

Mobile Honeypot

Theodor Nolte

Hochschule für Angewandte Wissenschaften Hamburg
Fakultät Technik und Informatik
Department Informatik

26. November 2010

1 SKIMS

2 Mobile Honeypot

- Honeypot
- Mobile Honeypot



Bundesministerium
für Bildung
und Forschung

*Schichtenübergreifendes kooperatives Immunsystem
für **mobile**, mehrseitige **Sicherheit***

Freie Universität  Berlin



Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

escrypt
Embedded Security

DFN
CERT

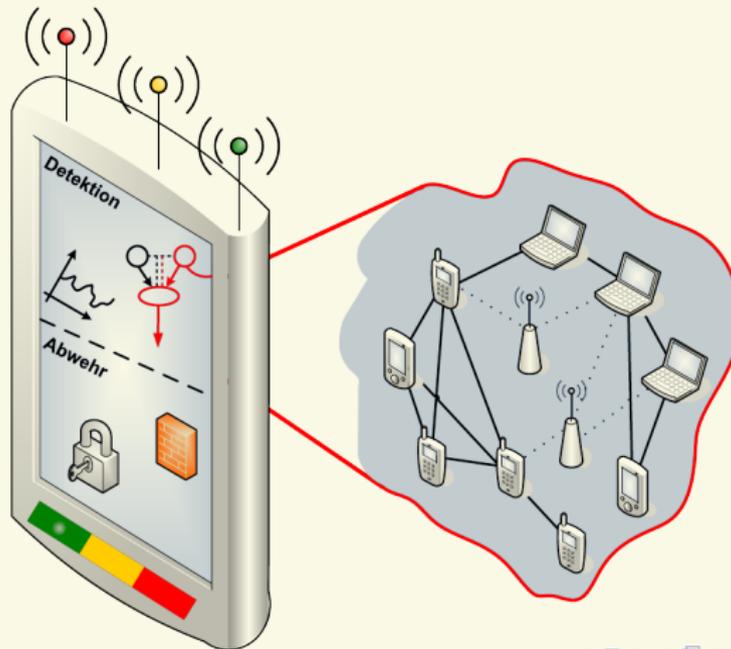
NEC

university-logic

SKIMS

Angriffe

- erkennen
- abwehren



Gliederung

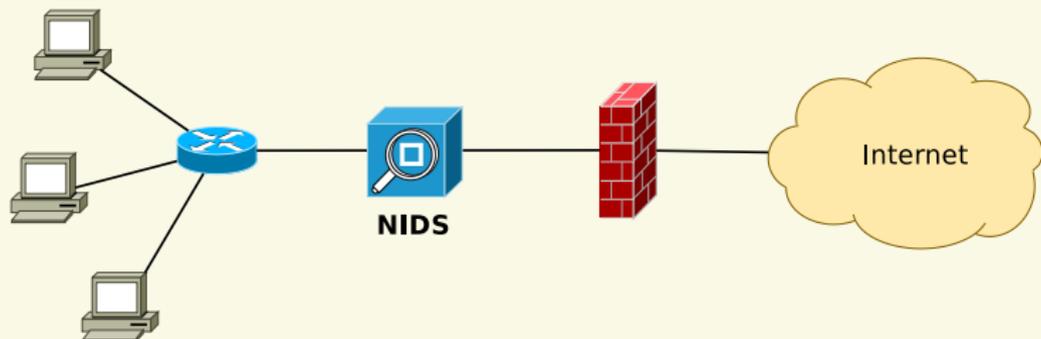
1 SKIMS

2 Mobile Honeypot

- Honeypot
- Mobile Honeypot

Network Intrusion Detection System (NIDS)

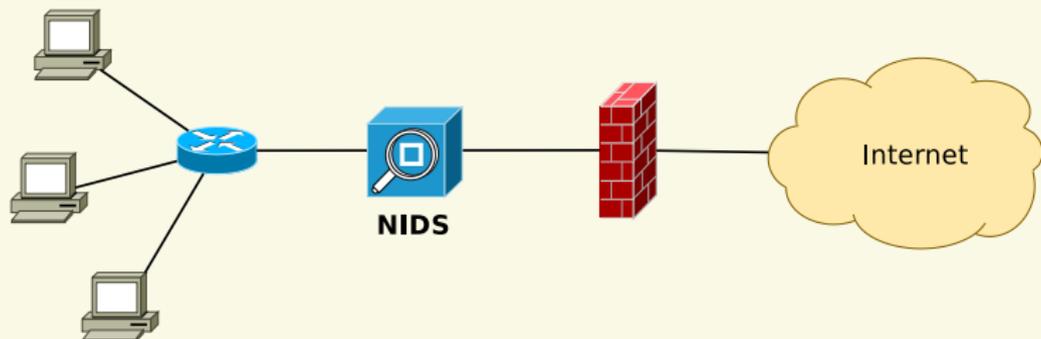
Traffic in Produktivsystemen beobachten
Alarm bei verdächtigen Paketen



Problem: *Good* versus *Bad* Traffic

Network Intrusion Detection System (NIDS)

Traffic in Produktivsystemen beobachten
Alarm bei verdächtigen Paketen



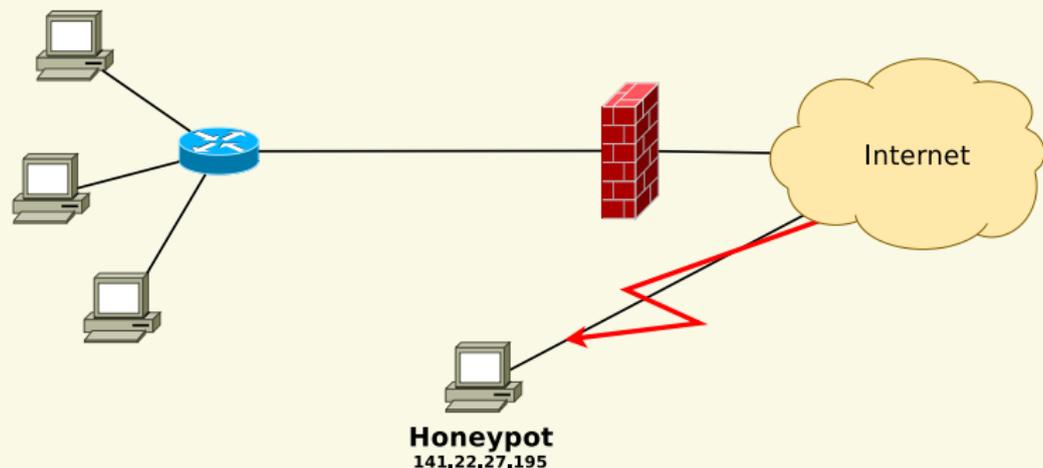
Problem: *Good* versus *Bad* Traffic

- False Positives
- keine Chance bei verschlüsseltem Traffic
- bisher unbekannte Angriffsweisen schwer zu erkennen

Wie genau läuft ein Angriff ab?

Honeypot

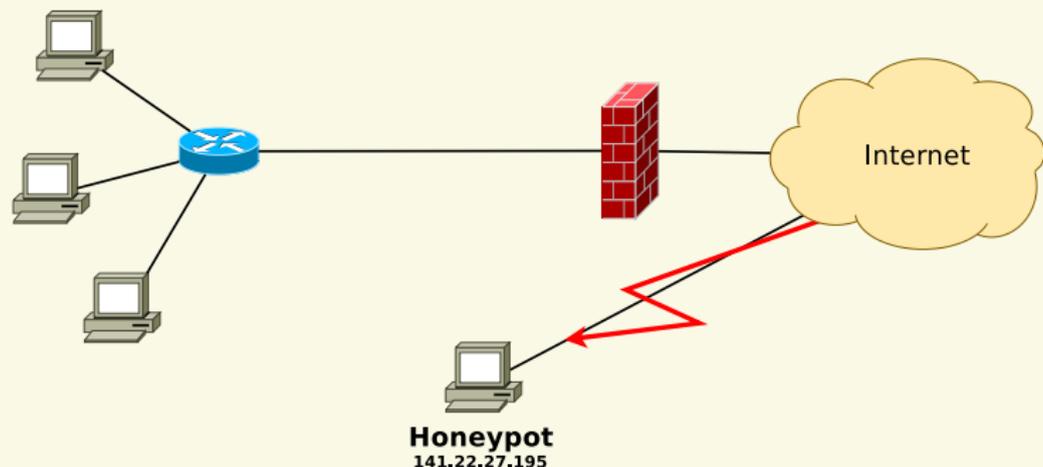
- Jeder Zugriff ist verdächtig
- Untersuchen des Angriffs am Endpunkt



Gefahren:

Honeybot

- Jeder Zugriff ist verdächtig
- Untersuchen des Angriffs am Endpunkt



Gefahren:

- Sprungbrett für weitere Angriffe
- Angreifer liefert Fehlinformationen

High Interaction Honeypot

Echtes System (auch virtualisiert möglich)

Hauptzweck: manuelle Angriffe analysieren

- aufwendig
- kann entdeckt und erobert werden

Server-Honeyspots: Sebek, Argos (basiert auf Qemu)

Client-Honeyspots: Capture-HPC

Low Interaction Honeypot

Funktionalität nachgebildet

Hauptzweck: automatisierte Angriffe aufdecken

- weniger aufwendig
- Informationsgewinn auf Simulation beschränkt

Server-Honeybots: honeyd, honeytrap

Client-Honeybots: phoneyc

Mehrere Honeybots -> Honeybot (Honeybots als Sensoren)

Mobiles Endgerät



Mobiles Endgerät



- Angriffe über Wireless Interfaces
 - Übertragungsmedium ungeschützt
 - räumlich begrenzt

Mobiles Endgerät



- Angriffe über Wireless Interfaces
 - Übertragungsmedium ungeschützt
 - räumlich begrenzt
- Angriffsziele
 - Angriffe auf Nutzerdaten
 - Angriffe sollen Kosten verursachen (0190...)

Mobiles Endgerät



- Angriffe über Wireless Interfaces
 - Übertragungsmedium ungeschützt
 - räumlich begrenzt
- Angriffsziele
 - Angriffe auf Nutzerdaten
 - Angriffe sollen Kosten verursachen (0190...)
- Hardware-Ressourcen stark beschränkt

honeyM

Paper (März 2010):

A Framework for Implementing Virtual Honeyclients for Mobile Devices

Rechner simuliert mehrere Mobilgeräte (z.B. iPhones)

- simuliert WLAN, Bluetooth und GPS
 - WLAN
 - Bluetooth
 - GPS
 - GMDA und 3G
- Fingerprinting

Realisierungsmöglichkeiten

- *Low Interaction Honeypot*
- *High Interaction Honeypot*
- *Kompromiss*

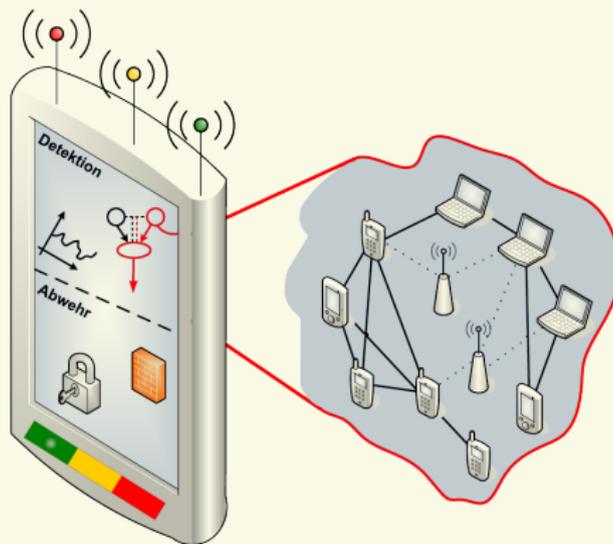
Low und High Interaction Honeypot

- Low Interaction Honeypot
 - leistungsfähiger Rechner simuliert mobile Geräte (z.B. honeyM)
 - Mobiles Gerät simuliert weiteres mobiles Gerät
- *High Interaction Honeypot*
 - Mobiles Gerät wird ausschließlich als Honeypot verwendet

Kompromiss

Solange ein Interface nicht genutzt wird, steht es dem Honeypot zur Verfügung

- Mobiles Gerät als Proxy: Eigentlicher Honeypot als Server
- Teilen der Rechenlast des Honeypots in einem Overlay



Vielen Dank für Eure Aufmerksamkeit

