Wireless LAN Sicherheit

Fachseminar Verteilte Systeme

30. April 2002, Martin Hinz

Betreuung: Harald Vogt
Professor: Dr. F. Mattern

Inhalt

1. Aufkommen von Wireless
2. WLAN IEEE 802.11
3. WLAN WEP Protokoll
4. WLAN IEEE 802.11 Attacke
5. Bluetooth – Sicherheit
6. Bluetooth – Attacke

Aufkommen von Wireless

- Wieso immer mehr wireless:
  -Mobilität
  -Einfachheit
  -Preise fallen
  -immer mehr und kleinere Geräte
- Risiken:
  -geringe Sicherheit, Medium Radiowellen, leicht und unbemerkt abhörbar
- Sicherheitsziele:
  1. Vertraulichkeit (Schutz gegen zufälliges Mithören)
  2. Zugriffskontrolle
  3. Datenintegrität [3]

Inhalt

1. Aufkommen von Wireless
2. WLAN IEEE 802.11
3. WLAN WEP Protokoll
4. WLAN IEEE 802.11 Attacke
5. Bluetooth – Sicherheit
6. Bluetooth – Attacke

WLAN IEEE 802.11 Standard

- Offener Standard, wurde schnell verabschiedet
- Verbinden zweier Geräte über Funk
- Verschiedene Standards:

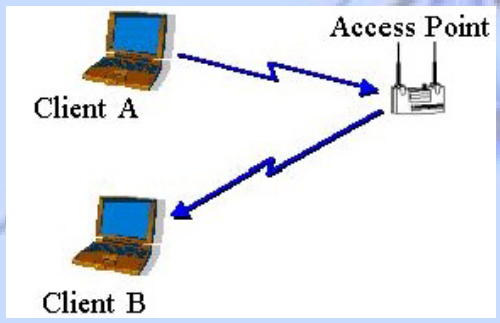
IEEE	Durchsatz	Frequenz	Markt
802.11	1-2 Mbps	2.4 GHz	1997
802.11b	11 Mbps	2.4 GHz	1999
802.11a	54 Mbps	5 GHz	2001
802.11g	54 Mbps	2.4 GHz	??

- Frequenzband wird in Kanäle unterteilt (11 Kanäle) (spread spectrum)

Devices operieren in zwei Modi

Infrastruktur Modus:

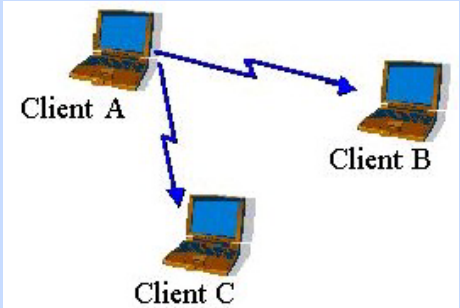
- zentrale Einheit, der Accesspoint (AP)
- operiert als hub und auch als bridge zwischen wire und wireless LAN



[1]

ad-hoc Modus:

- Client kommuniziert direkt mit Client ohne AP (geringere Reichweite)
- müssen im selben Frequenz-kanal senden



[1]

Access zu Infrastruktur

- jeder AP sendet beacon frame (Intervall) mit SSID (service set ID) [1]
- Client hört auf beacon frame oder sucht (probe) AP mit SSID [1]
- jeder AP funkt in einem Frequenzkanal (keine Überlappung der gleichen Frequenz)

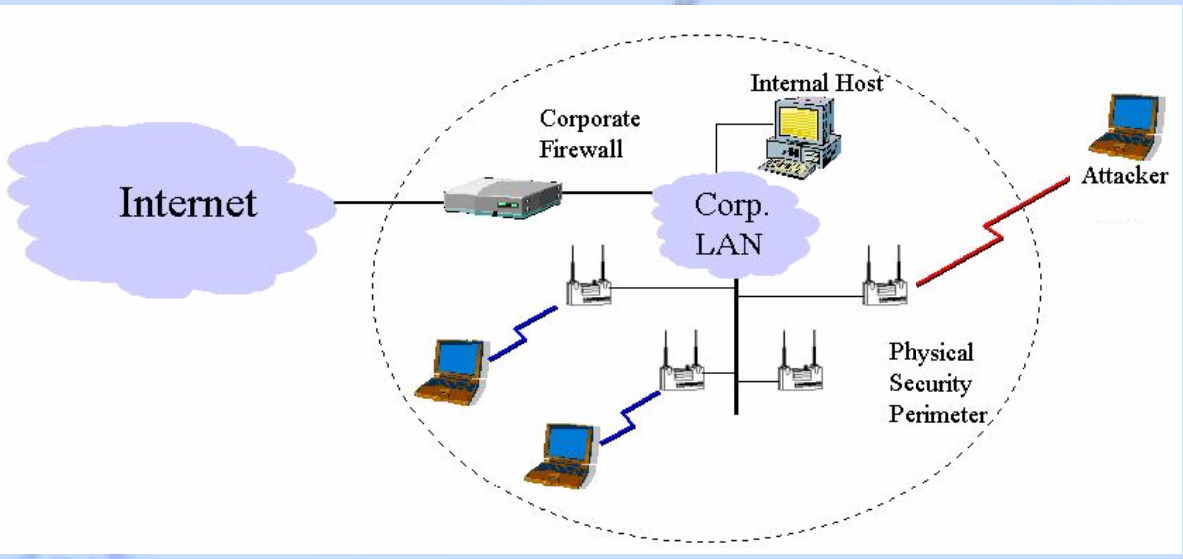
Verbindung

unauthenticated (jedes Device zugelassen)

authenticated (Device muss Zutrittschlüssel haben)

Risiken

- Funkübertragung bringt hohes Risiko mit sich
- Angreifer nicht an Geschäftsgebäude gebunden
- Firewall nützt nichts („back door“, „parking lot“ attack)



[1]

Sicherheit

- Um dies zu verhindern wird das WEP (wired equivalent privacy) Protokoll mit Geheimschlüssel verwendet:
  - Authentication: standard challenge response
  - Verschlüsselung der Nachricht
- zwei Einstellungsmöglichkeiten:
  - einen gemeinsamen Schlüssel
  - vier Schlüssel (Entschlüsselung mit allen vier möglich), doch nur mit default Schlüssel verschlüsseln [1]
- Doch WEP Protokoll nicht robust
- Vieles wurde vom Standard-Komitee offen gelassen:
  - Keymanagement, Implementierung

Alternative Sicherheiten

- zur Authentication:

  - MAC Adresse speichern → unsinnig, weil MAC Adresse lässt sich ändern (per Software) [1]
  - ETH: IP Freischaltung beim Gateway nach Authentication, doch schon vorher im Funknetz

- zur Verschlüsselung:

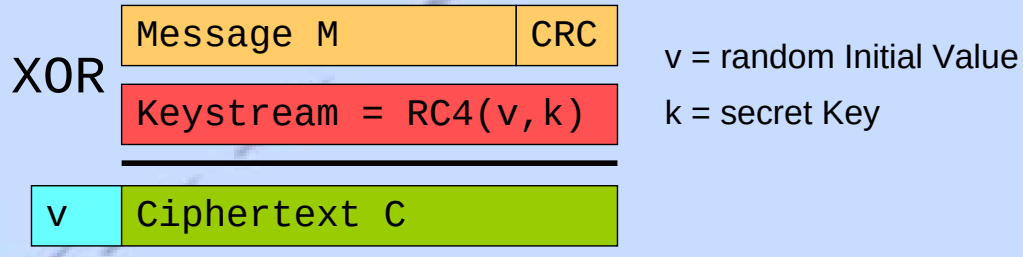
  - auf höherer Ebene verschlüsseln mit z.B. SSL, SSH, VPN (Virtuell Private Network)

Inhalt

1. Aufkommen von Wireless
2. WLAN IEEE 802.11
3. WLAN WEP Protokoll
4. WLAN IEEE 802.11 Attacke
5. Bluetooth – Sicherheit
6. Bluetooth – Attacke

WLAN WEP Protokoll

- Daten M werden mit geheimen symmetrischen Schlüssel verschlüsselt
- 2 Phasen:
  1. Checksumme: c(M) hier mit CRC
  2. Verschlüsselung von P = <M,c(M)>:



v = random Initial Value

k = secret Key

A -> B: <v,C> mit C= <M,c(M)> ⊗ RC4(v,k)

B: P'= C ⊗ RC4(v,k)= (P ⊗ RC4(v,k)) ⊗ RC4(v,k)=P

[3]

- 802.11b WEP1: k= 40bit v=24bit
  802.11a WEP2: k=104bit v=24bit

Risiko des Protokolls

- Keystream reuse: IV ist endlich und in Klartext
- zwei Nachrichten mit gleichem IV:
  $C1 = P1 \otimes RC4(v,k)$ und $C2 = P2 \otimes RC4(v,k)$

  $C1 \otimes C2 = (P1 \otimes RC4(v,k)) \otimes (P2 \otimes RC4(v,k)) = P1 \otimes P2$

  XOR zweier Verschlüsselungen gibt XOR der beiden Klartexte [3]
- statistische Suche in $P1 \otimes P2$ nach P1 oder P2
- noch schlimmer: Klartext bekannt
- Wahl von IV:
  - init der Karte mit IV = 0, dann pro Nachricht eins hochzählen
  - zufälliger IV → noch schlechter, Birthdayparadox
  - bei beschäftigtem AP gehen IVs nach halben Tag aus
  - 802.11 Standard setzt nicht voraus, dass IV geändert wird

Inhalt

1. Aufkommen von Wireless
2. WLAN IEEE 802.11
3. WLAN WEP Protokoll
4. WLAN IEEE 802.11 Attacke
5. Bluetooth – Sicherheit
6. Bluetooth – Attacke

Attacken (passiv)

- Gegner erkennt reuse des keystreams (sieht IV Wert in Klartext)
- viel Redundanz in Nachrichten, z.B. Passwort prompt oder Headerinfos von bekannten Protokollen
- statistische Suche in P1 ⊗ P2 mit redundanten Daten oder Gegner schickt dem Opfer bekannten Klartext (z.B. E-mail), dann Teile von P1 oder P2 bekannt
- es gibt AP's, welche Broadcastnachrichten im Klartext und verschlüsselt senden (Grund: damit Broadcast an alle Clients gelangt)
- auf Authentication eines Clienten warten (übers Netz gehen Klartext und Verschlüsselung einer Zufallszahl)

[3]

IV Wörterbuch

- aus Klartext und Ciphertext lässt sich Keystream berechnen:

$C = RC4(v,k) \otimes P$

C und P bekannt

$\longrightarrow$ $RC4(v,k) = C \otimes P$

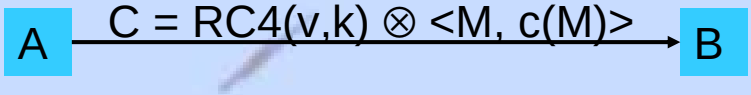
- anlegen eines IV Wörterbuch (mühsam aber erreichbar)
  bei 24bit IV Wort sind das ungefähr 24GB
  WEP2 keine Besserung (IV immer noch 24bit)

  für jede Nachricht mit bekanntem IV, lässt sich Klartext berechnen

[3]

Attacken (aktive)

- Keystream eines IV bekannt
  → neue Nachricht korrekt verschlüsselt erzeugen
  → erfolgreiche Authentication
- bei nicht bekanntem Keystream, Änderung möglich:
  CRC linear → als error checksum gedacht (Übertragungsfehler)
  weil CRC linear → Klartext in Ciphertext änderbar:



ohne bekanntem M, ist M nach M‘ mit bekanntem Δ änderbar:
C‘ = C ⊗ <Δ,c(Δ)>
= RC4(v,k) ⊗ <M, c(M)> ⊗ < Δ,c(Δ)>
= RC4(v,k) ⊗ <M ⊗ Δ, c(M) ⊗ c(Δ)>
= RC4(v,k) ⊗ <M‘, c(M‘)>
nützlich für z.B. IP Redirection (raten der IP in M und auf neue IP ändern, also Nachricht umleiten) [3]

Zusammenfassung

Schwachpunkte → Verbesserungen

WEP meistens auf disable	enable und Key häufig wechseln
linearer CRC checksum	auf MAC (secure message authentication code) wechseln
RF Signal weit entfernt empfangbar	W-LAN vor Firewall setzen
IV kurz, reuse tritt schnell auf und ist vorhersehbar	WEP2 leider keinen Ausweg (IV Länge ist gleich)
RC4 stream cipher unsicher, unabhängig von Message	AES (Blockverschlüsselung), braucht aber mehr Rechenleistung [5]

bei nächstem Design von Fehlern lernen und der Öffentlichkeit vorführen!!

Inhalt

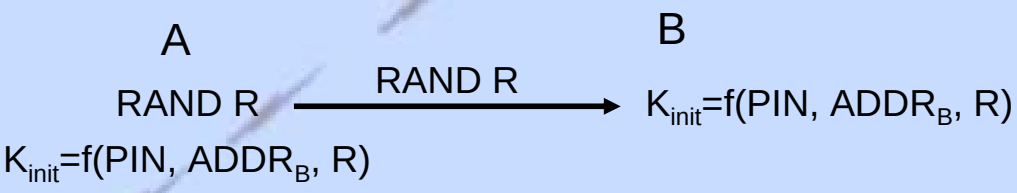
1. Aufkommen von Wireless
2. WLAN IEEE 802.11
3. WLAN WEP Protokoll
4. WLAN IEEE 802.11 Attacke
5. Bluetooth – Sicherheit
6. Bluetooth – Attacke

Bluetooth - Übersicht

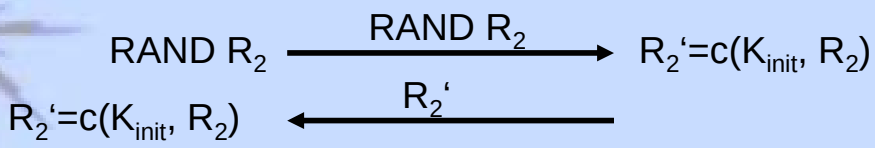
- Ziel: Geräte sollen sich selbständig zu PAN (Private Area Network) vernetzen, Service suchen und kommunizieren
  → Freiheit für Benutzer
- funkt auch im 2,4 GHz Bereich (weltweit freie Frequenz) mit fast frequenzy hopping [7]
- Kommunikation nur bis ungefähr 10m möglich
- jedes Gerät besitzt einmalige Geräteadresse, einen UNIT Key (geheim) und einen PIN
- Gerätestatus:
  - discoverable (offen für jede Kommunikation)
  - non-discoverable (Benutzer muss Kommunikation aktivieren)

Bluetooth - Sicherheit

- einseitige oder gegenseitige Authentication mit gemeinsamen Schlüssel (init key)
- Verschlüsselung mit encryption key
- encryption key abgeleitet aus link key, für jede session neu
- Verbinden zweier Geräte (erste mal): [2]



- Gegenseitige Authentication:



Rollen werden getauscht

[7]

Bluetooth - Sicherheit

- Zwei Protokolle für Link Key Generierung:

1. Protokoll: Gerät mit wenig freien Ressourcen
Gerät schickt seinen UNIT Key mit K_{init} verschlüsselt
UNIT Key wird zu Link Key

2. Protokoll: wenn 1. Protokoll nicht verlangt wird
Geräte machen unter sich einen gemeinsamen Link Key aus
(je eine Randomnumber und Geräteadressen)

- wenn Verschlüsselung gebraucht wird, aus link key den encryption key generieren

[8]

Inhalt

1. Aufkommen von Wireless
2. WLAN IEEE 802.11
3. WLAN WEP Protokoll
4. WLAN IEEE 802.11 Attacke
5. Bluetooth – Sicherheit
6. Bluetooth – Attacke

Bluetooth - Attacke

- pseudozufällige hopping sequenz lässt sich leicht abhören
- seed der Zufallssequenz aus master addr und master clock
- Angreifer sieht Verbindungsaufbau, also R, R_2 und R_2‘ mit R_2‘=c(K_{init}, R_2) und K_{init}=f(PIN, $ADDR_B$, R)
  kann offline nach richtigem PIN gesucht werden
- Angreiffer kann online alle PIN‘s durchprobieren und sich anmelden
- Geräte ohne Eingabe haben immer PIN 0000 (z.B. Headset)
- Master erhält UNIT Key eines memoryarmen Gerätes A
  → Master kann Gerät A imitieren und andere Kommunikation mithören
- viele Devices im discoverable Mode → Lokalisieren eines Devices möglich
  (wenn User-Device bekannt → Userlokalisierung)
- nur Payload verschlüsselt → Kommunikationshäufigkeit zwischen Geräten überwachbar

[7,8]

FAZIT

- beide Verfahren nur begrenzt sicher, doch Ziel:
  - Bluetooth: kabellose Übermittlung → erreicht
  - IEEE 802.11: WEP → Kabel auch abhörbar
- wenn grosse Sicherheit gefordert
  → auf Applikationsebene lösen z.B. mit SSL, SSH, VPN (Virtuell Private Network)
- Sicherheit einstellbar, für normalen Benutzer nicht naheliegend
- schon wenig Sicherheit schreckt willkürlichen Angreifer ab
- Bluetooth Technologie noch offen und im Entwicklungsstadium (Sicherheit nicht im Vordergrund)
- Lücken sind bekannt → man weiss wo man sich wie schützen kann

Literatur

[1] „Your 802.11 Wireless Network has No Clothes“
(William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan Uni Maryland)

[2] „A Survey on Security Issues in Wireless Networks“
(Praveen Yalagandula)

[3] **„Intercepting Mobile Communications: Insecurity of 802.11“**
(Nikita Borisov, Ian Goldberg, David Wagner)

[4] „Security of the WEP algorithm“
(Nikita Borisov, Ian Goldberg, David Wagner)

[5] „Flicken für Sicherheitslöcher in Funk-LANs“
(Heise News-Ticker, Meldung vom 19.12.2001)

[6] „Overview of IEEE 802.11b Security“
(Sultan Weatherspoon, Network Communications Group, Intel Corporation)

[7] **„Security of Bluetooth: An overview of Bluetooth Security“**
(Marjaana Träskbäck)

[8] **„Security Weaknesses in Bluetooth“**
(Markus Jakobsson, Susanne Wetzel, Lucent Technologies, Bell Labs, USA)