Proseminar
Kryptographische Protokolle: WLAN

Danilo Bürger
07.07.2009

Gliederung

- Motivation
- WLAN Standard
- WLAN Sicherheit

Motivation

- Warum sprechen wir über WLAN?
  - Seit Q3 2007 mehr Notebooks als Desktops im EMEA Bereich verkauft (IDC)
  - 14.000 Hotspots in Deutschland (DPA 2008)
  - 46 % der EU Haushalte mit Internetanschluss nutzen WLAN (DPA 2008)
  - 54 % aller großen Unternehmen investieren mehr Geld in die Datenübertragung über WLAN als über Kabel (Motorola 2008)

Motivation

- Nur 47 % aller Unternehmen schützen ihr WLAN mit WEP / WPA / o.ä. (Motorola / Vason Bourne 2009)
- Weniger als 30 % aller Unternehmen benutzen Intrusion Detection / Prevention System (Motorola / Vason Bourne 2009)
- Bis zu 14,7 % aller WLAN Netzwerke komplett offen (PC Praxis 2008)

Gliederung

- Motivation
- WLAN Standard
- WLAN Sicherheit

WLAN Standard

- Fast immer ist mit WLAN der Standard IEEE 802.11 (seit 1997) und dessen Erweiterungen gemeint
- Die Familie 802.11 besteht z.Z. aus 11 Normen
- Seit 1997 ständige Weiterentwicklung
- Weiteste Verbreitung: 802.11b/g
- Neuste Erweiterung in der Entwicklung: 802.11n

WLAN Standard - Normen

Standard	Datentransfer	Frequenz	Reichweite	Akzeptanz
802.11	2 Mb/s	ISM 2,4 GHz	n.a.	Veraltet
802.11a	54 Mb/s	5 GHz	10 - 15m	Geringe Verbreitung
802.11b	11 Mb/s	ISM 2,4 GHz	30 - 50m	Weite Verbreitung
802.11g	54 Mb/s	ISM 2,4 GHz	30 - 50m	Weltweite am verbreitetsten
802.11n (Draft)	600 Mb/s	ISM 2,4 GHz / 5 GHz	50 - 70m	Geräte schon verfügbar
802.11p (Draft)	27 Mb/s	5,85 GHz	n.a.	Favorisiert vom C2C-CC

WLAN Standard - Normen

Standard	Bedeutung
802.11c	MAC-Layer-Bridging
802.11d	Anpassung an die regulatorischen Bestimmungen verschiedener Länder
802.11e	Unterstützung von Quality-of-Service
802.11f	Interoperabilität zwischen Basisstationen
802.11h	Reichweitenanpassung, Indoor- und Outdoor-Kanäle (im 5-GHz-Band), TPC/DFS
802.11i	Erweiterungen bezüglich Sicherheit und Authentifizierung
802.11j	4,9 – 5 GHz Operation in Japan
802.11s (Draft)	Mesh-Netzwerke

Quelle: Wikipedia

WLAN Standard - Sendeleistung

- Regulierung durch Bundesnetzagentur

- Bei ISM 2,4 GHz in Deutschland 100 mW
  - Andere Länder bis zu 300 mW
- Bei 5 GHz in Deutschland 30 mW (802.11a)
  200 mW (802.11h)
  - Andere Länder bis zu 1000 mW

WLAN Standard - Frequenz

- ISM 2,4 GHz
  - ISM ist gebührenfrei
  - Kein Spektrum Management nötig
  - Hohe Verbreitung, geringe Gerätekosten
  - Häufig Störungen und Interferenzen da selbe Frequenz wie Bluetooth / Mikrowellen / etc.
  - Störungsfreier Betrieb bei max. 3 Netzwerken am selben Ort möglich (Kanäle 1, 7 und 13)

WLAN Standard - Frequenz

- 5 GHz
  - Weniger genutzt, daher weniger Störungen
  - 19 nicht überlappende Kanäle in Deutschland
  - Höhere Reichweite dank höherer Sendeleistung möglich
  - Stärkere Regulierung in Europa
  - Ad-hoc Modus kaum unterstützt
  - Geringe Verbreitung, teure Geräte

WLAN Standard – Funkübertragung

- Übertragungstechnik: Funkwellen
- Zwei Varianten auf ISO-OSI Schicht 1 (Bitübertragung)
  - Frequency Hopping Spread Spectrum
    - Frequenzsprungverfahren
    - 79 Frequenzbänder a 1 MHz im ISM Band
    - Auswahl über pseudo-zufällige Sprungsequenz
  - Direct Sequence Spread Spectrum
    - Bandspreizverfahren
    - 14 Kanäle (13 in Europa)
    - Frequenzspreiung über XOR mit Daten und einer Pseudozufallsfolge

WLAN Standard - Modi

- Ad-hoc Modus
  - Endgerät zu Endgerät
- Infrastruktur Modus
  - Endgerät zu Access Point
  - Access Point aggiert als Brücke
  - Brückenfunktion über ISO-OSI Schicht 2 (Data Link Layer)
  - Mehrere Access Points können zu einem Extended Service Set (ESS) zusammengefasst werden

WLAN Standard - Betriebsmodi

- Jeder Access Point besitzt einen Service Set Identifier (SSID)
- Kontaktaufnahme zum Access Point abhängig vom Betriebsmodi:
  - Open Network: Der Access Point akzeptiert jegliche SSID
  - Closed Network: SSID des Access Points muss dem Endgerät bekannt sein
  - Cloaked Network: Wie Closed Network, nur sendet der Access Point keine Broadcast Beacon Frames und reagiert nicht auf Probe Nachrichten

Gliederung

- Motivation
- WLAN Standard
- WLAN Sicherheit

WLAN Sicherheit

- WLAN Sicherheit hat immensen Stellenwert, da Übertragung per Funk stattfindet
- DEFCON hält Weltrekord mit einer Übertragung von über 200 km mit handelsüblichen WLAN Karten und Parabolspiegel
- Städtisch ist eine Abhörung von mehreren hundert Metern mit geringen Budget sehr realistisch

WLAN Sicherheit – Cloaked Network

- Vermutung: Durch betreiben eines Cloaked Network brauche ich ein „Passwort“ um überhaupt mit dem Access Point Kontakt aufzunehmen
- Die Kontaktaufnahme erfolgt über Management Nachrichten im Klartext
- Daher kann der SSID abgehört werden
- Security over Obscurity

WLAN Sicherheit – Denial of Service

- Endgeräte rechnen mit Interferenzen
- Endgeräte verzögern deshalb die Datenübertragung falls Störungen auftreten
- Angreifer sendet in festgelegter Zeitspanne Störsignale aus
- Die Datenübertragung kann nicht fortgesetzt werden, da Endgerät immer wieder verzögert
- Mittels Disassociation oder Deauthentication Management Nachrichten gezielt Endgeräte abmelden

WLAN Sicherheit - ACL

- Nur Endgeräte mit im Access Point eingetragener MAC Adresse können sich verbinden
- MAC Adressen werden im Klartext übertragen
- Fast jede WLAN Karte erlaubt das Ändern der MAC Adresse
- Durch Abhören einer gültigen MAC Adresse ist MAC Spoofing möglich

WLAN Sicherheit – Man in the Middle

- Endgeräte verbinden sich in der Regel mit dem Access Point mit der größten Signalstärke
- Spoofen des SSID und erhöhen der Signalstärke über dem zulässigen Grenzwert
- Endgeräte verbinden sich nun auf den Access Point des Angreifers

WLAN Sicherheit – Verschlüsselung

- Um WLAN effektiv gegen das Ablauschen und Man in the Middle Attacken zu schützen, wird eine Verschlüsselung eingesetzt:
  - WEP (Wired Equivalent Privacy, 802.11)
  - WPA (Wi-Fi Protected Access, 802.11i)
  - WPA2 (Wi-Fi Protected Access 2, 802.11i)

WLAN Sicherheit – Verschlüsselung: WEP

- Sender und Empfänger teilen einen gemeinsamen symmetrischen Schlüssel K um Nachricht M auszutauschen
- Der Sender berechnet die Prüfsumme CRC(M)
- Der Sender wählt einen 24 Bit langen Initialisierungsvektor IV
- Mittels RC4 wird ein Schlüsselstrom erzeugt: Key = RC4(IV | K)

WLAN Sicherheit – Verschlüsselung: WEP

- Die Nachricht wird verschlüsselt: C = (M | CRC(M)) mod Key
- Danach überträgt der Sender die verschlüsselte Nachricht C und den Initialisierungsvektor IV
- Der Empfänger generiert sich aus dem Schlüssel K und dem erhaltenen IV einen eigenen Schlüsselstrom Key

WLAN Sicherheit – Verschlüsselung: WEP

- Der Empfänger entschlüsselt die Nachricht: C mod Key = M | CRC(M‘)
- Der Empfänger überprüft anschließend die Nachricht mit CRC(M) = CRC(M‘)

WLAN Sicherheit – Verschlüsselung: Angriffe auf WEP

- WEP ist ein Shared Key Autentifikationsschema
- Einzelne Benutzer sind nicht individuell autentifizierbar
- Schlüssel ist in der Praxis vielen Administratoren wenn nicht gar allen Mitarbeitern bekannt
- Der Schlüssel ist also nicht mehr wirklich ein Geheimnis
- Da kein Schlüsselmanagement vorgesehen ist, gibt es keine periodische Schlüsselerneuerung
- Das ändern des Schlüssel ist bei einer großen Zahl an Mitarbeitern recht Zeit und Kosten intensiv

WLAN Sicherheit – Verschlüsselung: Angriffe auf WEP

- Einseitiges, symmetrisches Challenge-Response Protokoll
- Access Point muss sich nicht autentifizieren
- Access Point vom Angreifer mit erhöhter Signalstärke wird bevorzugt
- Angreifer kann daher alle verschlüsselten Daten zur späteren Analyse speichern

WLAN Sicherheit – Verschlüsselung: Angriffe auf WEP

- CRC-32 ist nicht geeignet um die Integrität der Nachricht M zu gewährleisten
- Es gilt CRC(M mod M‘) = CRC(M) mod (CRC M‘)
- Dadurch können verschiedene Bits einer Nachricht M verändert werden und zugleich kann die Prüfsumme angepasst werden
- Das Einspielen einer Nachricht D erweist sich mit C‘ = C mod (D | CRC(D)) als recht einfach da auch RC4 linear arbeitet

WLAN Sicherheit – Verschlüsselung: Angriffe auf WEP

- Es gibt noch weitere Angriffe auf WEP zum umlenken, einschleusen und entschlüsseln von Nachrichten
- Ausserdem können durch gezielte Nachrichten an den Access Point Datenpakete generiert werden
- WEP Schlüssel werden mittlerweile in unter 60 Sekunden geknackt (TU Darmstadt) mit nur 100.000 Datenpakete

WLAN Sicherheit – Verschlüsselung: WPA und WPA2

- WPA ist ein Übergangsprotokoll von WEP auf WPA2 da der Standard 802.11i sehr umfangreich ist und nicht rechtzeitig fertig gestellt werden konnte
- 2008 wurden Schwachstellen zu WPA öffentlich
- WPA2 gilt bisher als ausreichend sicher

Danke für die Aufmerksamkeit