Sicherheit in Funknetzen – alles nur Scheinsicherheit?

Thomas Nowey
Klaus Plößl
Universität Regensburg

Gliederung

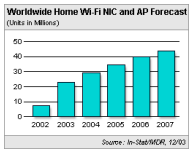
- Einführung
- Schutzziele und Risiken
- WLAN
- WLAN-Schwachstellen
- Maßnahmen zur Absicherung von WLANs
- Entwicklungstrends im WLAN Sicherheitsbereich
- Fazit

Gliederung

- **Einführung**
- Schutzziele und Risiken
- WLAN
- WLAN-Schwachstellen
- Maßnahmen zur Absicherung von WLANs
- Entwicklungstrends im WLAN Sicherheitsbereich
- Fazit

Einführung

- Drahtlose Netzwerke sehr populär
  - Zunehmende Verbreitung bei Unternehmen und Privathaushalten
  - Hardware-Umsätze steigen mit zweistelligen Wachstumsraten
- Vielfältige Vorteile
  - Erhöhte Mobilität
  - Ersatz physischer Anschlüsse
  - Vermeidung störender Verkabelung
  - Kostengünstig
  - Vereinfachte Planung
  - Spontane Vernetzbarkeit



Gliederung

- Einführung
- **Schutzziele und Risiken**
- WLAN
- WLAN-Schwachstellen
- Maßnahmen zur Absicherung von WLANs
- Entwicklungstrends im WLAN Sicherheitsbereich
- Fazit

Schutzziele

- Vertraulichkeit
- Integrität
- Verfügbarkeit

⇒ Unterscheiden sich nicht von denen in kabelgebundenen Netzen

⇒ Damit auch äquivalente Schutzmaßnahmen erforderlich

ABER

Zusätzliche Angriffsmöglichkeiten entstehen aus der unkontrollierten Ausbreitung der Funkwellen ➔ unerlaubte Eingriffe in den Netzverkehr werden möglich

Besondere Risiken bei drahtlosen Netzen

Risiken / Auswirkungen	Vertraulich-keit	Integrität	Verfügbar-keit
Abfangen und Manipulation des drahtlosen Netzwerkverkehrs	x	x	x
Einschleusen nicht autorisierter Hardware-Komponenten	x	x	x
Überlastung des Netzwerks			x
Client-to-Client Angriffe	x		x
Attacken auf Sicherheitsfunktionen des Protokolls	x	x	x
Fehlkonfigurationen	x	x	x

Abfangen und Manipulation

- Problemloses Abfangen der über den Äther versendeten Pakete möglich, da kein physischer Zugang zum Netzwerk(-kabel) nötig
- Manipulation des Netzwerkverkehrs
  - z.B. Hijacking der Verbindung
- Falls Access Points (APs) eingesetzt werden:
  - Broadcast Monitoring
    - Annahme: AP arbeitet als Hub
    - Datenverkehr, der nicht für drahtlose Clients bestimmt ist, gelangt ins drahtlose Netz
  - Access Point Clone (Evil Twin) Traffic Interception
    - Angreifer stellt eigenen AP mit hoher Sendeleistung auf
    - Clients versuchen, sich bei diesem einzuloggen
    - Geben dabei möglicherweise Passwörter und andere sensible Daten preis

Einschleusen nicht autorisierter Komponenten

- Aufbau neuer Netze unter Umgehung des normalen Sicherheits-Prozesses und -Reviews
- Nicht autorisierte Clients:
  - Angreifer versucht mit einem drahtlosen Client ohne Autorisierung auf das Netzwerk zuzugreifen
  - Ist der Zugriff nicht (passwort-)geschützt, hat der Angreifer Zugriff auf alle Ressourcen des Netzwerks
- Nicht autorisierte (Rogue, Renegade) Access Points:
  - Mitarbeiter stellen unberechtigt APs auf
  - Nicht autorisierte Clients können auf das Netzwerk zugreifen

Überlastung des Netzwerks

- Absichtlich:
  - Denial-of-Service Attacken leicht durchzuführen
    - Drahtlose Bandbreite vergleichsweise gering
    - Zum Senden kein Zugang zum Netzwerk benötigt
    - Auch Störsender können Übertragung verhindern
- Unabsichtlich:
  - Viele drahtlose Komponenten funken in den (knappen) lizenzfreien Frequenzen (z.B. Babyphone, Funktelefone, Bluetooth, WLAN..) und stören sich dabei gegenseitig
  - Mitarbeiter, die sehr viel Bandbreite benötigen, können das drahtlose Netzwerk zum Erliegen bringen (Network abuse)

Client-to-Client Angriffe

- Zwei drahtlose Clients können ohne Umwege direkt miteinander kommunizieren. Die Clients müssen also auch gegeneinander abgesichert werden.
- TCP/IP-Dienst-Angriffe
  - Alle Dienste die auf einem drahtlosen Client laufen, sind genauso anfällig für Exploits und Fehlkonfigurationen, wie ihre drahtgebundenen Pendants
- DoS (Denial-of-Service)
  - Ein drahtloses Gerät kann andere drahtlose Geräte mit fehlerhaften Paketen überfluten und so eine Denial-of-Service-Attacke durchführen
  - Doppelte IP- oder MAC-Adressen können den Datenfluss im Netzwerk unterbrechen

Attacken auf die Sicherheitsfunktionen des Protokolls

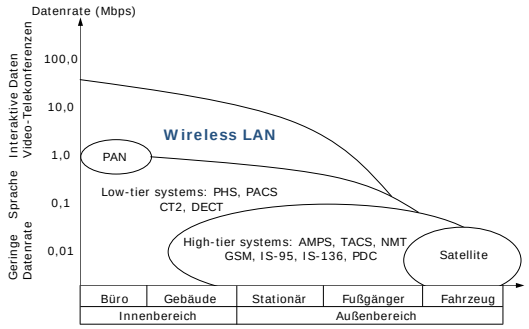
- Protokolle für drahtlose Netzwerke können folgende Sicherheitsfunktionen beinhalten:
  - Verschlüsselung
  - Authentifikation
  - Integritätssicherung
- Diese sind meist nicht perfekt und bieten Angriffsmöglichkeiten, wie z.B.:
  - Brechen der Verschlüsselung
  - Umgehung der Authentifikation

Fehlkonfigurationen

- Fehlerhafte Konfiguration von Soft- und Hardware durch
  - Schlechte Default-Einstellungen
  - Unachtsamkeit bzw. Unwissenheit der Benutzer
  - Feature-Drang der Hersteller (aber auch der Nachfrager)
  - ...

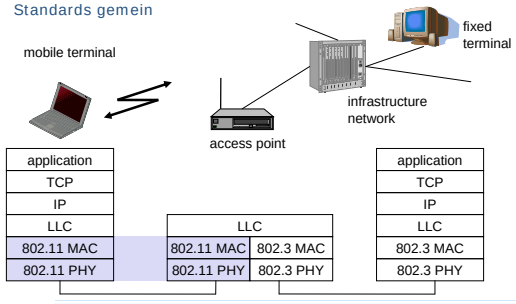
Gliederung

Drathlose Systeme: Datenrate vs. Ausdehnung



WLAN: 802.11 - Standard

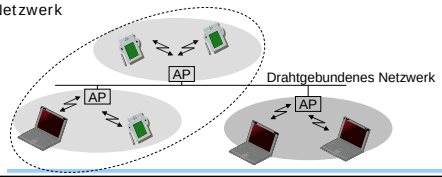
- Übertragungsprotokoll 802.11 für WLANs standardisiert von IEEE
- 802.11 definiert Schicht 1 und Teile von Schicht 2 des OSI-Modells
- 802.11 hat Logical Link Control (802.2) mit den anderen 802-Standards gemein



WLAN Topologien

- Ad-Hoc Modus: Peer-to-Peer Verbindungen

- Infrastrukturmodus:
  - Zugang über Access Points (APs)
  - Diese Basisstationen regeln den Zugang der Clients zum Netzwerk



IEEE 802.11 Protokollfamilie

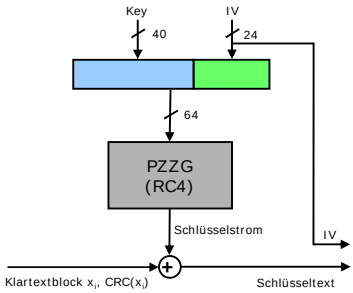
- Die bekanntesten Vertreter des WLAN-Standards:
  - IEEE 802.11:
    - Infrared (IR)
    - Radio frequency (RF) im 2,4-GHz ISM Band
    - 1 or 2 Mbps
  - IEEE 802.11b: 11 Mbps im 2,4-GHz ISM Band
  - IEEE 802.11a: 54 Mbps im 5-GHz ISM Band
  - IEEE 802.11g: 54 Mbps im 2,4-GHz ISM Band
  - IEEE 802.11i: Security (noch nicht fertig)
- 802.11 definiert WEP (Wired Equivalent Privacy) als optionalen Schutzmechanismus
- Die Erweiterungen a, b und g bieten keine zusätzlichen Sicherheitsmechanismen, erst 802.11i wird neue Sicherheitsmechanismen definieren

WEP - Wired Equivalent Privacy

- Optionales Subprotokoll von 802.11
- Definiert Verschlüsselung, Integritätssicherung und Authentikation
- Dient ausschließlich zur Sicherung der Funkstrecke zwischen Clients und AP
- In praktisch allen WLAN Geräten implementiert

- Verschlüsselung:
  - RC4 Algorithmus
  - Symmetrischer 40 bzw. 104 Bit Schlüssel
  - Initialisierungsvektor (IV) 24 Bit

Funktionsprinzip von WEP



WEP: Integritätssicherung und Authentikation

- Integritätssicherung:
  - Jedem Paket wird eine CRC-32 Checksumme angehängt
  - Checksumme wird zusammen mit Klartext verschlüsselt
  - Empfänger vergleicht berechnete Checksumme mit der gesendeten
  - Paket wird verworfen, wenn beide nicht identisch sind

- Authentikation:
  - Zwei Varianten: *Open* und *Shared Key*
  - *Open* deaktiviert Authentikation (nur Server Set ID)
  - *Shared Key*: Challenge-Response Verfahren

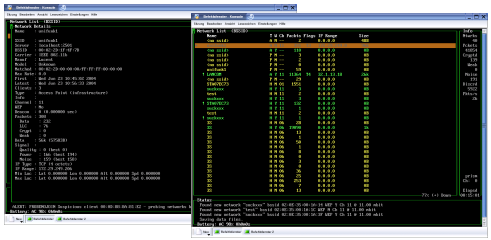
Gliederung

WLAN Schwachstellen

- SSID
- Sniffing
- MAC Adressen
- WEP
- Nicht autorisierte Access Points
- Fehlkonfigurationen

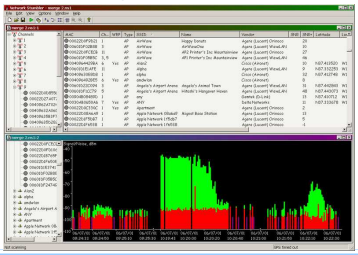
Service Set ID (SSID)

- SSID ist der Name des drahtlosen Netzwerks
- Wird benutzt, um sich mit einem AP zu verbinden
- Es können folgende Probleme auftreten:
  - Ist ein Netzwerk nicht mit WEP geschützt, reicht allein die SSID, um sich damit zu verbinden
  - SSID wird per default gebroadcastet
  - Änderungen der SSID müssen allen Benutzern mitgeteilt werden

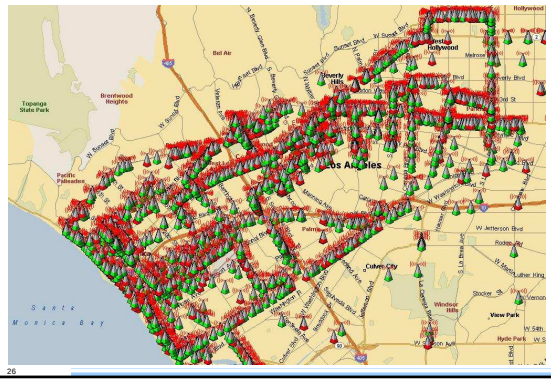


Sniffing

- Sniffing in WLANs sehr einfach
- War Driving ist ein richtiges Hacker-Hobby
  - http://www.wardriving.com/
- Man fährt durch Wohn- und Industriegebiete und scannt nach ungeschützten 802.11 WLANs
- Es sind viele War-Driving-Tools verfügbar:
  - NetStumbler
  - AiroPeek
  - MobileManager
  - Sniffer Wireless
  - THC-WarDrive

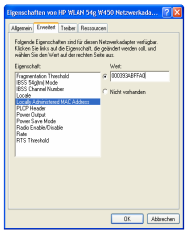


Bsp. Los Angeles



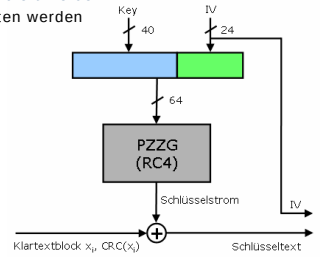
MAC Adressen

- Möglichkeit den Zugriff auf das Netzwerk auf bestimmte MAC-Adressen einzuschränken
- Dies führt zu folgenden Problemen:
  - Schwierig die Liste der gültigen MAC-Adressen zu verwalten und auf dem neusten Stand zu halten
  - MAC-Adressen können gefälscht werden (MAC spoofing)



WEP: Vorraussetzungen für die Sicherheit

- Schlüsselstrom darf sich nicht wiederholen
  - IV darf nicht wiederverwendet werden
  - oder Schlüssel muss gewechselt werden
- Schlüsselstrom kann aus IV und zugehörigem Klartext-Schlüsseltext-Paar rekonstruiert werden
  - Klartext darf nicht erraten werden



WEP: Schwachstellen (1), IV und Schlüssel

- Zu kurzer Initialisierungsvektor
  - IVs und damit die Schlüsselströme wiederholen sich oft (v.a., da meist Zähler verwendet werden, die nach einem Reboot bei 0 beginnen und linear hochzählen)
  - Angreifer kann eine Übersetzungstabelle erzeugen
- Zu geringe Verschlüsselungsstärke
  - nur 40 Bit im ursprünglichen Standard
- Nicht vorhandenes Schlüsselmanagement
  - anfällig für Brute-Force-Attacken, da die Schlüssel potentiell sehr lange benutzt werden
  - alle Clients benutzen den gleichen Schlüssel
- Frei verfügbares Brute-Force-Tool THC-RUT

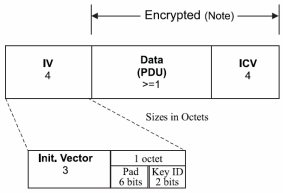
WEP: Schwachstellen (2), RC4

- RC4 Algorithmus schlecht implementiert:
  - „Schwache“ IVs können benutzt werden, um den Schlüssel mit einem statistischen Angriff zu berechnen
  - Known-Plaintext-Angriff: Jedes Paket beginnt mit demselben Bytes (Hex AAAA03), da die Daten mit einem SNAP-Header (Sub Network Access Protocol) versehen werden
  - Die ersten drei Bytes des temporären Schlüssels sind implizit bekannt (IV unverschlüsselt übertragen)
  - Nach kurzer Zeit frei verfügbare Tools im Internet (AirSnort, WEPCrack)

	Paketgröße		
Anzahl Pakete	512 Byte	1024 Byte	2048 Byte
2.000.000	0,95 GB	1,91 GB	3,81 GB
4.000.000	1,91 GB	3,81 GB	7,63 GB
6.000.000	2,86 GB	5,72 GB	11,44 GB
8.000.000	3,81 GB	7,63 GB	15,26 GB

WEP: Schwachstellen (3), CRC

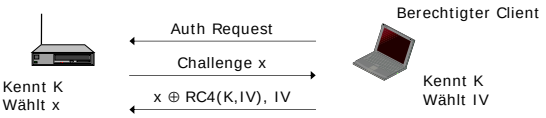
- CRC und Verschlüsselung sind linear:
  C(a XOR b) = C(a) XOR C(b)
- Fälschung von Daten leicht möglich:
  - XOR-Addition einer beliebigen Zahl zum (verschlüsselten) Klartext
  - XOR-Addition der CRC-Checksumme dieser Zahl zur verschlüsselten Checksumme



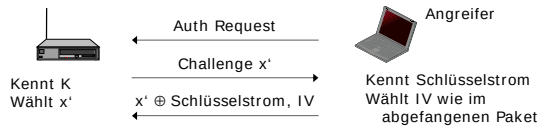
WEP: Schwachstellen (4), Authentikation

- Authentikation nicht nur unwirksam, sondern sogar gefährlich für die Verschlüsselung:
  - Challenge-Response-Paar kann abgehört werden
  - Schlüsselstrom durch XOR-Verknüpfung rekonstruierbar
  - Schlüsselstrom kann zur eigenen Authentikation, Ver- oder Entschlüsselung wiederverwendet werden
  - Nur einseitige Authentikation, kein Schutz vor falschen APs

Authentikation detailliert



- Angreifer kann IV, x und x ⊕ RC4(K,IV) abhören
- Mit Klartext x und Schlüsseltext x ⊕ RC4(K,IV) wird Schlüsselstrom unter IV rekonstruiert



Nicht autorisierte Access Points

- Zwei Möglichkeiten:
  - „Piraten“-APs von Angreifern
  - Nicht genehmigte APs von Mitarbeitern, die schlecht konfiguriert sind
- Beides kann zu nicht autorisiertem Zugriff auf das Netzwerk führen

Fehlkonfigurationen

- Viele APs werden mit unsicheren Default-Konfigurationen verkauft, um Probleme mit den Kunden zu vermeiden
- Gängige Probleme sind:
  - Default-SSIDs, z.B. tsunami (Cisco), Compaq (Compaq)...
  - WEP in den wenigsten Geräten aktiviert
  - Konfigurations-Interface: Zugriff per SNMP, serieller Schnittstelle, telnet, dem Web und dem WLAN möglich und aktiviert
  - Clientseitige Risiken:
    - SSID und Schlüssel auf den Clients gespeichert
    - Meist in ungesicherter Form in der Windows-Registry
  - Default-Passwörter und User für das Konfigurationsinterface
    - Manchmal sogar mehrere (undokumentierte) User mit Standardpasswörtern

Beispiel Netgear

- 04.06.2004:
  - Firmware von Netgears AP WG602v1 enthält ein undokumentiertes Administrationskonto für das Webinterface (Anmeldename: super, PW: 88635777364)
- 07.06.2004:
  - Die neue Firmware (v1.7.14) enthält wieder ein undokumentiertes Administrationskonto (Anmeldename: superman , PW: 21241036)
- 09.06.2004:
  - Wieder neue Firmware (v1.7.15)
- 18.06.2004:
  - Nochmals neue Firmware, da in der Version 1.7.15 via WLAN und LAN mit Hilfe von SNMP die Management Information Base (MIB) gelesen und die Konfiguration geändert werden konnte. Diese Funktion war nicht dokumentiert und lies sich nicht deaktivieren. Zusätzlich waren die SNMP Community Strings fest auf „public“ und „private“ eingestellt.

Gliederung

- Einführung
- Schutzziele und Risiken
- WLAN
- WLAN-Schwachstellen
- **Maßnahmen zur Absicherung von WLANs**
- Entwicklungstrends im WLAN Sicherheitsbereich
- Fazit

Absicherung - warum?

- Unternehmen ist der Schutzbedarf ihrer Daten meist klar, da Informationen heutzutage eine geschäftskritische Ressource sind
- Aber auch Privatpersonen sollten sich mit der Absicherung ihres WLANs aus folgenden Gründen beschäftigen:
  - Von Hackern verursachte Verbindungskosten müssen vom Betreiber des APs übernommen werden
  - Abmahnungen (und damit verbundene Gebühren) und Klagen gehen an die Adresse des AP-Betreibers
  - In Zivilprozessen muss man als Betreiber die entlastenden Tatsachen selbst nachweisen
  - Bei Strafverfahren müssen die Strafverfolgungsbehörden sämtliche be- und entlastenden Fakten ermitteln, werden aber mit großer Wahrscheinlichkeit eine Hausdurchsuchung vornehmen und das Computerequipment beschlagnahmen

Maßnahmen (1/2)

- Wie viel Aufwand man in die Sicherheit steckt, ist immer abhängig vom konkreten Einsatzszenario und dem Schutzbedarf der Informationen
- Gegen Script-Kiddies und Gelegenheitshacker schützen (den Privatmann) allerdings schon relativ wenige einfache Maßnahmen:
  - Standard SSID ändern und SSID Broadcast am AP abschalten
    - Problem: Windows findet mit Bordmitteln das Netz dann nicht mehr als verfügbares Netz
  - Standard Passwort zur Konfiguration des APs ändern
  - MAC Adress-Filterung am AP einschalten
  - Konfiguration der APs nur über sichere Kanäle zulassen (z.B. auf eine MAC beschränken und nicht aus dem WLAN) und Fernkonfiguration abschalten
  - Höchste mögliche WEP Verschlüsselung einschalten

Maßnahmen (2/2)

- Fortgeschrittene Maßnahmen für Unternehmen
  - Abschottung des drahtgebundenen Netzes durch Firewall und Intrusion Detection System
  - Verwendung einer zusätzlichen/anderen Sicherheitslösung (z.B. VPN, WPA...)
  - Regelmäßige Kontrollen der APs und Clients mittels Funk-LAN-Analysator, Netzwerk-Sniffer und Schwachstellenscanner; hierbei werden auch nicht autorisierte APs gefunden
- Achtung
  - Sieht man von der Verwendung anderer Sicherheitsmaßnahmen ab, bleiben die WEP-Schwachstellen erhalten, auch wenn man die aufgezeigten Maßnahmen durchführt!
  - Gegen Angreifer, die wissen was sie tun, hilft nur der Einsatz eines VPN bzw. der Austausch von WEP mit WPA
  - Denial-of-Service Angriffe können nicht abgewehrt werden!

Gliederung

- Einführung
- Schutzziele und Risiken
- WLAN
- WLAN-Schwachstellen
- Maßnahmen zur Absicherung von WLANs
- **Entwicklungstrends im WLAN Sicherheitsbereich**
- Fazit

Entwicklung der WLAN-Sicherheit

- Aufgrund der Schwäche von WEP gab es eine Vielzahl von (auch nicht viel sichereren) Weiterentwicklungen und Ergänzungen:
  - WEP128
  - WEPplus
  - Fast Packet Keying
  - EAP
  - WEP2
- Eine wirkliche Verbesserung wird erst der neue Standard IEEE 802.11i der Task Group i (TGi) bringen
  - WPA2
    - AES zur Verschlüsselung
    - CCM Protokoll zur Integritätssicherung
    - WPA-PSK (Pre-Shared-Key) trennt Anmeldung am Netzwerk und Verschlüsselung
    - Optional: Authentisierung von Client, Benutzer und AP (über EAP)

Vergleich von WEP, WPA, WPA2

	WEP	WPA	WPA2
Verschlüsselung	RC4	RC4	AES
Schlüssellänge	40 Bit	128 Bit	128 Bit
IV	24 Bit	48 Bit	48 Bit
Paket-Schlüssel	Zusammen-gesetzt	spezielle Funktion	nicht nötig
Daten-Integrität	CRC-32	Michael	CCM
Header-Integrität	-	Michael	CCM
Replay-Angriff	-	IV-Sequenz	IV-Sequenz
Schlüssel-management	-	basierend auf EAP	basierend auf EAP

Gliederung

Fazit

- Sicherheit:
  - Zur Zeit bieten Standardprotokolle keine ausreichende Sicherheit für sicherheitskritische Bereiche
  - Denial-of-Service Angriffe sind sehr einfach
- Empfehlung:
  - WLANs sollten nicht in sicherheitskritischen Bereichen eingesetzt werden, da die Verfügbarkeit nicht sichergestellt werden kann
  - VPN momentan beste Absicherungsmöglichkeit für WLANs, aber auch die aufwendigste
  - Drahtlose Netze müssen in das unternehmensweite Sicherheitskonzept eingebunden werden
- Ausblick:
  - IEEE 802.11i wird einen deutlichen Sicherheitszuwachs für die Masse der Anwender bringen