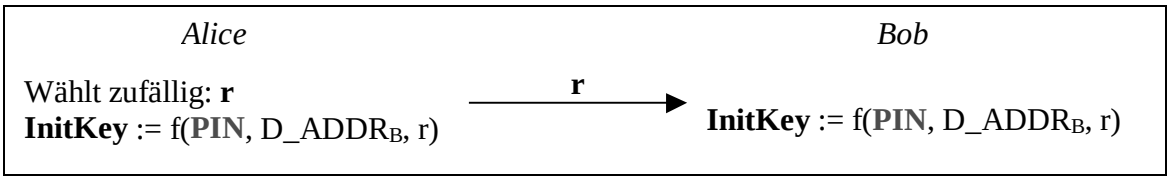

Abbildung 1: Generierung des init keys

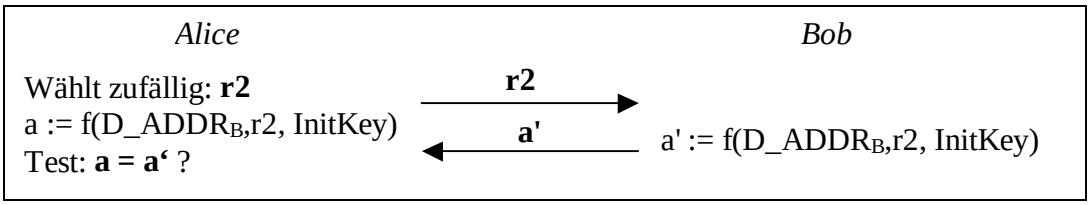

Abbildung 2: Überprüfung des init keys

Als nächster Schritt wird der link key generiert, wobei die Kommunikation zu diesem Zeitpunkt durch den init key verschlüsselt ist. Der link key wird permanent gespeichert und dient zur späteren Authentisierung der Geräte und als Grundlage zur Verschlüsselung.

2.2.1 Authentisierung

Zwei Geräte die eine Kommunikation wieder aufnehmen wollen, müssen sich zunächst authentisieren, falls die entsprechende Option gewählt wurde. Dabei wird geprüft, ob beide Geräte den gleichen link key verwenden, der bei der ersten Kommunikation generiert wurde. Die Überprüfung erfolgt analog zur Überprüfung des init keys (siehe Abb. 2).

2.2.2 Verschlüsselung

Der Encryption Key wird bei jeder Session, durch die bei der Authentisierung verwendete Funktion, als Nebeneffekt neu generiert und ist somit abhängig vom link key. Die Verschlüsselung erfolgt über eine Stream Cipher.

2.3 Attacken

2.3.1 „Hopping Along“

Oft wird die pseudozufällige hopping sequence, nach der Geräte auf bestimmten Frequenzen senden bzw. empfangen, als Sicherheitsmassnahme bezeichnet, da ein Angreifer nicht voraussagen kann, nach welchem Muster gesendet wird, und somit nicht in der Lage sein soll, die Kommunikation zu belauschen. Allerdings ist es technisch nicht sehr schwierig die 24 – 79 parallelen Kanäle zu überwachen. Zudem ist die Seed des Pseudozufallszahlengenerators einfach in Erfahrung zu bringen, da sie aus der device address und der clock des Masters besteht. Beide Informationen sind nicht geheim und werden in der Initialisierungsphase offen übertragen.

2.3.2 Brechen des geheimen Schlüssels

Wenn der PIN zu kurz oder schwach ist, kann der link key durch eine brute force-Attacke erraten werden.

Dazu belauscht der Angreifer die Initialisierungsphase und erfährt dabei die verwendete Zufallszahl zur Generierung des init keys und die Daten, die zur Verifikation des init keys übertragen werden. Er wählt einen Wert für den PIN, führt selbst offline die Schritte zur Initialisierung und Verifizierung durch und vergleicht den berechneten Funktionswert mit den belauschten Daten. Stimmt die eigene Verifikation mit der Belauschten überein, hat der Angreifer mit sehr hoher Wahrscheinlichkeit den richtigen PIN gewählt. Da alle weiteren Schlüssel auf dem geheimen PIN basieren, kann ein Angreifer nun alle weiteren Kommunikationen entschlüsseln und selbst Nachrichten einspeisen.

In einer Variante dieser Attacke initiiert der Angreifer selbst die Kommunikation. Sobald das Opfer auf die Challenge geantwortet hat, kann der Angreifer wie oben beschrieben vorgehen.

2.3.3 „Location Attack"

Da Bluetooth Geräte auf inqueries mit ihrer device address antworten, kann ein Angreifer den Standort eines Gerätes bestimmen, falls es auf eine inquery antwortet. Dazu kann der Angreifer gezielt an interessanten Orten Bluetooth Geräte verteilen, die inqueries senden und die device addresses der antwortenden Geräte aufzeichnen. Diese Attacke funktioniert allerdings nur, wenn das Gerät des Opfers im discoverable mode ist und somit auf inqueries antwortet.

Eine Variante wäre, einen Virus in das Gerät des Opfers einzuschleusen, so dass dieses in den entsprechenden Modus wechselt, oder selbst Inqueries sendet.

3 Sicherheit bei IEEE 802.11

3.1 Eigenschaften

Der IEEE 802.11 Standard beschreibt Authentisierung des mobilen Gerätes gegenüber dem access point und Verschlüsselung. Beides basiert auf einem geheimen Schlüssel, der vom access point und dem mobilen Gerät geteilt wird. Das Schlüsselmanagement ist nicht Teil des Standards. In der Praxis gibt es momentan sogar nur einen geheimen Schlüssel für ein ganzes Netzwerk.

Der Verschlüsselungsalgorithmus von IEEE 802.11 heisst WEP (Wired Equivalent Privacy) und soll – so der Name - für mobile Netzwerke einen Sicherheitsstandard äquivalent zu dem verkabelter Netze garantieren. Authentisierung und Verschlüsselung sind optional, wobei die Authentisierung auf dem WEP Algorithmus basiert.

3.1.1 Verschlüsselung

Die Verschlüsselung erfolgt mit einer stream cipher wie in Abb.3 illustriert.
Aus dem geheimen Schlüssel und dem initialization vector, die zusammen als seed in einen Pseudozufallsgenerator gespeist werden, wird ein Schlüsselstrom generiert, der zur Verschlüsselung eines Pakets verwendet wird (siehe Abb. 3).
An jede Nachricht wird eine Checksumme angehängt um zu verhindern, dass die Nachricht unbemerkt modifiziert werden kann. Verschlüsselt wird die Nachricht inklusive

Checksumme. Der initialization vector, welcher keinen Hinweis über den geheimen Schlüssel enthält, wird als Klartext übertragen (siehe Abb. 3).

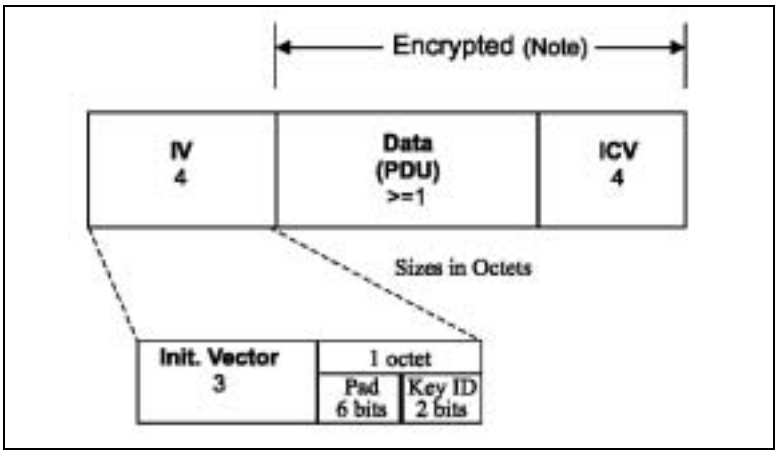

Abbildung 3: WEP Frame Body

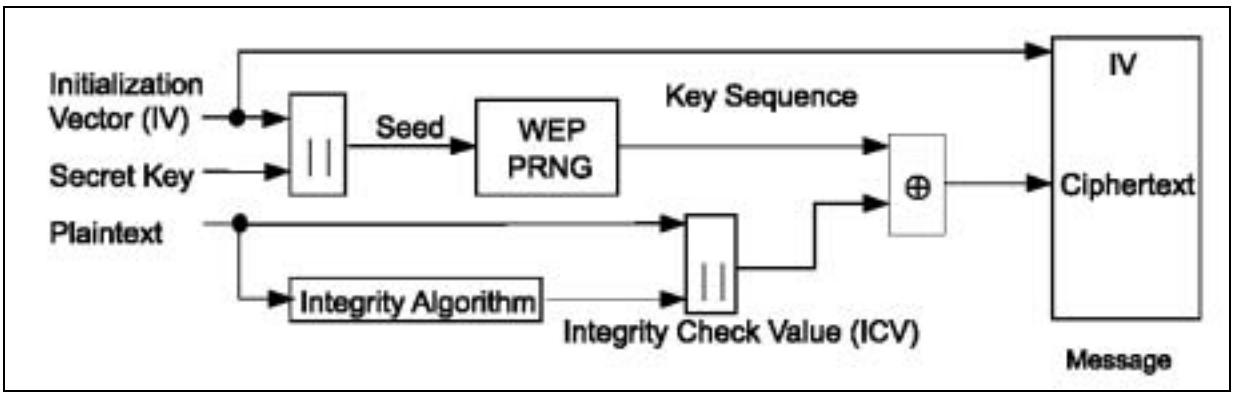

Abbildung 4: WEP encipherment block diagram

3.1.2 Authentisierung

Zur Authentisierung muss das mobile Gerät eine Challenge des acces points mit dem WEP Algorithmus korrekt verschlüsseln.

3.2 Attacken

3.2.1 Schwachstellen

Der initialization vector ist ein 24 Bit Feld. Wenn der access point konstant 1500 Byte-Pakete bei 11Mbps sendet, wiederholt sich der initialization Vector nach ca. 5 Stunden:

1500*8/(11*10^6)*2^24 =~ 18000 Sekunden = 5 Stunden

Im Laufe der Zeit werden also immer mehr Pakete mit dem gleichen Schlüsselstrom verschlüsselt.

Die Stream Cipher (RC4) besitzt folgende Eigenschaft:
Werden 2 Pakete mit dem gleichen initialization vector und gleichem geheimen Schlüssel verschlüsselt, dann ist das XOR ihrer Klartexte gleich dem XOR ihrer Chiffrate.
Ist einmal ein Klartext-Chiffrat Paar bekannt, sind alle Pakete mit diesem initialization vector entschlüsselbar.

Die Checksumme (CRC-32) ist kryptographisch nicht sicher. Es ist möglich eine Nachricht gezielt zu ändern, ohne dass die Checksumme geändert werden muss.

3.2.2 Lauschen

Können zwei Pakete mit gleichem initialization vector und gleichem geheimen Schlüssel abgefangen werden, kann man das XOR der beiden Chiffrate und somit der beiden Klartexte berechnen.
Auf dieser Grundlage können statistische Analysen, basierend auf Sprache oder IP-Verkehr gemacht werden, mit dem Ziel Klartext-Chiffrat Paare zu erhalten, womit dann alle weiteren Pakete mit gleichem initialization vector und gleichem Schlüssel entschlüsselt werden können.

3.2.3 Nachrichten einspeisen

Voraussetzung für diese Attacke ist die Kenntnis eines Klartext-Chiffrat Paares (X, RC4(X)).
Der Angreifer generiert eine neue Nachricht inkl. CRC-32. Da die stream cipher die Eigenschaft hat, dass

RC4(Y) xor Y xor X = RC4(X),

kann unter Verwendung des Klarttext-Chiffrat Paares eine neue korrekt verschlüsselte Nachricht generiert werden.

Auch wenn nicht der ganze Klartext bekannt ist, ist es möglich gezielt einzelne Bits der verschlüsselten Nachricht zu ändern ohne die Checksumme ändern zu müssen. Dies kann vor allem verwendet werden um Teile des IP Headers zu ändern, wie z B. die Zieladresse. Der Angreifer könnte sich somit die Nachrichten an einen eigenen Host im Internet schicken lassen. Da die Verschlüsselung nur zur Übertragung der Daten innerhalb des WLANs verwendet werden, wird der Angreifer auf seinem Host die unverschlüsselten Daten erhalten.

4 Zusammenfassung

Die Verschlüsselung von Bluetooth scheint sicher, falls ein geeigneter PIN gewählt wird.
Die Möglichkeit von location attacks wurde aber bei der Entwicklung anscheinend nicht in Betracht gezogen. Eine Möglichkeit zur Anonymisierung wird nicht einmal ansatzweise angeboten.

IEEE 802.11 bietet zwar eine sichere Authentisierung, die Verschlüsselung ist allerdings kryptographisch nicht sicher. Durch eine schlechte Auswahl, Kombination und Anwendung von kryptographischen Algorithmen, kann ein Angreifer nach einiger Zeit, abhängig von der gesendeten Datenmenge, Nachrichten entschlüsseln und sogar einspeisen.
Bedenkt man, dass Wireless LAN vor allem für Firmen angeboten wird, und sicher ein Teil davon auf die eingebaute Verschlüsselung vertraut, ist das sehr bedenklich. Nicht nur der Industriespionage ist so Tür und Tor geöffnet, sondern auch sensible Daten der Kunden werden nicht sicher verwaltet und der Datenschutz ist somit nicht gewährleistet.

5 Literaturliste

5.1 Bluetooth

- Bluetooth Security Architecture, Version 1.0
  Thomas Muller, 15.7.1999
  http://www.bluetooth.com/developer/download/download.asp?doc=174
- Security Weaknesses in Bluetooth
  Markus Jakobsson, Susanne Wetzel
  http://www.bell-labs.com/user/markusj/bt.html
- Flaws In Bluetooth Said To Allow Eavesdropping
  John Markov, 19.9.2000
  http://www.info-sec.com/internet/00/internet 091900b j.shtml
- Bluetooth Security
  Juha T. Vainio, 25.5.2000
  http://www.niksula.cs.ut.fi/~jitv/bluesec.html
- Bluetooth Specification, Version 1.1
  22.2.2001
  http://www.bluetooth.com/developer/specification/specification.asp

5.2 IEEE 802.11

- (In)Security of the WEP algorithm
  http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Wired Equivalent Privacy Vulnerability
  Princy C. Mehta, 4. 4. 2001
  http://www.sans.org/infosecFAQ/wireless/equiv.htm
- IEEE Standards: IEEE 802.11 Wireless
  http://standards.ieee.org/getieee802/802.11.html

5.3 CRC-32

- Connected: An Internet Encyclopedia 6.4.1. The CRC-32 Checksum (crc32)
  http://www.freesoft.org/CIE/RFC/1510/78.htm
- CRC and how to Reverse it
  Anarchriz/DREAD, 29 april 1999
  http://www.yates2k.co.uk/anarchriz_crc.htm

5.4 Kryptographie

- Informationssicherheit und Kryptographie WS 2000/2001
  http://www.inf.ethz.ch/personal/meierl/teaching/InfKrypto00/index.shtml