

# **Mobile Security**

IIR Internet Security Forum  
12.–14. November 2002

**Enno Rey & Michael Thumann**

- Mobile Security
- Sicherheit bei IPSec
- Empfehlungen
- Wireless Security
- Empfehlungen

- People move. Networks don't.

oder

- Wie ‚mobile Technologien‘ unsere Wahrnehmung von Netzen und Netzwerksicherheit verändern sollten.

- Traditionelle Netzwerke werden räumlich und logisch erweitert durch:
- Mobile User, die [meist IPsec-basierte] VPN-Verbindungen in Unternehmensnetze aufbauen
- Mobile Netzwerk-Segmente auf Basis von 802.11 [Wireless LANs]
- Mobile Devices, die nur temporär an Netze angeschlossen werden [*intermittently connected clients*: Laptops, PDAs, Handys]

- Wir sprechen heute über:
- Sicherheitsprobleme üblicher IPsec-Installationen
- Sicherheitsprobleme von Wireless LANs
- Natürlich über Gegenmaßnahmen

- Wir sprechen (aus Zeitgründen) *nicht* über Sicherheitsprobleme mobiler Devices...
- ... möchten hier aber einige Anregungen (mit-) geben:
- Wer von Ihnen betreibt eine ‚Quarantäne-Station‘ für Mitarbeiter-Laptops?
- In wessen Policy wird der Umgang mit PDAs geregelt?
- <http://www.blackhat.com/presentations/bh-usa-02/higbee-davis/higbeedavis-bh-us-02-phone.ppt>
- <http://www.blackhat.com/presentations/win-usa-02/johansson-winsec02.ppt>
- [csrc.nist.gov/publications/drafts/draft-sp800-48.pdf](http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf)

- Vernachlässigung der Sicherheit der (mobilen) Endpunkte
- Fehlendes Verständnis grundlegender IPsec-Funktionalität beim zuständigen Personal
- Großflächiger Einsatz von *preshared keys*
- Überfrachtete Erwartungen [=> Konfiguration nach Funktionalitäts-, nicht nach Sicherheitskriterien]
- Missachtung von *Segregation of Duties*



## Vernachlässigung der Sicherheit der (mobilen) Endpunkte

- Endpunkte von VPN-Verbindungen sitzen virtuell im LAN => sie sollten auch ebenso behandelt werden (oder: „was nützt mir x-fache Authentifizierung mit State-of-the-Art Technologie, wenn der Endpunkt über weitere aktive Netzwerkverbindungen verfügt und dort Filesharing-Tools laufen?“)
- VPN-Komponenten sind... nicht immer ausgereift...

# Vernachlässigung der Sicherheit der (mobilen) Endpunkte

SecurityFocus HOME Vulns Archive: Vendor - Microsoft Internet Explorer

Address: http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl

by vendor | by title | by keyword | by bugtraq id | by cve id

Vendor: Cisco  
Title: Select One  
Version: Any

- \* 2002-09-19: Cisco IP Phone 7960 Firmware TFTP Authentication Weakness
- \* 2002-09-19: Cisco IP Phone 7960 Unsigned Content Weakness
- \* 2002-09-18: Cisco VPN 5000 Client Buffer Overrun Vulnerabilities
- \* 2002-09-18: Cisco Mac OS VPN 5000 Client Password Disclosure Vulnerability
- \* 2002-09-05: Cisco VPN Client NETBIOS TCP Packet Denial Of Service Vulnerability
- \* 2002-09-05: Cisco VPN Client Password Disclosure Vulnerability
- \* 2002-09-05: Cisco VPN Client TCP Filter Information Leakage Vulnerability
- \* 2002-09-05: Cisco VPN Client Distinguished Name Validation Vulnerability
- \* 2002-09-05: Cisco VPN Client Predictable Sequence Number Vulnerability
- \* 2002-09-03: Multiple Cisco VPN 3000 Vulnerabilities
- \* 2002-09-03: Cisco VPN 3000 Series Concentrator User Credential Disclosure Vulnerability
- \* 2002-09-03: Cisco VPN 3000 Series Concentrator Certificate Credential Disclosure Vulnerability
- \* 2002-09-03: Cisco Internal Group Authentication External Access Vulnerability
- \* 2002-09-03: Cisco VPN 3000 Series Concentrator XML Filter Misconfigured Access Vulnerability
- \* 2002-09-03: Cisco HTTP Interface Long Request Denial Of Service Vulnerability
- \* 2002-09-03: Cisco VPN 3000 Series Concentrator Web Interface Information Disclosure Vulnerability
- \* 2002-09-03: Cisco VPN 3000 Series Concentrator Posted User Credential Denial Of Service Vulnerability
- \* 2002-09-03: Cisco VPN 3000 Series Concentrator ISAKMP Denial of Service Vulnerabilities
- \* 2002-09-03: Cisco VPN 3000 Series Concentrator Client Authentication Denial Of Service Vulnerability
- \* 2002-09-03: Cisco VPN Concentrator SSH Banner Device Information Leakage Vulnerability
- \* 2002-09-03: Cisco VPN 3000 Concentrator IPSEC Tunnel Denial of Service Vulnerability
- \* 2002-09-03: Cisco VPN Concentrator FTP Banner Device Information Leakage Vulnerability
- \* 2002-09-03: Cisco VPN Concentrator HTTP Error Page Device Information Leakage Vulnerability
- \* 2002-09-03: Cisco VPN Concentrator PPTP Client Remote Denial Of Service Vulnerability
- \* 2002-08-22: Microsoft Network Share Provider SMB Request Buffer Overflow Vulnerability
- \* 2002-08-12: Cisco VPN Client Zero Length IKE Packet Denial Of Service Vulnerability
- \* 2002-08-12: Cisco VPN Client IKE Security Parameter Index Payload Buffer Overflow Vulnerability
- \* 2002-08-12: Cisco VPN Client IKE Packet Excessive Payloads Vulnerability
- \* 2002-08-08: iSCSI Insecure Configuration File Permissions Information Disclosure Vulnerability
- \* 2002-08-07: Cisco VPN 5000 Concentrator Plaintext Password
- \* 2002-07-30: OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability

ARM YOURSELF  
Against Security Threats

FREE TRIAL

Sign up for a **FREE** Trial of  
QualysGuard Vulnerability  
Assessment now:

[First Name]  
[Last Name]  
[Email Address]  
[Phone Number]  
[Company]  
[Select a State or Province]  
[Zip]  
[Select a Country]

Submit

qualys

- Oder sollten wir fragen:
- Wer von Ihnen setzt IPsec-basierte VPNs ein?
- Falls ja... was ist IKE? XAuth? Hybrid Mode? [einiges davon verwenden Sie mit hoher Wahrscheinlichkeit]
- Können Sie uns erklären, warum der *aggressive mode* potentiell unsicherer ist als der *main mode*... oder was das überhaupt ist?
- Ist der *hybrid mode* sicherer als Zertifikat-basierter *main mode* ... oder warum setzen Sie dann diesen oder jenen ein?
- Sie setzen keinen von beiden ein, sondern den *aggressive Mode* mit *preshared key* [und variablen Endpunkten]? Na dann...

## Eine übliche IPsec-Installation verläuft in etwa so:

[beteiligt sind Admin A und Admin B an einem Freitag gegen 19:00 Uhr]

- Admin A: Läuft's endlich?
- Admin B: Nein. Ich versteh' aber nicht, weshalb nicht.
- Admin A: Probier' doch mal den Parameter X.
- Admin B: Funktioniert auch nicht... ich könnte aber 'mal Parameter Y verwenden.
- Admin A: Wieso?
- Admin B: Weiß ich auch nicht... war nur so'ne Idee.
- Admin A: Ich teste mal... jetzt geht's!!
- Admin B: Kapierst Du, weshalb es nun funktioniert?
- Admin A: Nein, ich speicher' aber jetzt die Einstellungen (und fass es bloss nie wieder an!)
- Admin B: Na dann... schönes Wochenende!

Noch immer werden IPsec-Verbindungen überwiegend mithilfe sog. *preshared keys* authentifiziert [weil's so schön einfach ist... und IPsec doch eh' schon so komplex...]

Dabei...

- skalieren diese schlecht
- haben auch sonst die meisten schlechten Eigenschaften von Paßwörtern...
- werden sie je nach Device [z.B. bei Cisco-Routern] im Klartext abgespeichert (und diese Devices werden dann per Telnet/TFTP remote-administriert...)
- und dann gibt es ja auch noch Sniffing und Bruteforcing

```
ca C:\WINDOWS\System32\cmd.exe - perl ikecrack.pl 10.1.1.85.500
S:\Daten\ERNW\UORTR\UI\IIR\UPNUN\CM>perl ikecrack.pl 10.1.1.85.500
Looking for Initiator : 10.1.1.85.500
Header IPs 10.1.1.85.500 10.1.3.1.500:
Matching Header 10.1.1.85.500 10.1.3.1.500
Init
tcookie_i : edc9e9af144486a8
tcookie_r : 0000000000000000
xchg type: 04
Aggressive Mode - Continue
ikelen : 280
SA_i : 00000001000000010000002c0101000100000024010100008001000580020001800300
0180040002800b0001000c000400015180
KE_i : cf6dd6e659949368d790658df7bc0b4cf440b6cd1bcb946404085499af45b50d702ac8
cccf6e9b4621ed96c6dfbca1bf890fd1695f2225d824aeb05ba10b56848151233fbb63539484b659f
5f1d0a900aa800922f025750fb05e6f588d9f9a01440f377fcb9e0b85842da7a948058d510088ae8
d459a2a1332a13c091f2cd7022
KE : cf6dd6e659949368d790658df7bc0b4cf440b6cd1bcb946404085499af45b50d702ac8ec
cf6e9b4621ed96c6dfbca1bf890fd1695f2225d824aeb05ba10b56848151233fbb63539484b659f
1d0a900aa800922f025750fb05e6f588d9f9a01440f377fcb9e0b85842da7a948058d510088ae0d4
59a2a1332a13c091f2cd7022
nonce_i : 0ad0fe7d5059a11f53ab7b7e2hc7940bf828c2fe875faf052ec066e7071c49d1
ID_i : 010000000a010155

Header IPs 10.1.3.1.500 10.1.1.85.500:
Reply Header? 10.1.3.1.500 10.1.1.85.500
Resp
tcookie_i : edc9e9af144486a8
tcookie_r : 1626863636df7966
xchg type: 04
Aggressive Mode - Continue
ikelen : 351
SA_r : 00000001000000010000002c0101000100000024010100008001000580020001800400
0280030001800b0001000c000400015180
KE_r : 3f7189035a31640fb3c46ca42ce0b2b9d64f23fa2974896252d2e8fbaa9ff6bfec77fe
12476ae4feda6e1415b972d0cbea31baf062dfd0d074c3c68c7bd46044bc2c0f2f9457c35507470c
bec47f8d0564ca4b964b1aa915ee312f4e29ac64ca68caf64521e679eea130945bc686472a67d041
3524fb1720758f3d24418bb8ca
KE : 3f7189035a31640fb3c46ca42ce0b2b9d64f23fa2974896252d2e8fbaa9ff6bfec77fe12
476ae4feda6e1415b972d0cbea31baf062dfd0d074c3c68c7bd46044bc2c0f2f9457c35507470c
c47f8d0564ca4b964b1aa915ee312f4e29ac64ca68caf64521e679eea130945bc686472a67d04135
24fb1720758f3d24418bb8ca
ID_r : 021101f45461752e65726e772e6465
nonce_r : 7c15851939995262369341699774bdfdeaeaf1e
HASH_r : 71e953cf8db30f7c65d73dcc2e154828

Header IPs 10.1.1.85.500 10.1.3.1.500:
Header IPs 10.1.1.85.500 10.1.3.1.500:
Header IPs 10.1.3.1.500 10.1.1.85.500:

Starting Crack Process.
Responder Sent MD5 HASH_R : 71e953cf8db30f7c65d73dcc2e154828
Character 1 Done : Time 0 seconds
Character 2 Done : Time 0 seconds
Character 3 Done : Time 10 seconds
```

- IKE PSK Cracker – dictionary, hybrid, brute
- Einfache Implementierung – Nur Aggressive mode
- Setzt IETF HASH\_R Berechnung (RFC 2409) voraus
- Nur MD5 HMAC – 93K kps auf 1.8Ghz P4
- PERL Skript, daß HMAC PerlMod und tcpdump –nxq -s 500 Output voraussetzt

```
Take Command/32
File Edit Apps Options Utilities Help

[s:\daten\vernu\vortraege\iir\vpn und wireless]perl ikeprober.pl
Usage:
  -s SA [encr:hash:auth:group]
  -k x|auser value|user value [KE repeatedX times|ascii_supplied|hex_supplied]
  -n x|auser value|user value [Nonce repeatedX times|ascii_supplied|hex_supplied]
  -v x|auser value|user value [VendorID repeatedX|ascii_supplied|hex_supplied]
  -i x|auser value|user|raup value [ID repeatedX|ascii_supplied|hex_supplied|Hex_IPV4]
  -h x|auser value|user value [Hash repeatedX|ascii_supplied|hex_supplied]
  -spi xx [SPI in 1byte hex]
  -r x [repeat previous payload x times]
  -d ip_address [Create Init packet to dest host]
  -eac [Nortel EAC transform - responder only]
  -main [main mode packet instead of aggressive mode - logic will be added later for correct init/respond]
  -sa_test 1|2|3|4 [1=86400sec life, 2=0xffffffff life, 3=192 group attribs, 4=128 byte TLV attrib]
  -rand randomize cookie
  -transforms x [repeat SA transform x times]
ikeprober.pl V1.13 -- 02/14/2002, updated 9/25/2002
  By: Anton T. Rager - arager.com

Error: Must supply options

[s:\daten\vernu\vortraege\iir\vpn und wireless]

22.10.02 12:39:46 Load: 50%
```

- Command-line Utility zum Bau von IKE Paketen
- Unterstützt die gängigen IKE Optionen
- Nützlich, um Cisco/PGPNet/Safenet Implementierungen zu finden
- Perl basierend, benötigt NetCat
- Kann auch für das Auffinden von gültigen Benutzernamen benutzt werden

- Diese Tools sind (noch) experimentell. Beim nächsten Security-Forum könnten sie mit GUIs, herstellerspezifischen Menüs, konfigurierbaren Timeouts etc. verfügbar sein...

- VPNs sollen Remote-Zugriff *ermöglichen*, leicht konfigurierbar & administrierbar sein, am besten wenig kosten... und, ach ja, auch noch sicher sein  
=> oft wird schon die Konfiguration an solchen Kriterien ausgerichtet

```
crypto isakmp key xyz address 217.227.0.0 255.255.0.0 no-xauth  
crypto isakmp key xyz address 217.83.0.0 255.255.0.0 no-xauth  
crypto isakmp key xyz address 80.131.0.0 255.255.0.0 no-xauth
```

!! bei kaum einem anderen Sicherheits-Instrument wird in der alltäglichen Administration so sehr *Funktionalität* fokussiert!

Eine Firewall ist eine Firewall ist eine Firewall...

- ... und **kein** Crypto-Device
- => beide Funktionalitäten auf einer Komponente zu vereinen, stellt ein **gravierendes Design-Problem** dar,
- denn: Kompromittierung des VPN-Gateways ist dann = Kompromittierung der Firewall!
- Die IPsec-“Forschung“ befindet sich (s.o.) noch „in den Anfängen“...

- Behandeln Sie VPN-Clients (mindestens) wie LAN-Clients hinsichtlich User-Verhalten [qua Policy], Patchlevel, Virenschutz etc.
- Einsatz guter Authentifizierungsmechanismen [Zertifikate oder Token-Verfahren/Hybrid Mode]
- Trennung von Firewalls und VPN- Gateways
- VPN-Gateways sollten 'untrusted' sein => sie gehören in dedizierte, gesicherte Segmente

- Typische Sicherheitsprobleme beim Einsatz von Wireless LANs:
- die Funkreichweite (also „physische Erweiterung“ des Netzes) wird unterschätzt... oder überhaupt nicht bedacht...
- Access Points werden nicht wie Netzwerkdevices behandelt (Problem wird verschärft durch Multifunktionalität & Default-Einstellungen vieler APs)
- WLANs sind durch und durch *shared media*
- 802.11-Sicherheitsmechanismen werden nicht genutzt
- 802.11-Sicherheitsmechanismen sind meist unzureichend

- **beträgt bei einem handelsüblichen Cisco Access Point (Aironet 350, typical @ 100-mW transmit power setting with 2.2 dBi diversity dipole antenna)**

Indoor:

130 ft (39.6 m) @ 11 Mbps

350 ft (107 m) @ 1 Mbps

Outdoor:

800 ft (244 m) @ 11 Mbps

2000 ft (610 m) @ 1 Mbps

([http://www.cisco.com/en/US/products/hw/wireless/ps45/products\\_data\\_sheet09186a008009247c.html](http://www.cisco.com/en/US/products/hw/wireless/ps45/products_data_sheet09186a008009247c.html))

- Können Sie diesen Bereich überwachen oder überblicken?
- Haben Sie den Standort Ihrer APs danach optimiert?

- Sie verfügen über Management-Zugänge [SNMP, HTTP, Telnet]...
- über die ihr “Verhalten im Netz” gesteuert wird
- und die wiederum mit (Default-) Passwörtern “gesichert” sind oder werden können...
- => Access Points sollten dieselbe Sicherheitsbehandlung wie alle anderen Devices erfahren  
[Policy-Einbindung, Zugriffskontrolle, Audit etc.]

# Funktionalität eines typischen Access Points:

```
[erey@mobile vortrag]$ sudo nmap -sU -p 1-200 192.168.96.16
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
```

```
Interesting ports on (192.168.96.16):
```

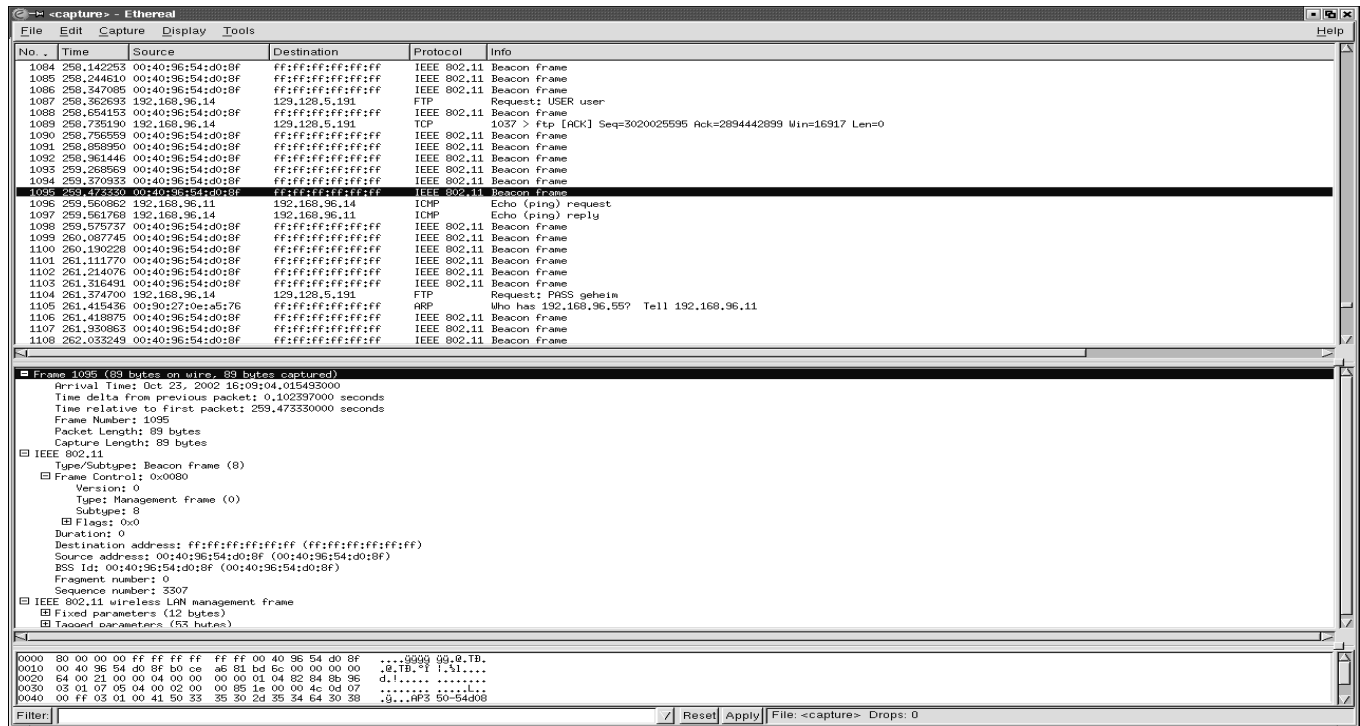
```
(The 194 ports scanned but not shown below are in state:  
  closed)
```

Port	State	Service
53/udp	open	domain
67/udp	open	dhcpserver
69/udp	open	tftp
75/udp	open	priv-dial
137/udp	open	netbios-ns
161/udp	open	snmp

```
Nmap run completed -- 1 IP address (1 host up) scanned in 23  
  seconds
```

# WLANs sind *shared media*!

- => im sog. *RF Monitor[ing] Mode* kann der komplette Verkehr aller Wireless-Clients mitgelesen werden [und – sollte der AP an einen Hub kaskadiert sein – natürlich auch der aller anderen Stationen an diesem Hub...]



The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of captured packets. The selected packet (No. 1095) is expanded to show its details:

- Arrival Time: Oct 23, 2002 16:09:04.015493000
- Time delta from previous packet: 0.102397000 seconds
- Time relative to first packet: 259.473330000 seconds
- Frame Number: 1095
- Packet Length: 89 bytes
- Capture Length: 89 bytes
- IEEE 802.11
  - Type/Subtype: Beacon frame (8)
  - Frame Control: 0x0080
  - Versions: 0
  - Type: Management frame (0)
  - Subtype: 8
  - Flags: 0x0
  - Duration: 0
  - Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  - Source address: 00:40:96:54:d0:8f (00:40:96:54:d0:8f)
  - BSS Id: 00:40:96:54:d0:8f (00:40:96:54:d0:8f)
  - Fragment number: 0
  - Sequence number: 3307
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters (12 bytes)
  - Tagged parameters (53 bytes)

The packet bytes pane shows the raw hex and ASCII data:

```
0000 80 00 00 00 ff ff ff ff ff ff ff ff 00 40 96 54 d0 8f ...9999 99,0.TB.
0010 00 40 96 54 d0 8f b0 ce a5 81 bd 8c 00 00 00 00 .0.TB.* !.51...
0020 04 00 21 00 00 04 00 00 00 01 04 82 84 8b 96 d.....
0030 03 01 07 05 04 00 02 00 00 85 1e 00 00 4c 07 .....
0040 00 ff 03 01 00 41 50 33 35 30 2d 35 34 64 30 38 .g...HP3 50-54008
```

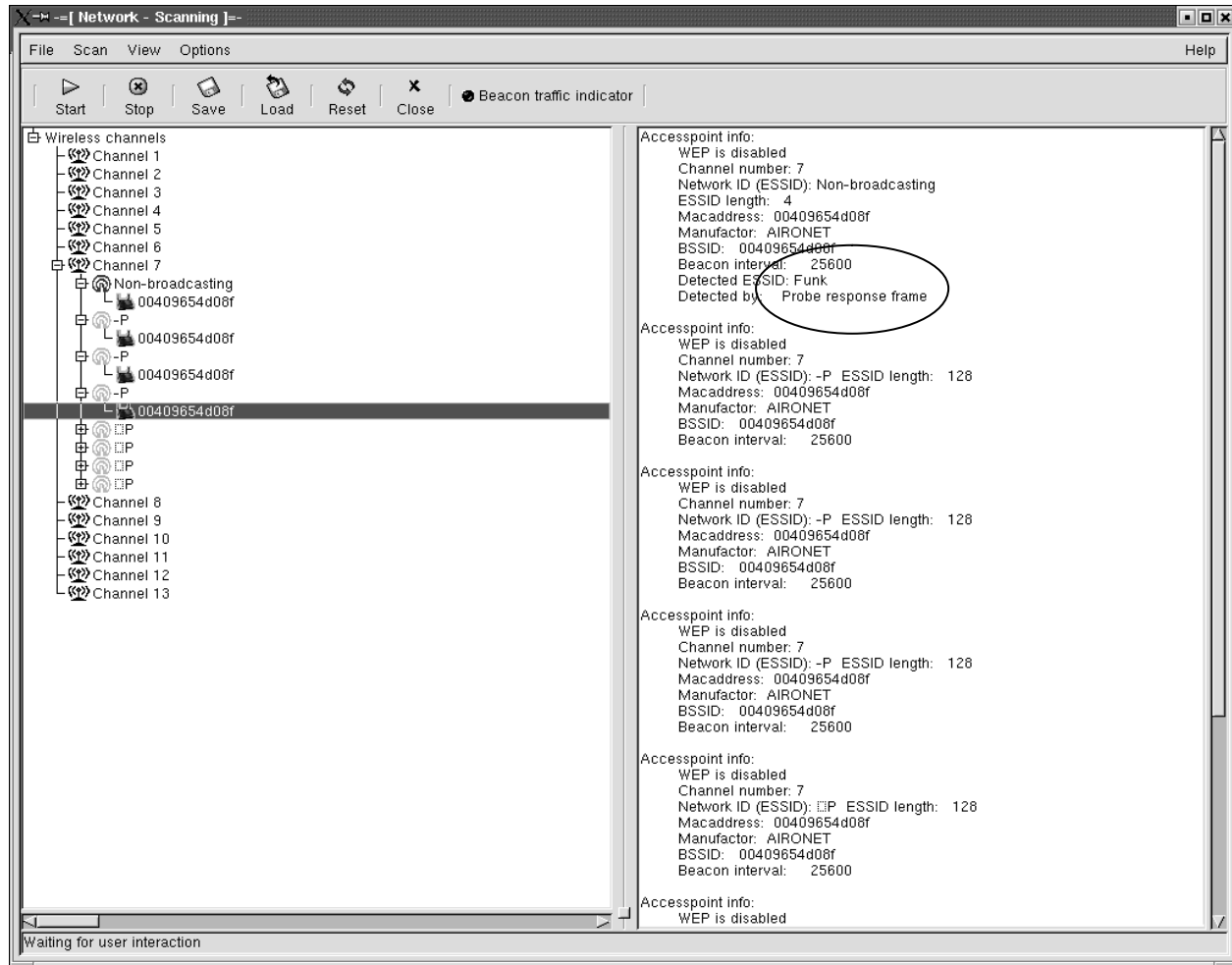
Die Arbeit eines Angreifers kann üblicherweise zumindest erschwert werden durch

- den Einsatz von MAC-basierten ACLs
- die Unterdrückung von Broadcast-SSIDs
- die Aktivierung von WEP
- => Sie sollten diese Mechanismen einsetzen... aber sich dabei bewusst sein, dass...

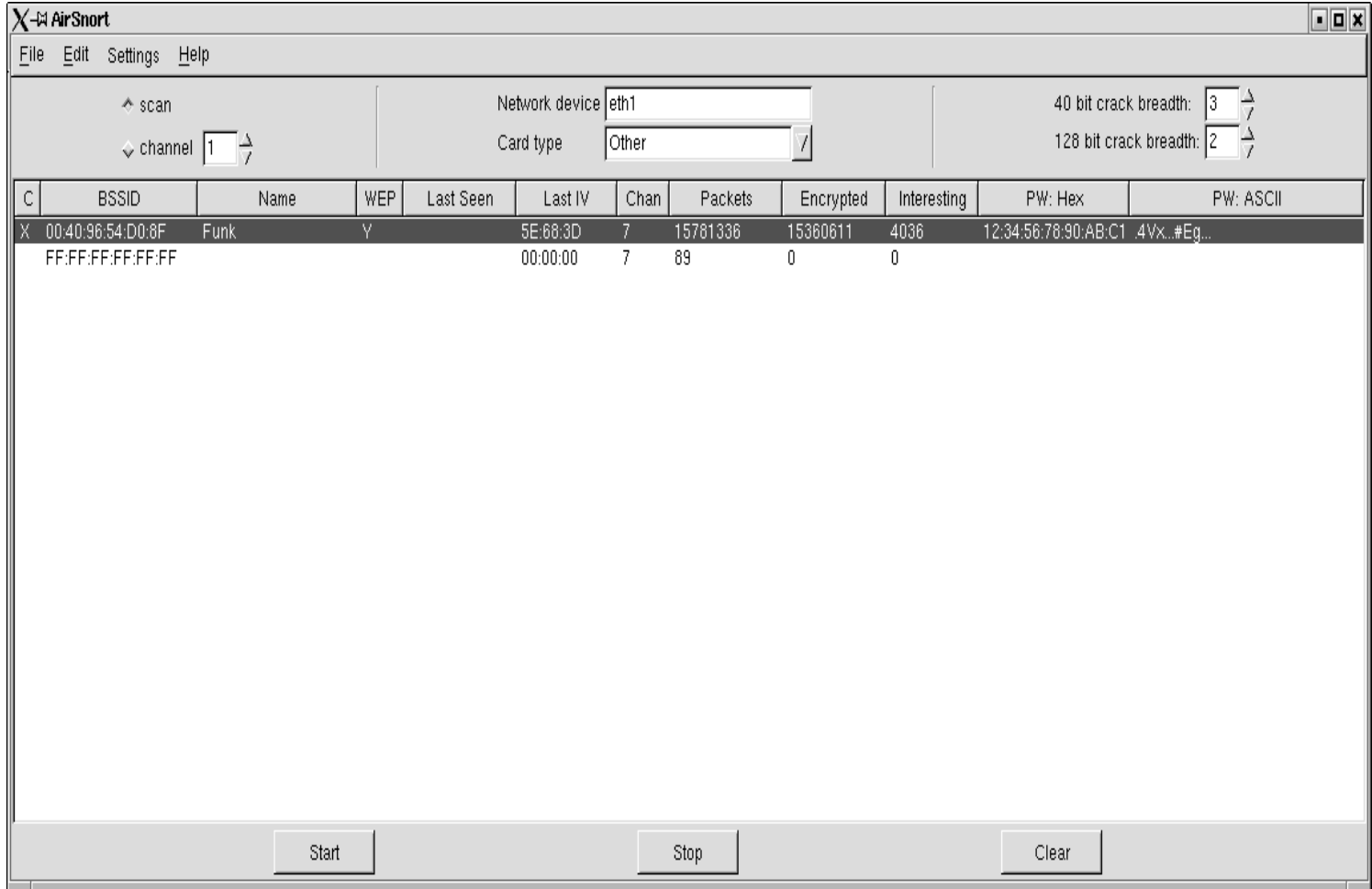
- MAC-basierte ACLs können (nach Mitlesen von Management-Verkehr) durch Spoofing von MAC-Adressen getäuscht werden:

```
[erey@mobile vortrag]$ sudo ifconfig eth1 hw ether 08:15:47:11:00:00
Password:
[erey@mobile vortrag]$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:15:47:11:00:00
          inet addr:1.1.1.1  Bcast:1.255.255.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10  errors:364  dropped:0  overruns:0  frame:364
          TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:100
          RX bytes:791 (791.0 b)  TX bytes:0 (0.0 b)
          Interrupt:3  Base address:0x100
```

# SSID und Kanal können (selbst bei Einsatz von WEP) durch geeignete Sniffer schnell ermittelt werden:



# ... WEP ist (unabhängig von der Schlüssellänge!) leicht zu brechen...



The screenshot shows the AirShort application window. The interface includes a menu bar (File, Edit, Settings, Help), a control panel with 'scan' and 'channel' (set to 1) buttons, and configuration fields for 'Network device' (eth1) and 'Card type' (Other). It also features '40 bit crack breadth' (3) and '128 bit crack breadth' (2) spinners. The main area is a table with the following data:

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASCII
X	00:40:96:54:D0:8F	Funk	Y	5E:68:3D	7	15781336	15360611	4036	12:34:56:78:90:AB:C1	4Vx...#Eg...	
	FF:FF:FF:FF:FF:FF			00:00:00	7	89	0	0			

At the bottom of the window are three buttons: 'Start', 'Stop', and 'Clear'.

- Installationspunkte von Access Points hinsichtlich Funkradius optimieren (ggf. mithilfe geeigneter Antennen)
- Access Points & Clients immer in eigene Segmente (Subnetze); diese sind potentiell *untrusted*
- Access Points als schützenswerte Devices begreifen + immer an Switches kaskadieren, nie an Hubs
- Sicherheitsfeatures nutzen (MAC-ACLs, WEP, kein SSID-Broadcasting), idealerweise 802.1x
- WEP bietet keine ausreichende Sicherstellung von Vertraulichkeit, Integrität und Authentizität der übertragenen Daten => Einsatz von IPsec, SSH o.ä.

## Weiterführende Links:

- <http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>
- [http://www.iss.net/wireless/WLAN\\_FAQ.php](http://www.iss.net/wireless/WLAN_FAQ.php)
- <http://ikecrack.sourceforge.net>

## ■ Fragen?

- Danke für die Aufmerksamkeit!