Mobile Honeypot

Theodor Nolte

Hochschule für Angewandte Wissenschaften Hamburg
Fakultät Technik und Informatik
Department Informatik

30. November 2010

university-logo

Gliederung

university-logo

SKIMS

Bundesministerium
für Bildung
und Forschung

***S**chichtenübergreifendes **k**ooperatives **I**mmunsystem*
*für **m**obile, mehrseitige **S**icherheit*

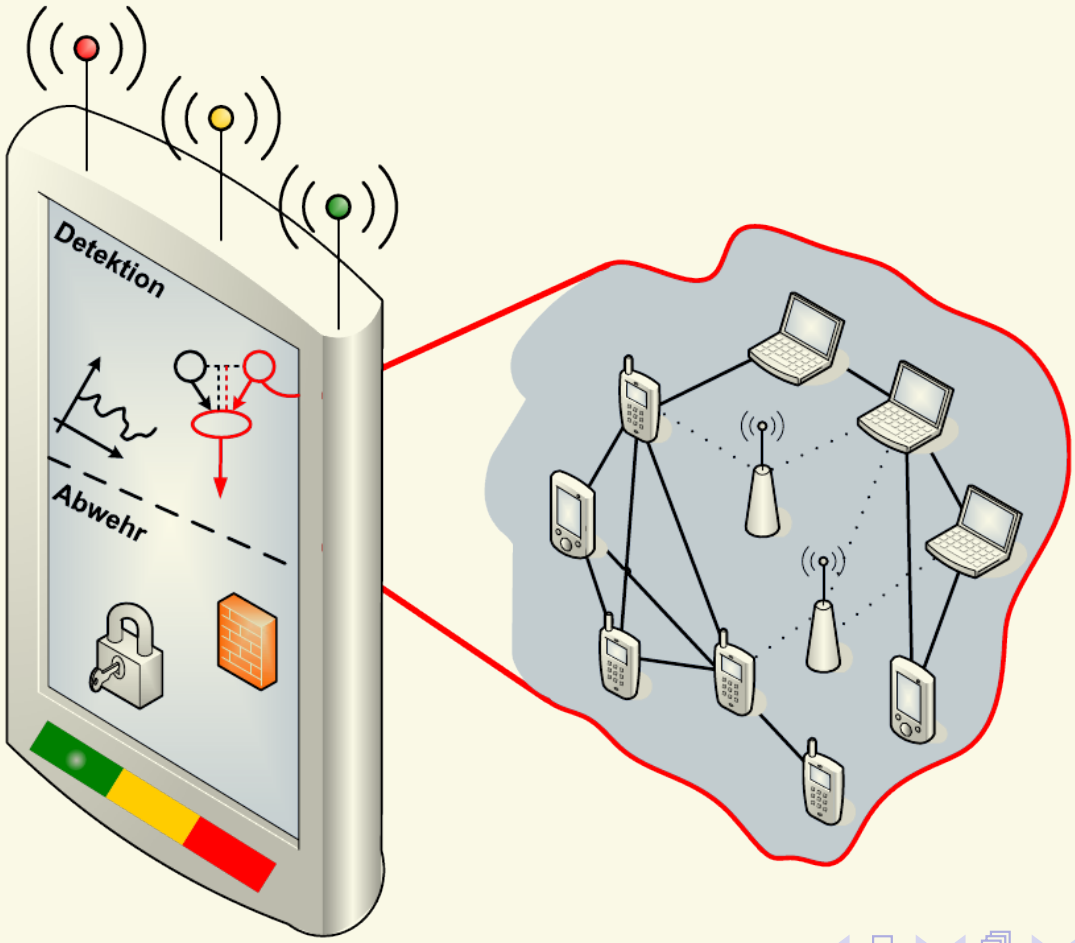
Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

university-logo

SKIMS

Angriffe

- erkennen
- abwehren



Gliederung

university-logo

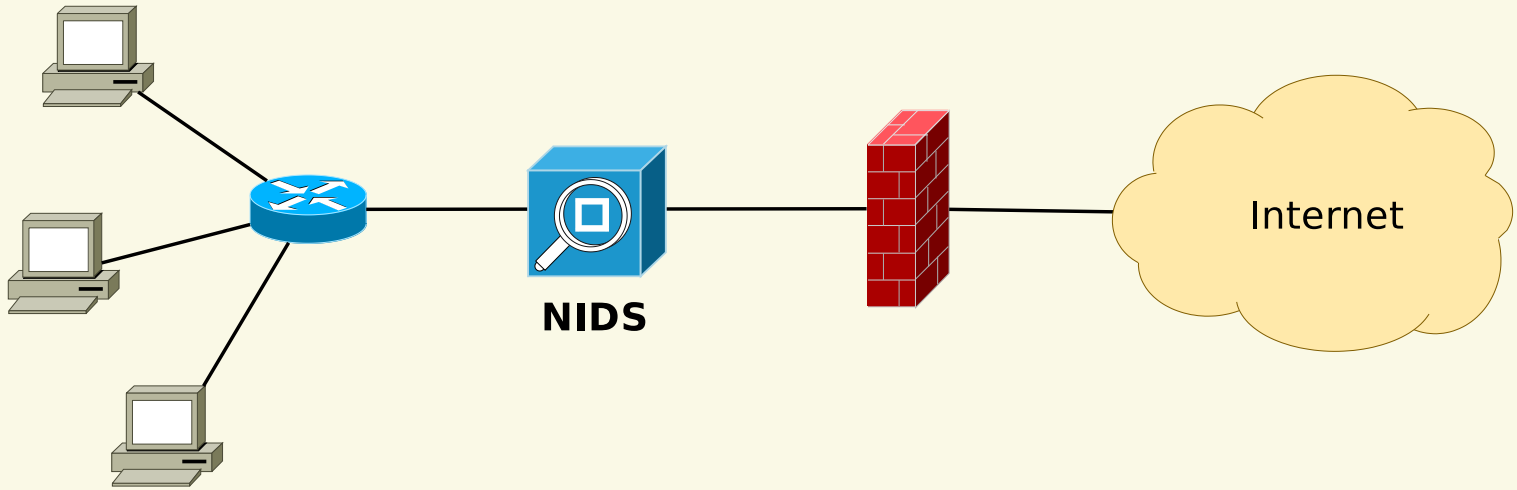
Honeypot

Angriffe

- detektieren
- analysieren

Network Intrusion Detection System (NIDS)

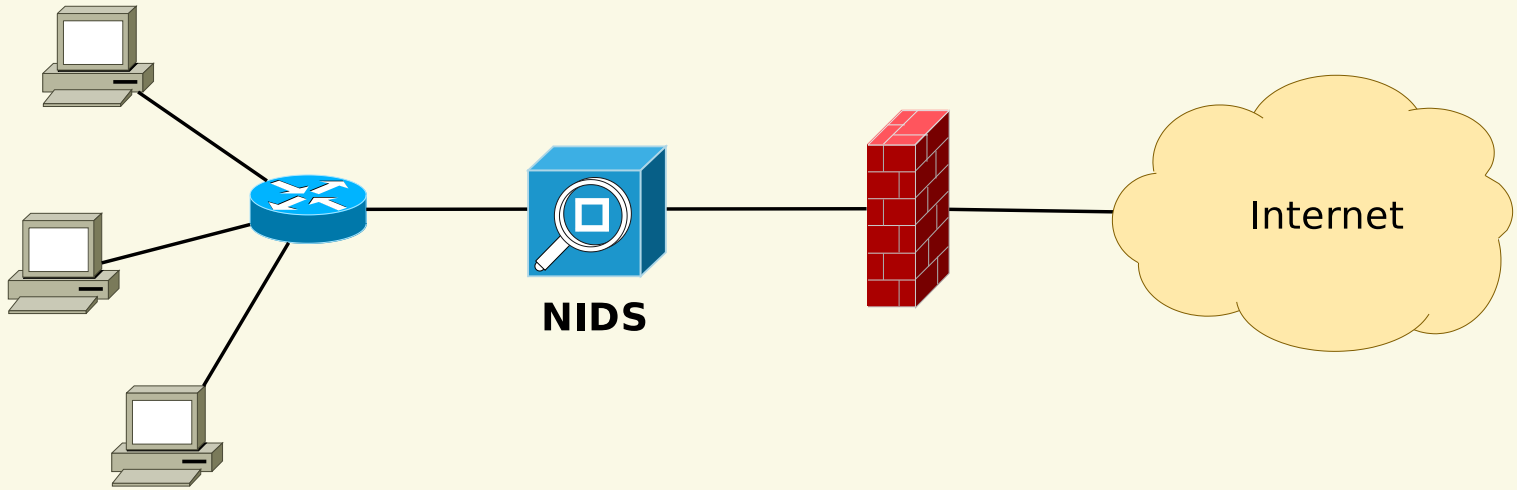
Traffic in Produktivsystemen beobachten
Alarm bei verdächtigen Paketen



Problem: *Good* versus *Bad* Traffic

Network Intrusion Detection System (NIDS)

Traffic in Produktivsystemen beobachten
Alarm bei verdächtigen Paketen



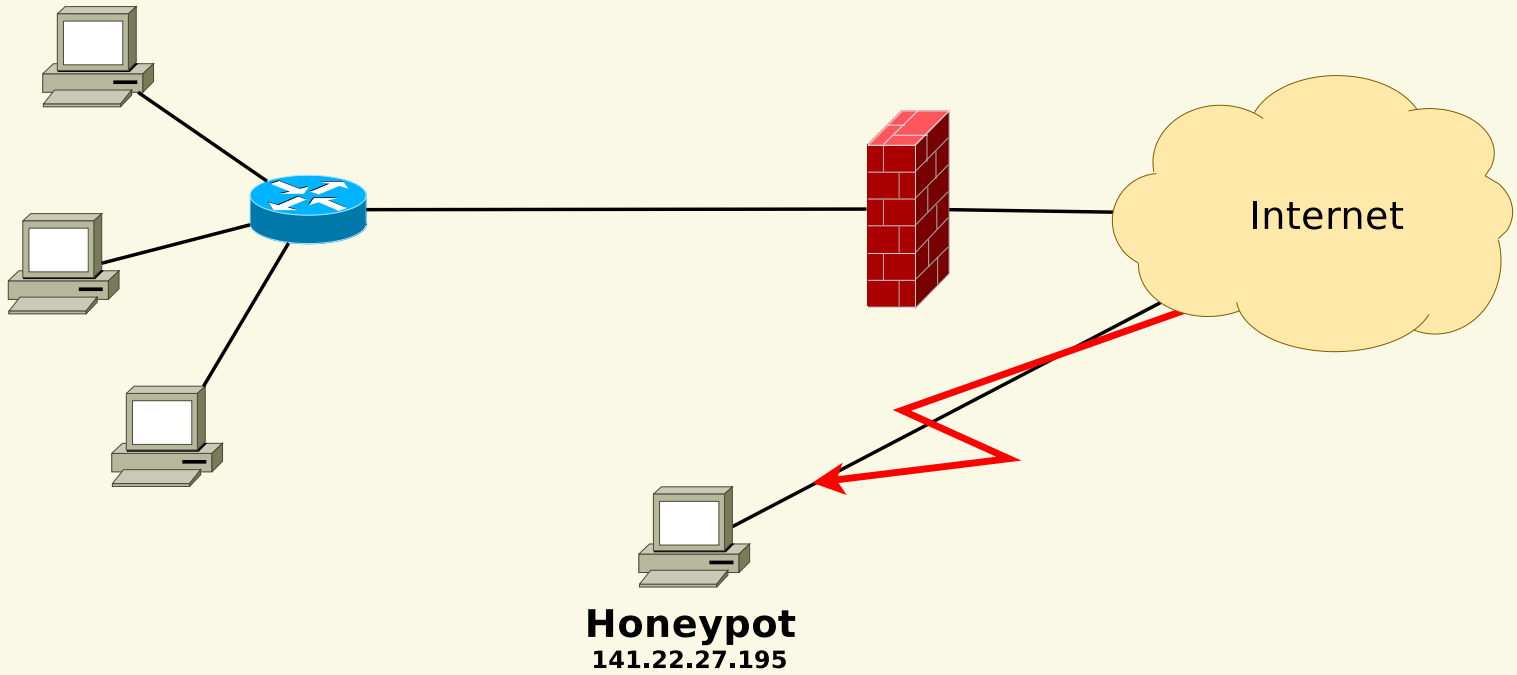
Problem: *Good* versus *Bad* Traffic

- 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



High Interaction Honeypot

Echtes System (auch virtualisiert möglich)
Hauptzweck: manuelle Angriffe analysieren

- aufwendig
- kann entdeckt und erobert werden

Server-Honeypots: Sebek, Argos
Client-Honeypots: Capture-HPC

Gefahren:

High Interaction Honeypot

Echtes System (auch virtualisiert möglich)
Hauptzweck: manuelle Angriffe analysieren

- aufwendig
- kann entdeckt und erobert werden

Server-Honeypots: Sebek, Argos
Client-Honeypots: Capture-HPC

Gefahren:

- Sprungbrett für weitere Angriffe
- Angreifer liefert bewußt Fehlinformationen

Low Interaction Honeypot

Funktionalität nachgebildet
Hauptzweck: automatisierte Angriffe aufdecken

- weniger aufwendig
- Informationsgewinn auf Simulation beschränkt

Server-Honeypots: honeyd, honeytrap
Client-Honeypots: phoneyc

Mehrere Honeypots -> Honeynet (Honeypots 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...)

university-logo

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
  - ~~CDMA und 3G~~
- Fingerprinting

Realisierungsmöglichkeiten

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

Low und High Interaction Honeypot

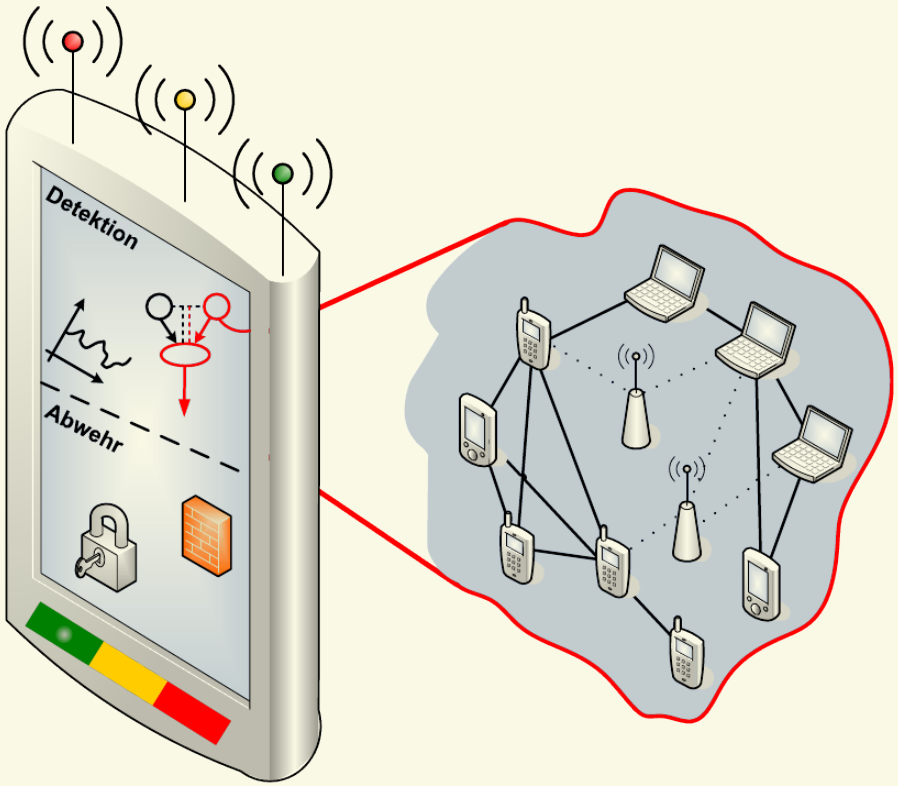
- Low Interaction Honeypot
  - leistungsfähiger Rechner simuliert mobile Geräte (z.B. honeyM)
  - Mobiles Gerät simuliert weiteres mobiles Gerät
  - **Mobiles Gerät simuliert nur einzelne Protokolle**
- *High Interaction Honeypot*
  - Mobiles Gerät wird ausschließlich als Honeypot verwendet

university-logo

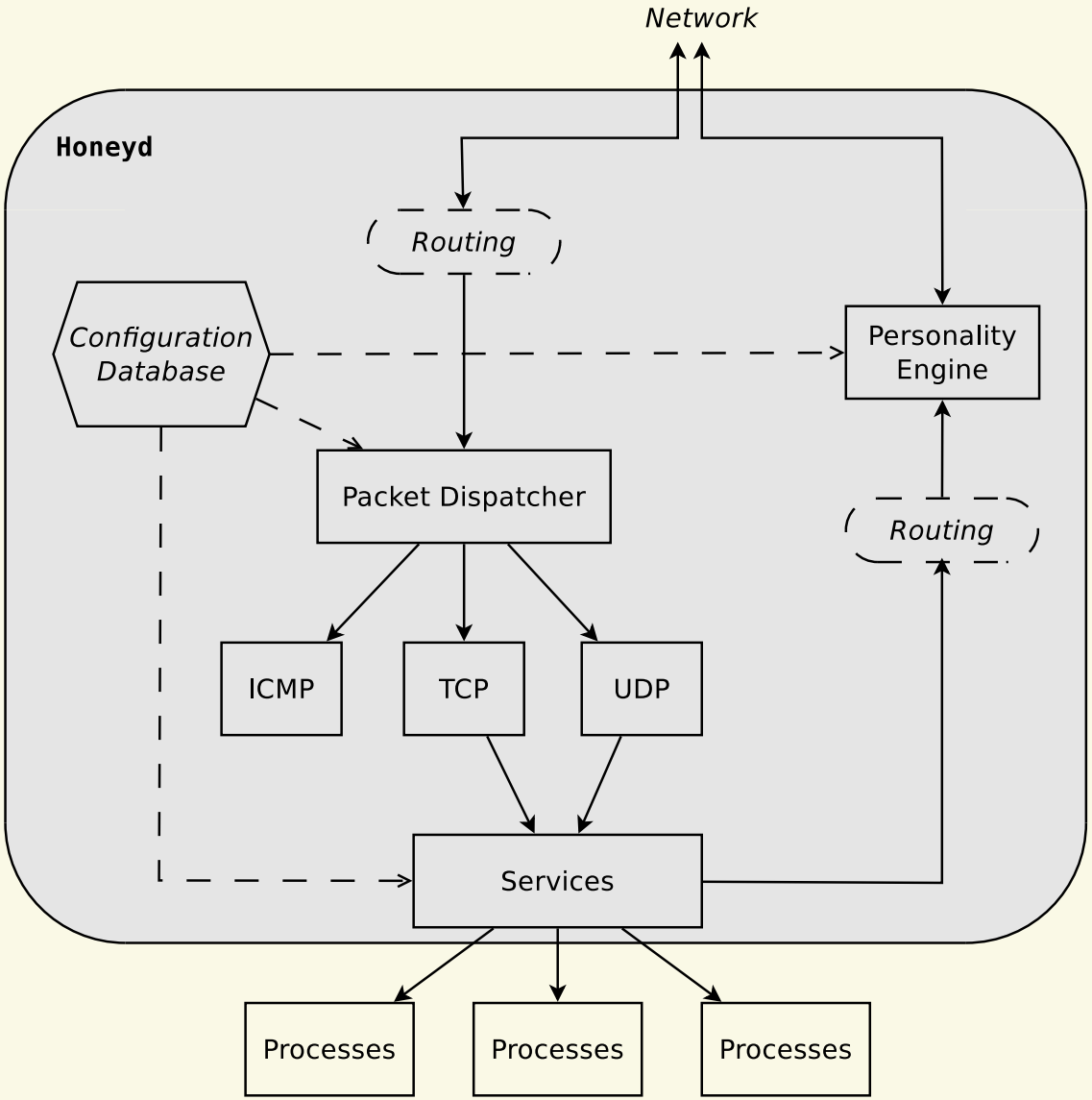
Kompromiss

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

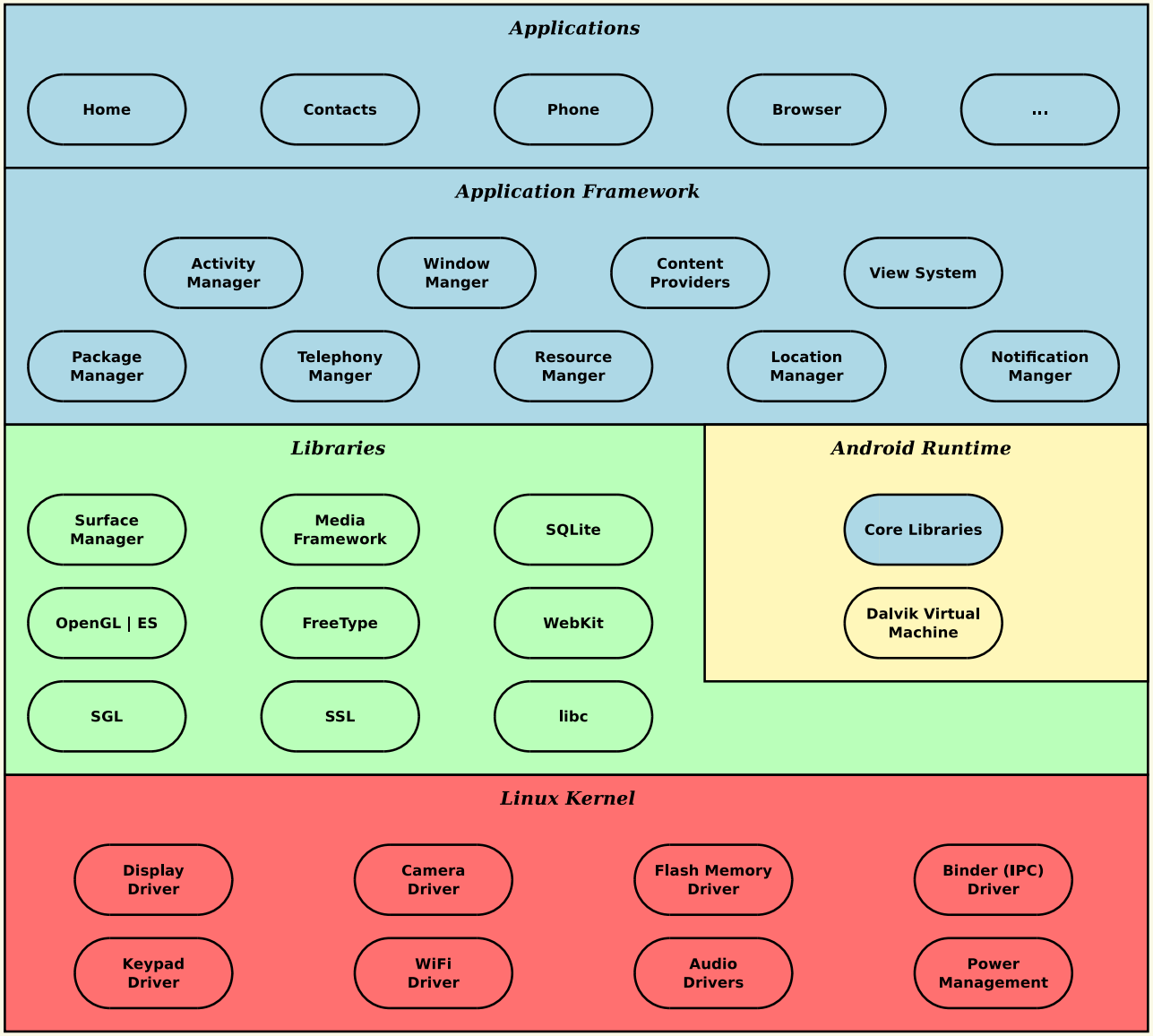
- Mobiles Gerät als Proxy: Eigentlicher Honeypot als Server
- Teilen der Rechenlast des Honeypots in einem Overlay



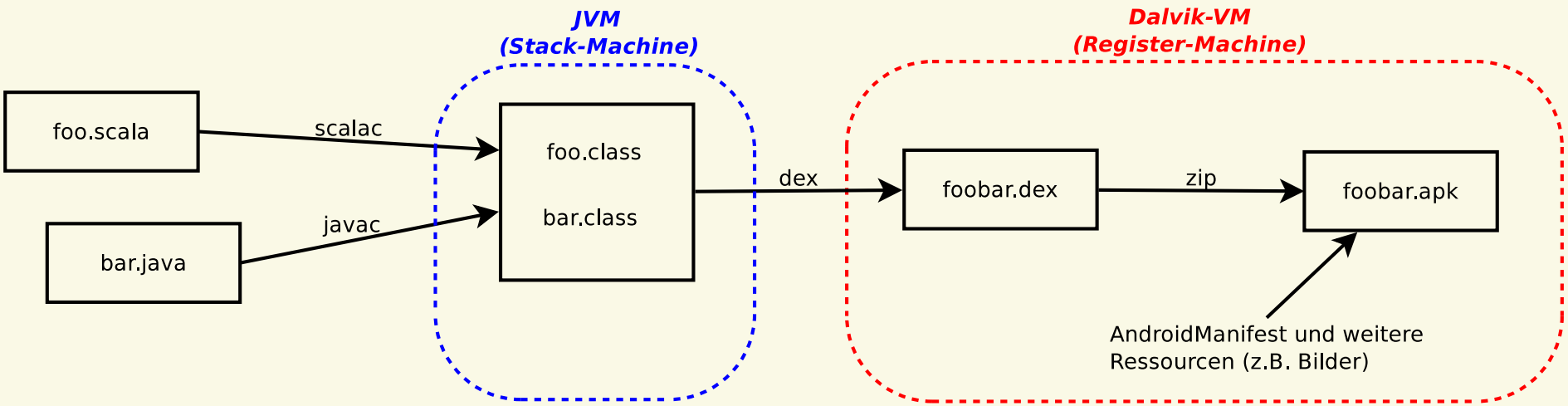
honeyd – Architektur



Android – Architektur



Android – Build Path



Quellen

- *Niels Provos und Thorsten Holz*
  Virtual Honeypots – From Botnet Tracking to Intrusion Detection
  Addison-Wesley Longman, Amsterdam; Auflage: 1 (16. Juli 2007)
  ISBN: 978-0-321-33632-3
- *TJ OConnor und Ben Sangster*
  honeyM: A Framework for Implementing Virtual Honeyclients for Mobile Devices
  WiSec ’10 Proceedings of the third ACM conference on Wireless network security, März 2010

Vielen Dank für Eure Aufmerksamkeit

university-logo