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

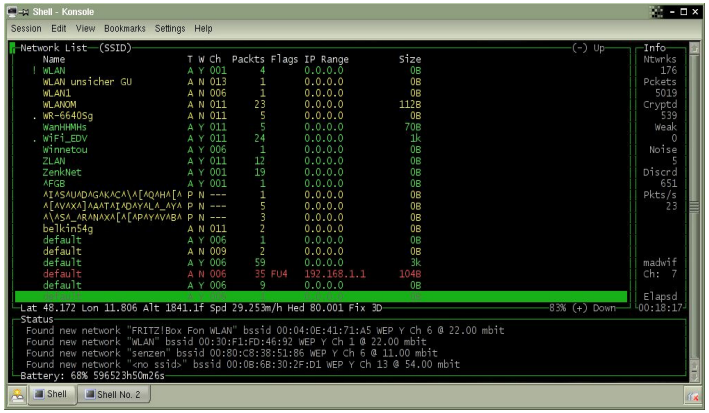
Methoden

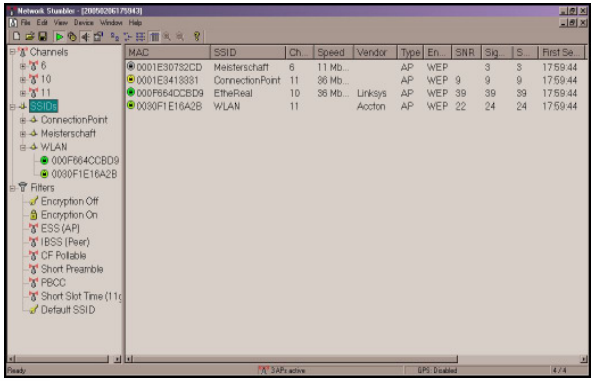
- Wireless IDS (WIDS) unterstützen verschiedene Erkennungsmethoden
  - Signaturbasierte Erkennung
    - Updates für Signaturen nötig, keine Zero-Day Erkennung …
  - Anomalieerkennung
    - Unpräzise Alarme, z.T. hohe False Positive Raten
    - Varianten:
      - Statistische Anomalieerkennung
      -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





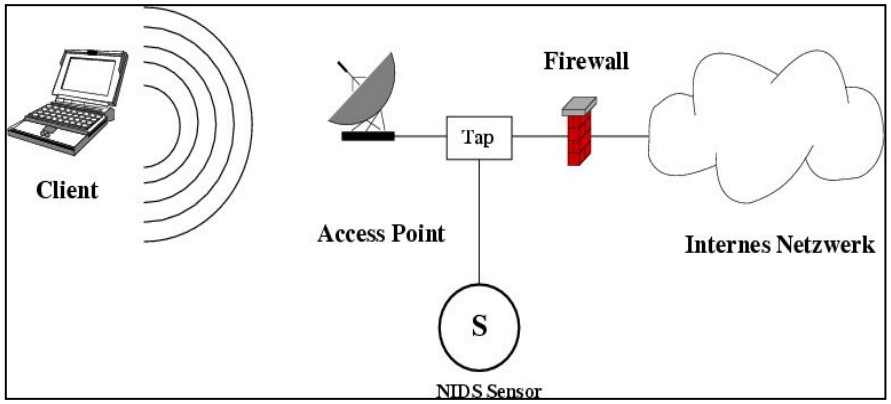
Architektur

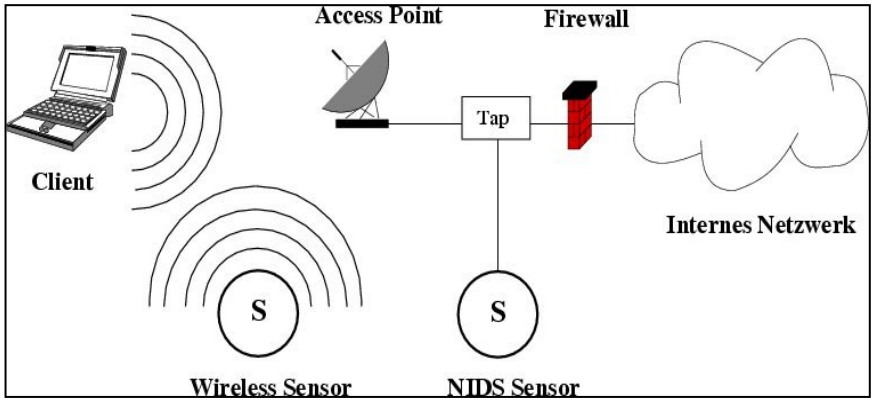
- Systemaufbau
  - Dezentral/Standalone
    - Einzelne Einheit, die als Sensor und Auswerteeinheit fungieren
  - Zentral
    - Zentraler Server zur Auswertung und Konfiguration, verteilte Sensoren
  - Datenauswertung:
    - Kann auf Sensor (bessere Hardware nötig) oder auf Server (komplette Kopie des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

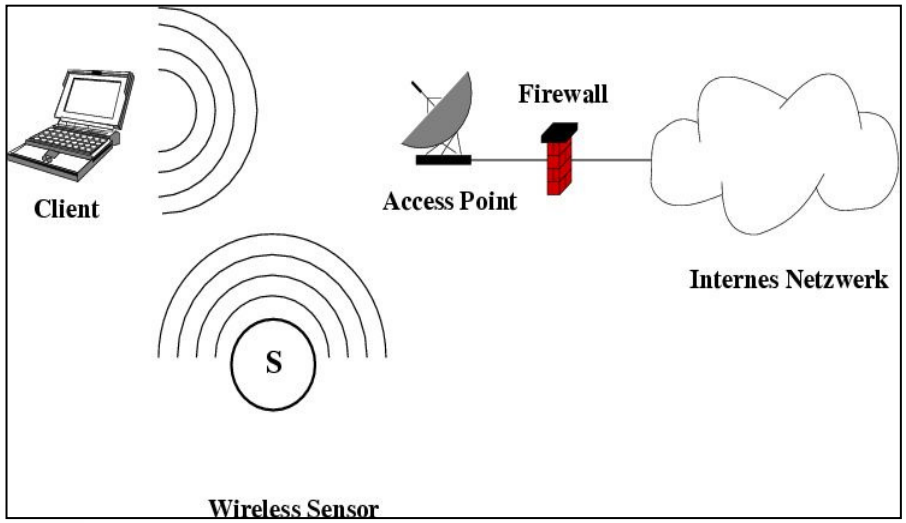
NIDS / WIDS

- 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

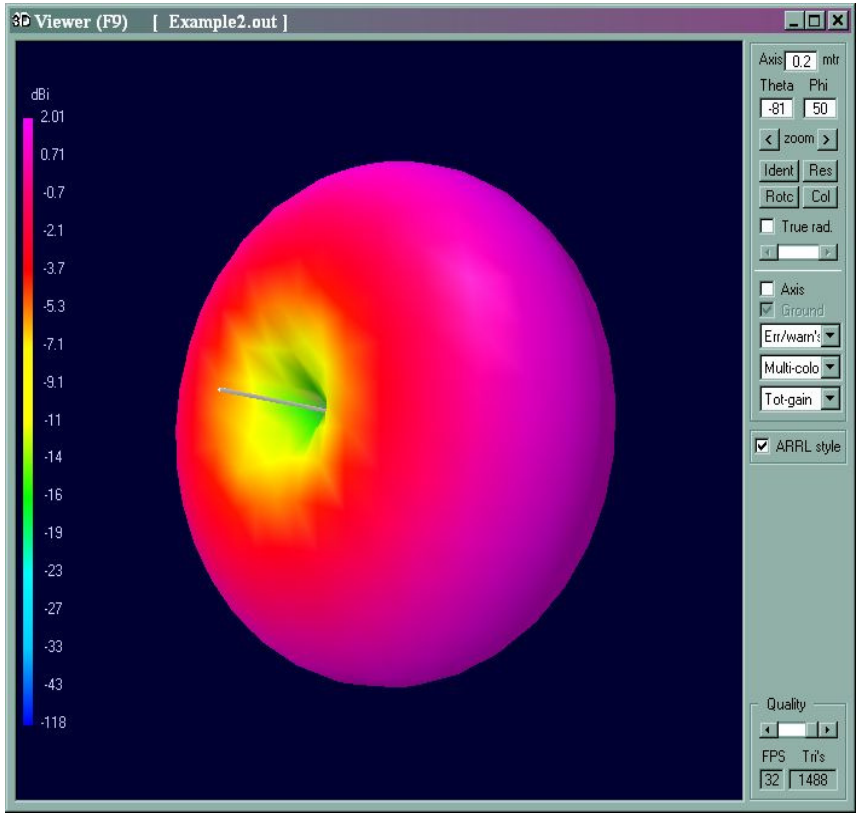
Wireless Intrusion Prevention

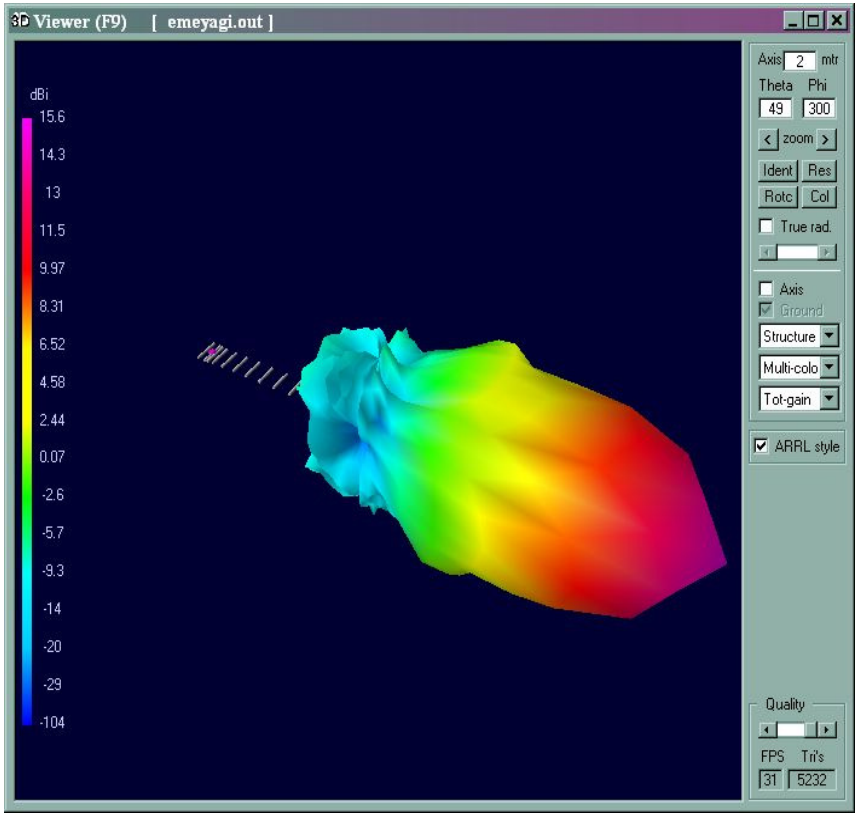
- Das System leitet aktive Gegenmaßnahmen ein, um einen Angriff zu stoppen
- Verschiedene Methoden
  - Jamming des Kanals
  - Isolierung des Angreifers durch Deauth/Disassoc
  - Blockierung durch Firewall (Shunning)
  - Switch Port deaktivieren
- Alle Methoden haben Nebeneffekte, die vorher in der Evaluationsphase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





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