Willkommen

Advanced Attacks in Shared Media Networks

Open-Router Project
Germany

Was ist ein "Shared Medium"?

- "Geteiltes Übertragungsmedium"
- Traditionelle Netzwerktechnologien:
  - Ethernet, Token Ring, FDDI, ...
- Alle Netzwerkteilnehmer haben Zugriff auf das selbe Medium
  - Übertragungmedium wird geteilt
  - Sendebetrieb eines TLN blockiert gleichzeitig das Senden aller anderen TLN.

Zugriffs-Kontrolle

Weil immer nur ein Teilnehmer das Medium nutzen kann, muss ein Mechanismus für den Medienzugriff existieren!

- Ethernet
  - CSMA/CD
- Token Ring
  - wandernder Token
- FDDI
  - wandernder Token
- WaveLan
  - CSMA/CD
- Bluetooth
  - Master - Slave

Switchen - Die Lösung?

- Switching:
  - Abschottung der einzelnen Stationen durch separate kleine Layer-1 Netze
  - Angriffe können weiterhin auf OSI-Layer 2/3 stattfinden!
    - ARP-Spoofing ...
  - Spezielle Hardware verteilt nur benötigte Daten auf das Medium
- Switching über Luftschnittstelle?
  - Nicht möglich, da nur ein Funkbereich zur Verfügung steht

Luftschnittstelle

- ISM-Band: "Industrial, Scientific and Medical" (ISM)
  - Frequenzbereich zwischen 2,400 GHz und 2,4835 GHz
  - Fast weltweit kostenlos zur Verfügung
  - Benutzt von vielen Shared-Media Technologien
  - WLANs 802.11, HomeRF und Bluetooth
  - Starke Störquellen sind vorhanden!
    - Garagentorsteuerungen, Mikrowellenherde und schnurlose Telefone

Funknetze nach IEEE 802.11

802.11 definiert:

- Physikalische Schicht (PHY)
- MAC-Schicht (WMAC)
- Es gibt drei Übertragungstechniken:
  - Das Frequenzsprungverfahren (FHSS)
  - Spreizbandtechnik (DSSS) {noch keine Produkte}
  - Infrarot-Übertragung (IR) {noch keine Produkte}
- Maximale Sendeleistung:
  - 100 mW (Europa)
    1.000 mW (USA)
- Minimale Kanal-Sprungrate 2,5 Sprünge/Sekunde

802.11a

802.11a:

- High Speed Physical Layer im 5-GHz-Band
- OFDM und der Direct-Sequence-Modulation (DSSS)
- Acht 20-MHz-Kanäle im Frequenzband von 5,15 GHz bis 5,35 GHz
  - zu je 52 Schmalband-Kanälen mit 300 kHz Bandbreite
  - splitting und reassembling mittels OFDM
  - Datenrate pro Kanal 125 kBit/s

802.11b

802.11b:

- Higher Speed Physical Layer im ISM Band
- CCK mittels Spreizbandtechnik
- Fünfzehn Kanäle im Frequenzband
  - Datenrate 5,5 MBit/s, 11 MBit/s - 20 MBit/s
- "Sicherheit" im Standard ,-)
  - (WEP) 40 Bit bzw. 128 Bit mit RC4-Algorithmus
  - Systemidentifikation via MAC gesichert
  - Funksignale entweder im ständigen Frequenzwechsel übertragen oder gescrambelt
- Betriebsarten:
  - Punkt-zu-Punkt-Verbindung
  - Punkt-zu-Multipunkt-Verbindung
  - Access-Point (AP)
  - Ad-Hoc Zugriff

802.11g

802.11g:

- Rückwärtskompatibel zu 802.11b
- Orthogonal Frequency Division Multiplex (OFDM) wie in 802.11a
- Modulationsverfahren Complementary Code Keying (CCK)
- Optional CCK-OFDM und CCK-PBCC
  - Übertragungsraten bis 54 MBit/s

Wireless ATM

WATM:

- Übertragung im 15 bis 38 GHz Band
- QPSK und QAM Modulation
- SDH Bandbreiten E1 bis E3 Mbit/s
  - optional STM-1
  - Datenrate 2 MBit/s - 155 MBit/s
- "Sicherheit" im Preis ,-)
- Protokoll und Signaling-Stack aus der ATM Welt
- Punkt-zu-Punkt Verbindungen

HiperLAN/Access/Link

HiperLAN:

- HiperLAN (High Performance Radio LAN)
- Übertragung im 5 GHz Band
- ETSI-Standard für Ethernet mit 24 MBit/s

HiperACCESS:

- Variante vom HiperLan
  - Wireless Local Loop mit 20 MBit/s

HiperLINK:

- übertragung im 17 GHz Band
- Punkt-zu-Punkt-Verbindung 155 MBit/s

HomeRF

Home Radio Frequency:

- Shared Wireless Access Protocol(SWAP)
- Ebenfalls Übertragung im ISM Band
  - 1 MBit/s 2FSK1 Modulation
  - 2 MBit/s 4FSK Modulation
- Sicherheit:
  - Blowfish Encryption Algorithm
  - 48-Bit Network ID:
  - LZRW3-A Algorithm

Bluetooth

Ziel: Funk-Kommunikation mit geringen Reichweiten

- Max. 15 Meter durch Sendeleistung von 0 dBm
- Durch Einsatz von Verstärkern kann die Entfernung auf 100 Meter erhöht werden
- Ursprünglich eingeführt, um Kabelverbindungen durch Funk zu ersetzen
- Kein Sichtkontakt wie bei IrDA nötig
- Max. acht Endgeräte
  - Zugang zu Laptops, Notebooks, Druckern, Handys ...

Bluetooth-Netz

- Netzaufbau:
  - Bis zu 8 Endgeräte bilden ein Piconet
  - Bis zu 10 Piconets lassen sich vereinen
  - Mehrere Piconets mit überlappenden Funkbereichen bilden ein Scatternet
  - Master-Slave Aufbau
- Betriebsarten:
  - Park-Mode bei asynchronen verbindungslosen Diensten (vergl. UDP)
  - Sniff-Mode

Bluetooth-Beispielnetz

Ein Scatternet bestehend aus drei Piconets:

- Jedes Piconet wird von einem Master gesteuert
  - Master kann sieben aktive Slaves haben
  - Zusätzlich kann er bis zu 255 passive Slaves (im Park-Modus) haben
  - Passive Slaves synchronisieren sich permanent mit dem Master
  - Master kann Slaves in den "Aktive"-(Kommunikations)-Status versetzen
- Sicherheit
  - Der Master bestimmt mittels eines Zufallsgenerators die Abfolge der Frequenzsprünge
  - Alle TLNs eines Piconets haben diese zu verwenden

Bluetooth Protokollstack

Der Bluetooth Protokollstack ist ein ähnliches Chaos wie bei ATM
"Keep-It-Simple" wird von der Industrie selten verstanden...

- Kernprotokolle
  - Cable Replacement
  - Telephony Control Protocols (TCS)
    - Aufgesetzte Transport- und Anwendungsprotokolle
- Baseband-Protokoll,
  - LMP, L2CAP und SDP
- Adaption des Mediums von dem Cable Replacement (RFCOMM)
  - Repräsentation als Serial-Device
    - SLIP, PPP, TCP, UDP, WAP und WAE
- Protokollschnittstelle für die Telefon-API
  - AT-Befehle oder TCS-Binary, abgebildet auf RFCOMM

Die Titanic ist Unsinkbar

http://www.bluetooth.com/news/news.asp?A=2&PID=539

"The differences in operating characteristics between Bluetooth and Wi-Fi also provide a certain level of additional security. While war-drivers are looking for Wi-Fi access points because of the LAN access they provide, Bluetooth technology does not expose a company's entire network through wireless access. Bluetooth has a much smaller perimeter to physically secure compared to 802.11, and it uses a frequency-hopping mechanism of 1,600 hops per second, making the transmissions difficult to tap into..."

- Schwachpunkte:
  - Keine kryptographische Sicherung
  - Sniffer kann von Master Frequenzwechsel mitlesen
  - Durch zu komplexen Aufbau: Implementierungsfehler fast garantiert
  - Angreifer kann Master übernehmen

Angriffe auf das Übertragungsmedium

DoS:

- Einfacher DoS Angriff auf das Medium, um das Netz lahmzulegen
  - Stecknadel im Yellocable
    - Angreifer muss sich Zugang zum Kabel verschaffen
  - Breidbandstörung im ISM Band
    - Angreifer kann remote agieren ,-)

Die Angriffe

- Front-Door Attacken
  - Sniffen von TCP Verbindungen
  - Mitlesen von Klartext-Passwörtern (telnet, pop3...)

Die Angriffe

- Man-In-The-Middle Attacke
  - Bei diesem Angriff schaltet sich der Angreifer zwischen zwei Systeme und ist in der Lage,
    - Daten auszuspähen
    - und zu verändern

Die Angriffe

- Spoofing Attacke
  - Es wird ein gefälschtes IP-Datagram gesendet, dessen Source-Adresse außerdem gefälscht ist, so dass der Empfänger davon ausgeht, dass dieses Paket von einem vertrauenswürdigen System stammt

Die Angriffe

Um einen Angriff auf das Shared-Medium Netz duchführen zu können, muss sich Zugang verschafft werden.

Bei Kabel-Netzen muss auf das Kabel zugegriffen weden, einfacher ist es bei Wave-LANs

Reichweiten und Abhörweiten

Standard	Geschw.	max. Reichweite	max. Reichw. bei max. Speed	Abhörweite
801.11a	6 - 54 MBit	150-300m	10-15m	500-600m
802.11b	5,5-20MBit	300-500m	30-50m	1-1,5 km
802.11g	22&54MBit	300-500m	30-50m	1-1,5 km
Bluetooth	1 MBit	10m	10m	30-50m

Sniffen auf Layer 1

- Vorteile:
  - Gesamtes Spektrum incl. Header und Encoding wird erfasst
  - Schwachstellen und Krypto-Analyse möglich, da wiederkehrendes Signaling und Status-Informationen mitgelesen werden
- Nachteile:
  - Die Physical Protocol Data Unit (PPDU) müssen in Software decodiert werden

Sniffen auf Layer 2

- Vorteile:
  - Duch Monitor-Modi kann das gesammte Spektrum mitgelesen werden
    - z.b. Cisco AiroNET Karte mit RF-Mon Modus
  - Frequenz-Hopping- und andere Kontroll-PDUs werden mitgelesen
  - Guter Kompromiss, um sich Zugang zum Netz zu beschaffen
  - Auswertung mit TCPDUMP möglich
  - Daten wie ARP können mitgelesen werden
    - Wenn APs über MAC-Adressen Filter verfügen, kann eine MAC gespooft werden
- Nachteil:
  - Es können Low-Level Informationen verloren gehen
  - Data Encapsulation für libpcap muss angepasst werden

Beispiel Sniffen auf Layer 2

Ein Wireless LAN 802.11b mit einer Cisco AiroNET Karte 350
Daten sind mit TCPDUMP mitgelesen wurden.

Dafür muss die libpcap an das Format vom Monitor-Modus angepasst werden

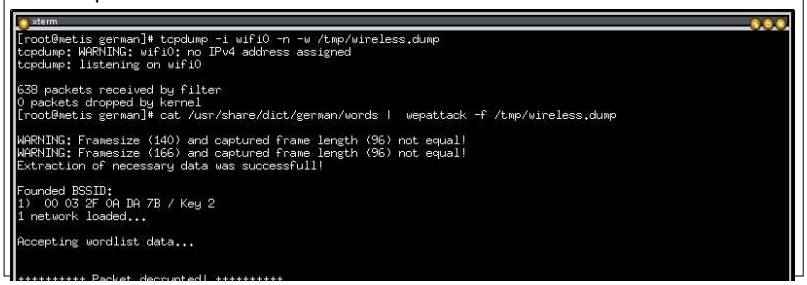
Nun kann das TCPDUMP auch Wireless LANs decodieren und das gesamte

WEP, RC4 und andere Protokolle

Es gibt sehr einfach die Möglichkeit, eine Brute-Force Attacke auf einen Mittschnitt des

Netzwerktraffics auszuführen.
Der Vorteil ist, dass hierbei der Betreiber des Netzwerkes diesen Angriff nicht erkennen kann.

Tool: wepattack



Angriffe auf Layer >2

Da viele APs und Netzwerkhardware immer kürzere Time-to-Market Zeiten haben,
wird auf die Sicherheit das Wireless LAN APs ebensowenig geachtet, trotz WEP.

- Hardware:
  - Longshine LCS-883R-AC-B External WLAN Access Point 22 MBps
- Software:
  - ThreadX ARM7/Green Hills Version G3.0f.3.0c from Express Logic Inc.

tftp
tftp> connect 192.168.108.48
tftp> get config.img
Received 780 bytes in 1.0 seconds
tftp> quit

Angriffe auf Layer >2

Eine Auswertung der gezogenen Datei ergibt:

[~]/-\>strings config.img
DNXLABAP01 <- name of the AP
root <- name of the superuser
XXXXXX123 <- password from superuser
DNXLABLAN <- ssid
Abbauleistung <- secret for WEP
7890abcdef <- secret for WEP2 ..

Audit Tools

- TCPDUMP
  - http://www.tcpdump.org/
  - Dekodiert den Netzwerkverkehr
  - Kommt mit fast allen Medien klar (FDDI, Ethernet, DHLC, ISDN, PPP, WLAN, ATM ...)
    - Kann bei Shared-Medien den gesamten Verkehr mitlesen
    - Dekodiert auch Verkehr im Tunnel (PPTP, PPPoE, GRE, 802.1q ...)
  - Mächtige Skript-Spache
  - Frei verfügbar
    - BSD Lizenz

Audit Tools

- KISMET
  - http://www.kismetwireless.net
  - Sniffer und Audit-Tool
  - Besonders beliebt bei War-Driver
  - 802.11a & 801.11b Support
  - Multiple Paketquellen
  - Channel Hopping
  - IP-Block Detection / CDP Auswertung
  - Erkennt APs im Default-Mode
    - Offen mit Default PW
  - Laufzeit WEP-Decoding
  - Mapping und GPS Support
    - für Karten von WLANs
  - Frei verfügbar
    - GPL Lizenz

Prognose

- War-Driving wird immer beliebter
  - Nur die Kosten halten von Wireless ATM und andren Funknetzen ab
- Angriffe auf Bluetooth sehr wahrscheinlich
- TCPDUMP, libpcap, DSNIFF und andere UNIX-Tools lassen sich sehr leicht an neue Medien anpassen
- Audit und Kontrolle sind wichtig
- Wireless LANs sind immer öffendlich zugänglich, daher muss eine weitere Sicherung duchgeführt werden
- Leichte Adaption an neue Verfahren und Protokolle, wenn IP benutzt wird
- Angriffe hängen z. Zt. nur vom Hardware-Preis ab