



The information security provider



---

## Wireless Intrusion Detection

Matthias Hofherr, [matthias@atsec.com](mailto: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

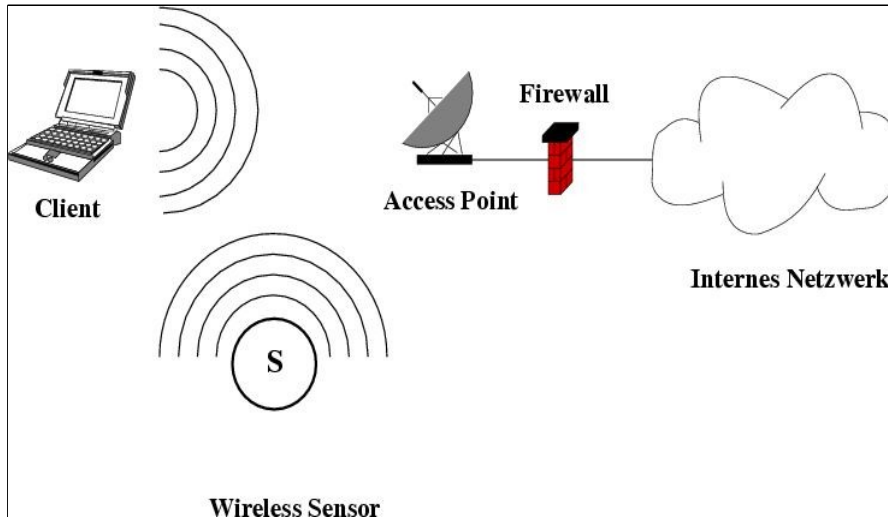
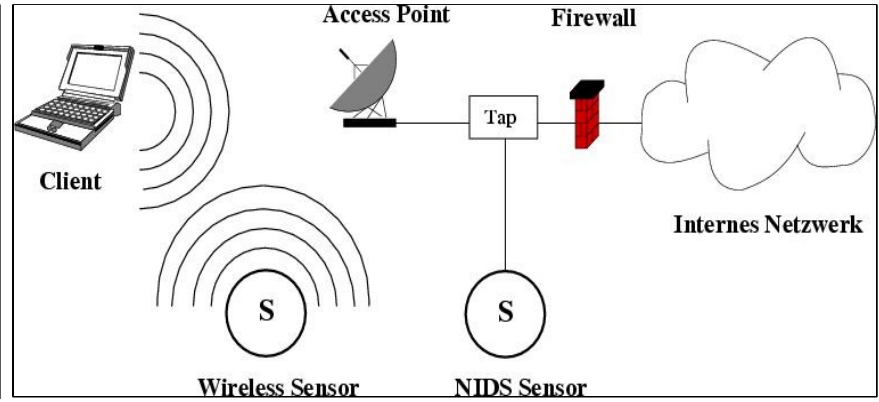
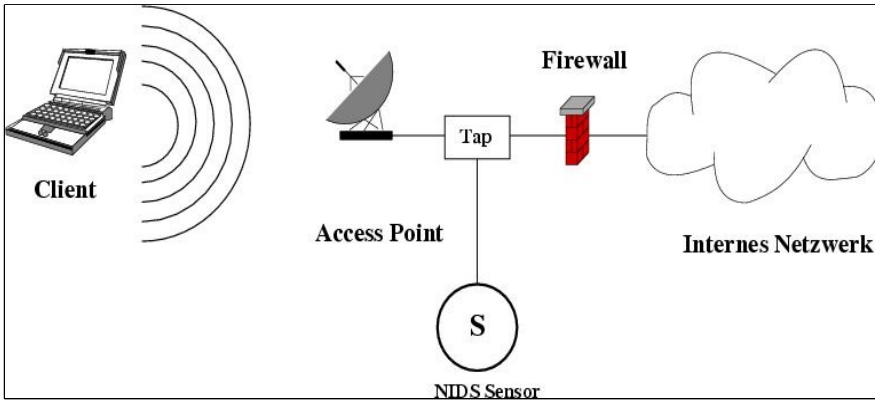
```
Network List - (SSID)
Name      T W Ch  Packets  Flags  IP Range  Size
-----
WLAN      A Y 008   4    0.0.0.0  08
WLAN unsicher GU  A N 013   1    0.0.0.0  08
WLAN1     A N 006   1    0.0.0.0  08
WLAN2     A N 011  23    0.0.0.0 1128
WLAN3     A N 011   5    0.0.0.0  08
WLAN4     A Y 011   5    0.0.0.0  708
WLAN5     A Y 011  24    0.0.0.0  1k
WLAN6     A Y 006   1    0.0.0.0  08
WLAN7     A Y 011  12    0.0.0.0  08
WLAN8     A Y 001  19    0.0.0.0  08
WLAN9     A Y 001   1    0.0.0.0  08
WLAN10    A Y 001   1    0.0.0.0  08
WLAN11    A Y 001   1    0.0.0.0  08
WLAN12    A Y 001   1    0.0.0.0  08
WLAN13    A Y 001   1    0.0.0.0  08
WLAN14    A Y 001   1    0.0.0.0  08
WLAN15    A Y 001   1    0.0.0.0  08
WLAN16    A Y 001   1    0.0.0.0  08
WLAN17    A Y 001   1    0.0.0.0  08
WLAN18    A Y 001   1    0.0.0.0  08
WLAN19    A Y 001   1    0.0.0.0  08
WLAN20    A Y 001   1    0.0.0.0  08
WLAN21    A Y 001   1    0.0.0.0  08
WLAN22    A Y 001   1    0.0.0.0  08
WLAN23    A Y 001   1    0.0.0.0  08
WLAN24    A Y 001   1    0.0.0.0  08
WLAN25    A Y 001   1    0.0.0.0  08
WLAN26    A Y 001   1    0.0.0.0  08
WLAN27    A Y 001   1    0.0.0.0  08
WLAN28    A Y 001   1    0.0.0.0  08
WLAN29    A Y 001   1    0.0.0.0  08
WLAN30    A Y 001   1    0.0.0.0  08
WLAN31    A Y 001   1    0.0.0.0  08
WLAN32    A Y 001   1    0.0.0.0  08
WLAN33    A Y 001   1    0.0.0.0  08
WLAN34    A Y 001   1    0.0.0.0  08
WLAN35    A Y 001   1    0.0.0.0  08
WLAN36    A Y 001   1    0.0.0.0  08
WLAN37    A Y 001   1    0.0.0.0  08
WLAN38    A Y 001   1    0.0.0.0  08
WLAN39    A Y 001   1    0.0.0.0  08
WLAN40    A Y 001   1    0.0.0.0  08
WLAN41    A Y 001   1    0.0.0.0  08
WLAN42    A Y 001   1    0.0.0.0  08
WLAN43    A Y 001   1    0.0.0.0  08
WLAN44    A Y 001   1    0.0.0.0  08
WLAN45    A Y 001   1    0.0.0.0  08
WLAN46    A Y 001   1    0.0.0.0  08
WLAN47    A Y 001   1    0.0.0.0  08
WLAN48    A Y 001   1    0.0.0.0  08
WLAN49    A Y 001   1    0.0.0.0  08
WLAN50    A Y 001   1    0.0.0.0  08
WLAN51    A Y 001   1    0.0.0.0  08
WLAN52    A Y 001   1    0.0.0.0  08
WLAN53    A Y 001   1    0.0.0.0  08
WLAN54    A Y 001   1    0.0.0.0  08
WLAN55    A Y 001   1    0.0.0.0  08
WLAN56    A Y 001   1    0.0.0.0  08
WLAN57    A Y 001   1    0.0.0.0  08
WLAN58    A Y 001   1    0.0.0.0  08
WLAN59    A Y 001   1    0.0.0.0  08
WLAN60    A Y 001   1    0.0.0.0  08
WLAN61    A Y 001   1    0.0.0.0  08
WLAN62    A Y 001   1    0.0.0.0  08
WLAN63    A Y 001   1    0.0.0.0  08
WLAN64    A Y 001   1    0.0.0.0  08
WLAN65    A Y 001   1    0.0.0.0  08
WLAN66    A Y 001   1    0.0.0.0  08
WLAN67    A Y 001   1    0.0.0.0  08
WLAN68    A Y 001   1    0.0.0.0  08
WLAN69    A Y 001   1    0.0.0.0  08
WLAN70    A Y 001   1    0.0.0.0  08
WLAN71    A Y 001   1    0.0.0.0  08
WLAN72    A Y 001   1    0.0.0.0  08
WLAN73    A Y 001   1    0.0.0.0  08
WLAN74    A Y 001   1    0.0.0.0  08
WLAN75    A Y 001   1    0.0.0.0  08
WLAN76    A Y 001   1    0.0.0.0  08
WLAN77    A Y 001   1    0.0.0.0  08
WLAN78    A Y 001   1    0.0.0.0  08
WLAN79    A Y 001   1    0.0.0.0  08
WLAN80    A Y 001   1    0.0.0.0  08
WLAN81    A Y 001   1    0.0.0.0  08
WLAN82    A Y 001   1    0.0.0.0  08
WLAN83    A Y 001   1    0.0.0.0  08
WLAN84    A Y 001   1    0.0.0.0  08
WLAN85    A Y 001   1    0.0.0.0  08
WLAN86    A Y 001   1    0.0.0.0  08
WLAN87    A Y 001   1    0.0.0.0  08
WLAN88    A Y 001   1    0.0.0.0  08
WLAN89    A Y 001   1    0.0.0.0  08
WLAN90    A Y 001   1    0.0.0.0  08
WLAN91    A Y 001   1    0.0.0.0  08
WLAN92    A Y 001   1    0.0.0.0  08
WLAN93    A Y 001   1    0.0.0.0  08
WLAN94    A Y 001   1    0.0.0.0  08
WLAN95    A Y 001   1    0.0.0.0  08
WLAN96    A Y 001   1    0.0.0.0  08
WLAN97    A Y 001   1    0.0.0.0  08
WLAN98    A Y 001   1    0.0.0.0  08
WLAN99    A Y 001   1    0.0.0.0  08
WLAN100   A Y 001   1    0.0.0.0  08
```

```
Network Scanner - [2005020175943]
MAC      SSID      Ch.  Speed  Vendor  Type  En.  SNR  Sig.  S.  First Se.
-----
0001E30732CD  Meisterschaft  8  11 Mb...  AP  WEP  3  3  1759.44
0001E3413331  ConnectionPoint  11  36 Mb...  AP  WEP  9  9  1759.44
000F64CCBD9  Ethereal  10  36 Mb...  Linksys  AP  WEP  39  39  1759.44
0030F1E16A2B  WLAN  11  Acton  AP  WEP  22  24  24  1759.44
```

- 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



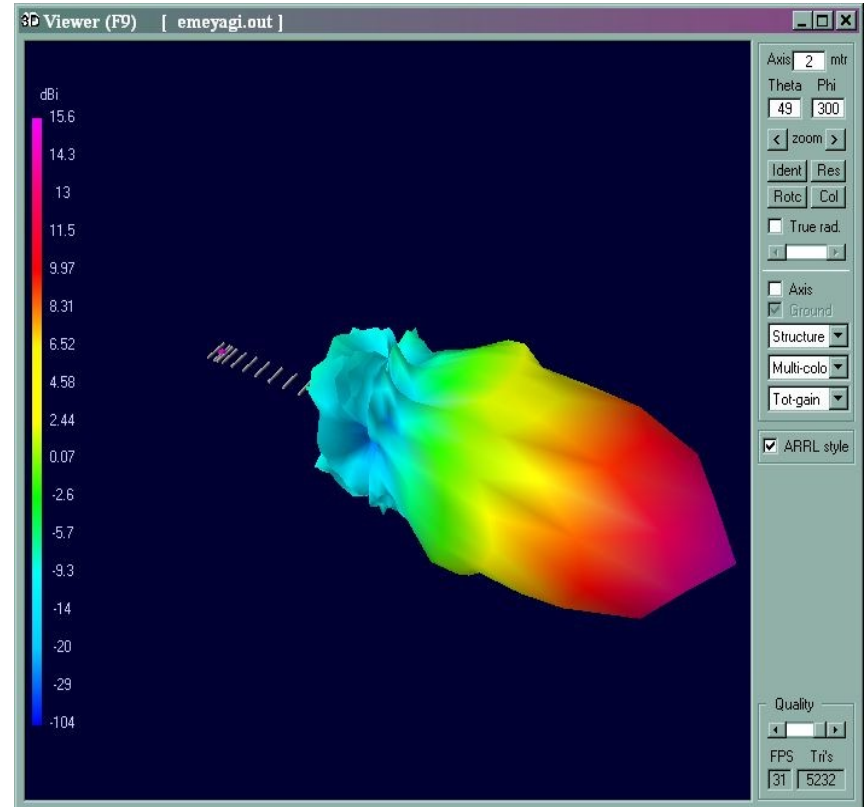
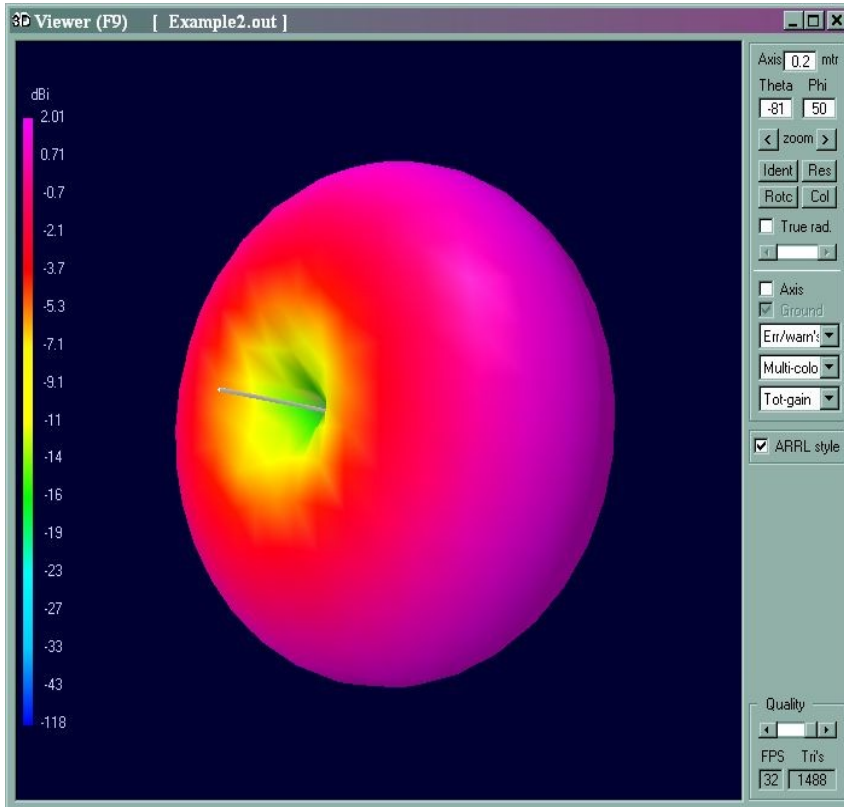
# Wireless Intrusion Prevention

---

- 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

- 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





# 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