



The information security provider



Wireless Intrusion Detection

Matthias Hofherr, matthias@atsec.com





Agenda

- Methoden
- Anforderungen
- Architektur
- NIDS/WIDS
- Datenkorrelation
- Channel Hopping
- Ortung
- Wireless Intrusion Prevention
- Hardware
- Aufwände

Methoden

- Wireless IDS (WIDS) unterstützen verschiedene Erkennungsmethoden
 - Signaturbasierte Erkennung
 - Updates für Signaturen nötig, keine Zero-Day Erkennung ...
 - Anomalieerkennung
 - Unpräzise Alarme, z.T. hohe False Positive Raten
 - Varianten:
 - Statistische Anomalieerkennung
 - Protokollbasierte Anomalieerkennung

Die besten Ergebnisse liefern WIDS, die eine Kombination dieser Methoden einsetzen

Anforderungen

- Ein WIDS muss verschiedene Ereignisse erkennen:
 - Wireless Scanner
 - Angriffe auf 802.11 Netzwerke
 - Hijacking von MAC Adressen
 - Denial-of-Service Angriffe
 - Rogue Access Points / Evil Twins
 - Policy Überwachung

```
Network List (SSID)
Name      T W Ch Packets Flags IP Range  Size
-----
WLAN      A Y 001  4  0.0.0.0  0B
WLAN unsicher GU  A N 013  1  0.0.0.0  0B
WLAN1     A N 006  1  0.0.0.0  0B
WLANOM    A N 011 23  0.0.0.0 112B
WLAN100g  A N 011  5  0.0.0.0  0B
wanH@Hs  A Y 011  5  0.0.0.0  70B
WIFI_EDV  A Y 011 24  0.0.0.0  1k
Wlanetou  A Y 006  1  0.0.0.0  0B
ZLAN      A Y 011 12  0.0.0.0  0B
ZenkNet   A Y 001 19  0.0.0.0  0B
AFGB      A Y 001  1  0.0.0.0  0B
A[ASAMUDAGAKACAV[AQMH[A P N --- 1  0.0.0.0  0B
A[AVAXA]AATAIADAYALA_AYA P N --- 5  0.0.0.0  0B
A[ASL_ARANAXA[AAPAYAVIBA P N --- 3  0.0.0.0  0B
b[ks]n5g  A N 011  2  0.0.0.0  0B
default   A Y 006  1  0.0.0.0  0B
default   A N 009  2  0.0.0.0  0B
default   A Y 006 59  0.0.0.0  3k
default   A N 006 35 P14 192.168.1.1 104B
default   A Y 006  9  0.0.0.0  0B

Lat 49.172 Lon 11.806 Alt 1841.1f Spd 29.253m/h Hed 80.001 Ffx 3D 83% (+) Down
Status
Found new network "FRITZ!Box Fon WLAN" bssid 00:04:0E:41:71:A5 WEP Y Ch 6 @ 22.00 mbIt
Found new network "WLAN" bssid 00:30:F1:FD:46:92 WEP Y Ch 1 @ 22.00 mbIt
Found new network "sercon" bssid 00:80:33:38:51:85 WEP Y Ch 6 @ 11.00 mbIt
Found new network "cno ssid:" bssid 00:0B:6B:30:2F:D1 WEP Y Ch 13 @ 54.00 mbIt
Battery: 68% 596523h50m26s
```

MAC	SSID	Ch.	Speed	Vendor	Type	En.	SNR	Sig.	S.	First Se.
0001E30782CD	Meisterschaft	6	11 Mb...		AP	WEP	3	3	3	1759.44
0001E3418331	ConnectionPoint	11	80 Mb...		AP	WEP	9	9	9	1759.44
000F64C28D9	Ethernal	10	36 Mb...	Linksys	AP	WEP	39	39	39	1759.44
0030F1E16A2B	WLAN	11		Action	AP	WEP	22	24	24	1759.44

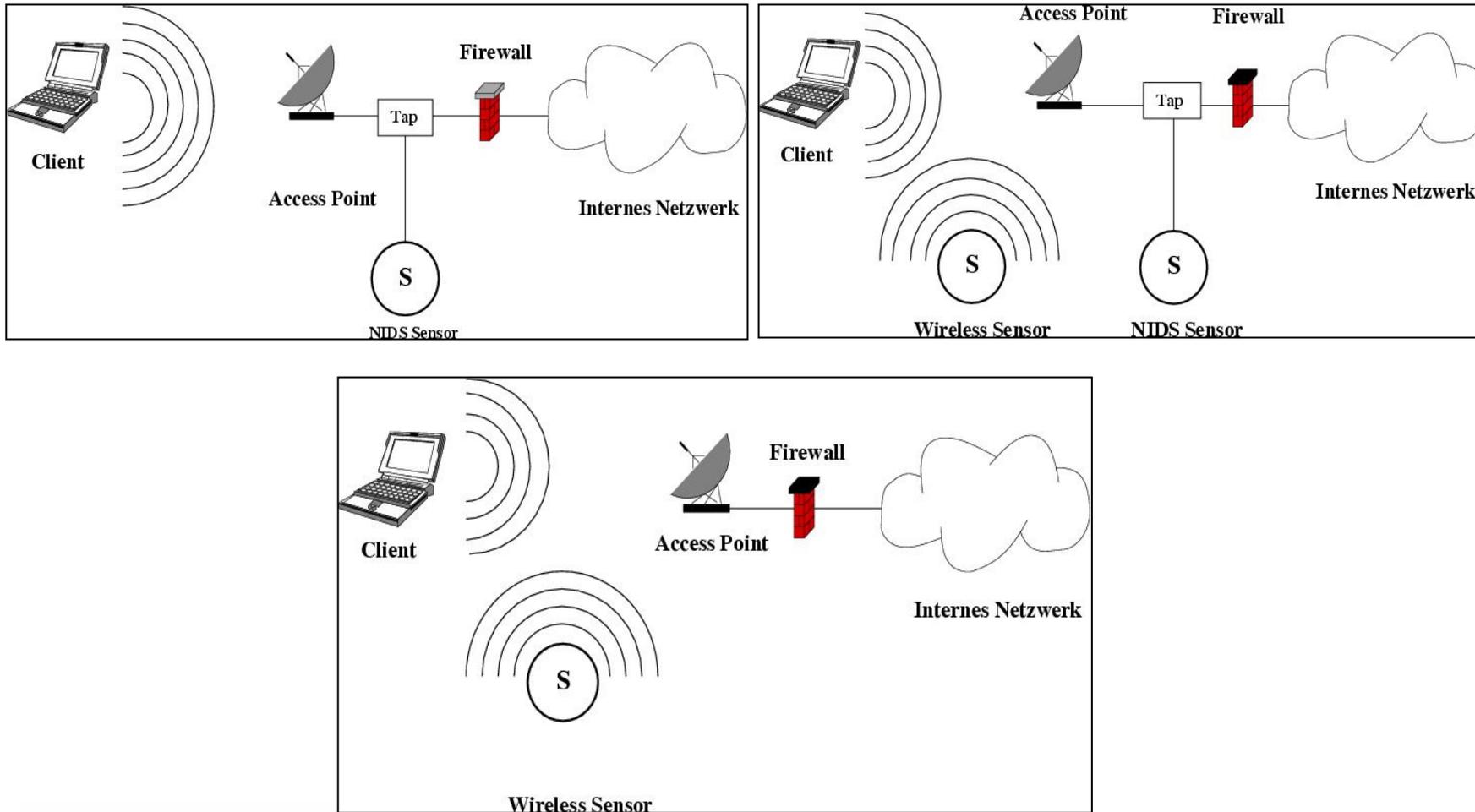


Architektur

- Systemaufbau
 - Dezentral/Standalone
 - Einzelne Einheit, die als Sensor und Auswerteeinheit fungieren
 - Zentral
 - Zentraler Server zur Auswertung und Konfiguration, verteilte Sensoren
 - Datenauswertung:
 - Kann auf Sensor (bessere Hardware nötig) oder auf Server (komplette Kopie des Datenstroms nötig) erfolgen
 - Sensornutzung:
 - Dedizierter Sensor
 - Integriert in Access Point
 - Access Point, der bei Bedarf zu dedizierten Sensor mutiert

- Integration von NIDS und WIDS
 - Vorteile: weniger Hardware, kein eigener Abgreifpunkt für NIDS nötig
 - Problem: Entschlüsselung von
 - WEP: möglich mit bekanntem Schlüssel
 - WPA(2): außerhalb des AP schwer umsetzbar
 - VPNs: nicht möglich, wenn „hinter“ AP terminiert
 - In Access Point integrierte WIDS haben hier Vorteile, da Verschlüsselung am AP terminiert

NIDS / WIDS





Datenkorrelation

- Zentrale Datenauswertung mit Korrelation
 - WIDS muss offene Netzwerk-Schnittstellen bieten
 - Datenlieferung an SEM/SIM, Abgleich mit
 - NIDS
 - Logfiles (OS, Applikationen)
 - Antivirus-Systemen
 - Firewalls / Router
 - AAA Server
 - ...
 - Macht nur Sinn bei zeitsynchronen Systemen



Channel Hopping

- Nicht alle verfügbaren Kanäle können gleichzeitig überwacht werden
 - Channel Hopping schaltet Sensor wechselweise auf die verschiedenen Kanäle
 - Jeder Kanal kann nur eine bestimmte Zeit überwacht werden
 - Verhalten bei Angriffserkennung
 - Schaltet weiter
 - Bleibt länger auf Kanal
 - Schaltet zweite Empfangseinheit auf Kanal



Ortung

- Angreifer soll nicht nur erkannt, sondern auch geortet werden
- Manuelle Ortung mit einem tragbarem Gerät und Richtantenne kann sehr zeitaufwändig sein
- Verschiedene automatisierte Methoden:
 - Nächstgelegener Sensor
 - Triangulation
 - RF Fingerprinting
- Kann auch zum Tracking von Equipment/Personen eingesetzt werden



Wireless Intrusion Prevention

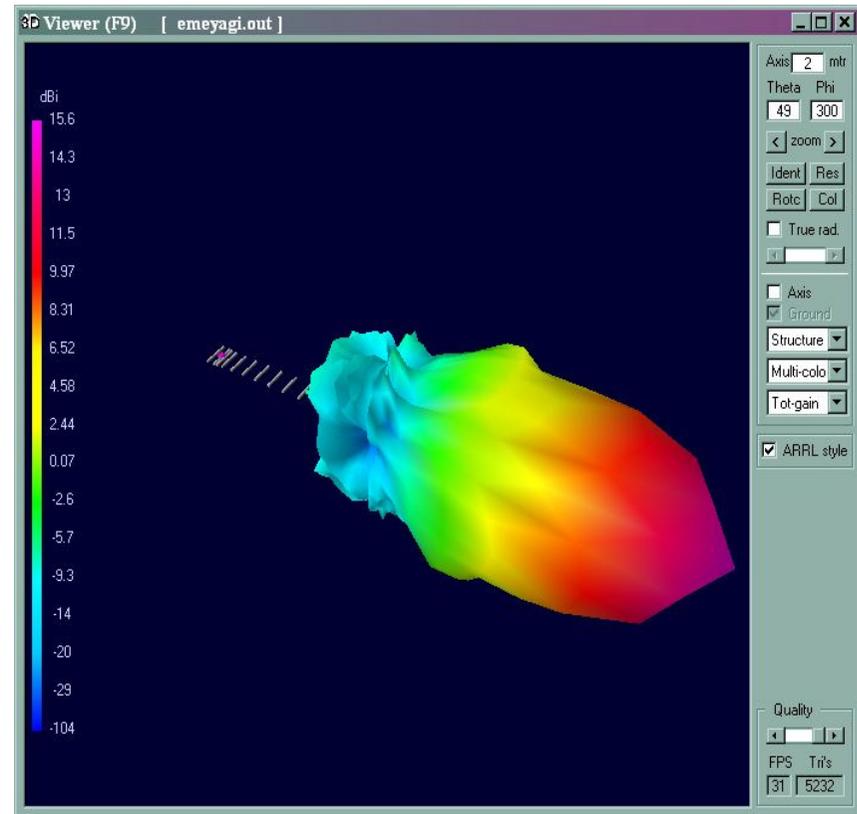
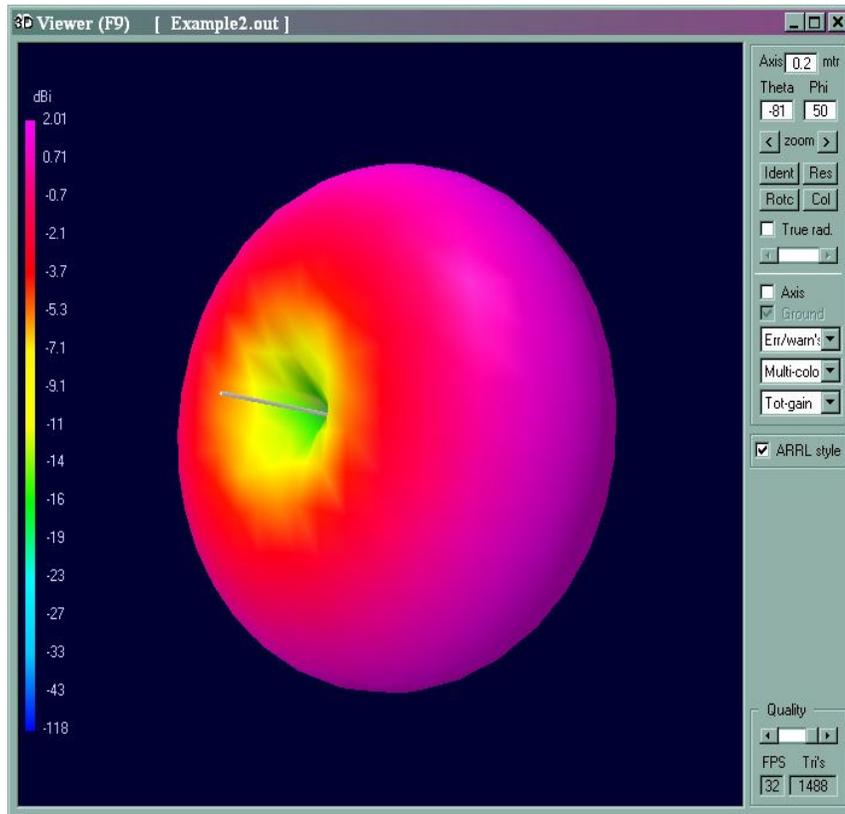
- Das System leitet aktive Gegenmaßnahmen ein, um einen Angriff zu stoppen
- Verschiedene Methoden
 - Jamming des Kanals
 - Isolierung des Angreifers durch Deauth/Disassoc
 - Blockierung durch Firewall (Shunning)
 - Switch Port deaktivieren
- Alle Methoden haben Nebeneffekte, die vorher in der Evaluationsphase geprüft werden sollten



Hardware

- Sensorenauswahl
 - Eigenbau (meist OpenSource) oder COTS
 - Unauffällige Kleinstbauweise oder PC-Größe
 - Getarnte Sensoren (z.B. als Rauchsensor)
 - Einsatz externer Antennen
 - Konnektoren
 - Richtstrahler oder Rundstrahler (Reichweite)
 - Antenne bestimmt Sensordichte

Antennen



Copyright atsec information security, 2006



Aufwände

- „Turnkey Solutions“ sind ein Marketing-Mythos
- Kein IDS (insbesondere kein IPS) kann einfach angeschaltet und ohne größeren Aufwand betrieben werden
- Aufwände (OPEX) sollten vorher kalkuliert werden, bevor die Liste gescheiterter IDS Projekte Zuwachs erhält
- Vor Einführung eines WIDS sollte eine Wireless Policy erstellt werden
- Das WIDS muss in eine (hoffentlich) bestehende Notfallplanung und in bestehende Sicherheitsprozesse integriert werden

Fragen ?





Vortragender

Dipl.-Inf. (FH)

Matthias Hofherr

Senior Security Consultant

atsec information security GmbH
Steinstr. 80
D - 81667 München
www.atsec.com

Tel: +49 (0) 89 442 498 30
Fax: +49 (0) 89 442 498 31
Mobile: +49 (0) 172 86 72 518
e-mail: matthias@atsec.com