

Mit Trusted Computing zur mobilen Sicherheit der Zukunft

Malte Hesse

Hesse (at) internet-sicherheit.de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen



Mobile Integration

Geräte



Plattform
Soft- &
Hardware

heterogenes
Umfeld



Schwachstellen

Globalisierung
& Kostendruck

Schwächen
in Standards



facettenreiche
Konnektivität



Daten

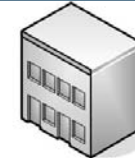
Anwendungen

Dienste

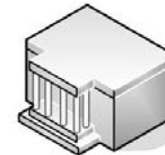
wechselnde
Einsatzumgebungen



- Mitarbeiter flexibel eingesetzt
- verlangen bestimmte Geräte
Benutzer - bringen eigene Geräte mit



- erhofft Wertschöpfung
- trennt sich von Perimeter-
sicherheit
Unternehmen



- meist ausländische Unter-
nehmen (Hochsicherheit)
- „Out of the box“-Lösungen
Hersteller



Mobilfunkbetreiber, ISP,
Internet Cafés, WLAN-AP,
Treffen beim Konkurrenten
Provider



unterschiedlichste Motivation:
- gezielte Spionage
- zufälliger Vandalismus
Angreifer

■ Vertraulichkeit

- Techniken vorhanden – sollte kein Problem mehr sein?!

■ Verfügbarkeit

- Techniken vorhanden: z. B. Synchronisation und Backup
- Hohe Akkulaufzeit der Geräte; redundante Anbindung

■ Integrität

- „Sorgenkind“

news 05.12.2007 09:45

**Vertraulichkeit & Verfügbarkeit
auch ohne Integrität?**

Botnetz-Studie: Bots verbreiten sich über uralte Lücken

Die Univ **Erste "Schadsoftware" fürs iPhone** 1 Bericht über IRC-basiert

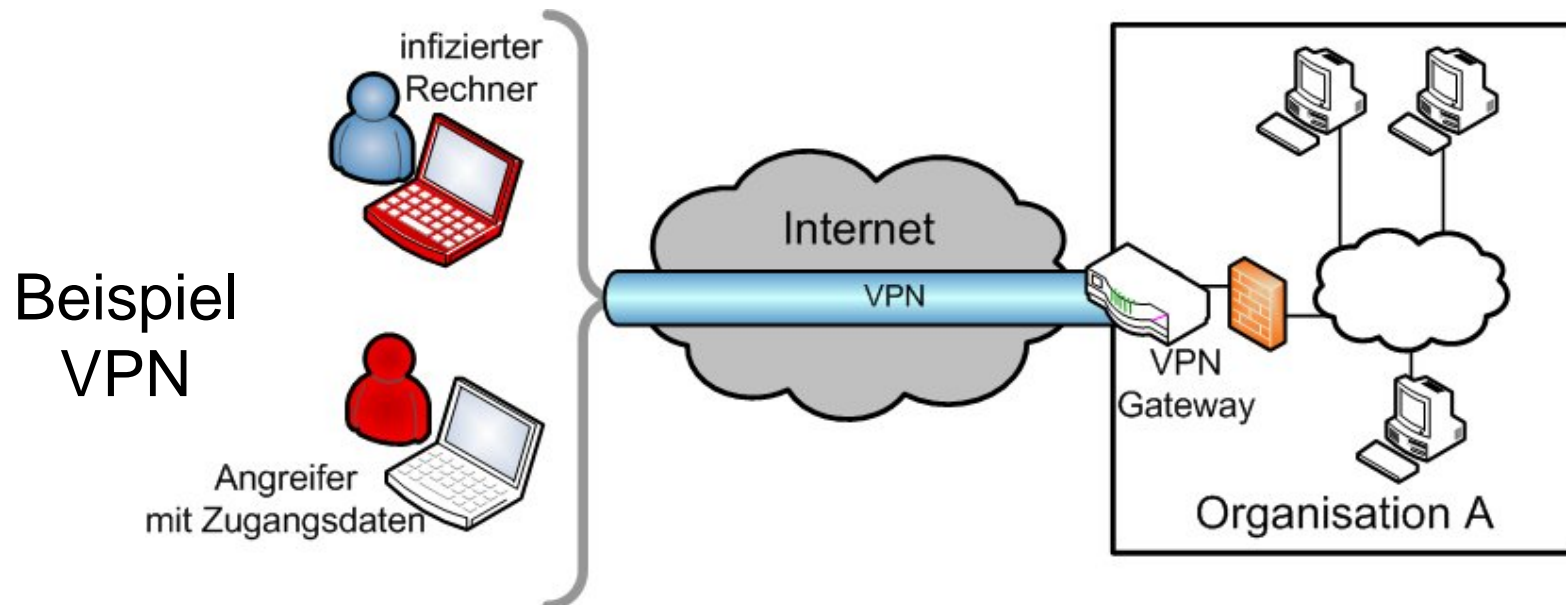
Ein elf **24C3: Gezielte Trojaner-Attacken im Informationskrieg**

Der be **BKA-Chef: Zur Online-Durchsuchung gibt es keine Alternative**

Im Rahmen der [beliebten](#) Osnabrücker [Ringvorlesung Kriminalistik](#) sprach am gestrigen Mittwochabend Jörg Z

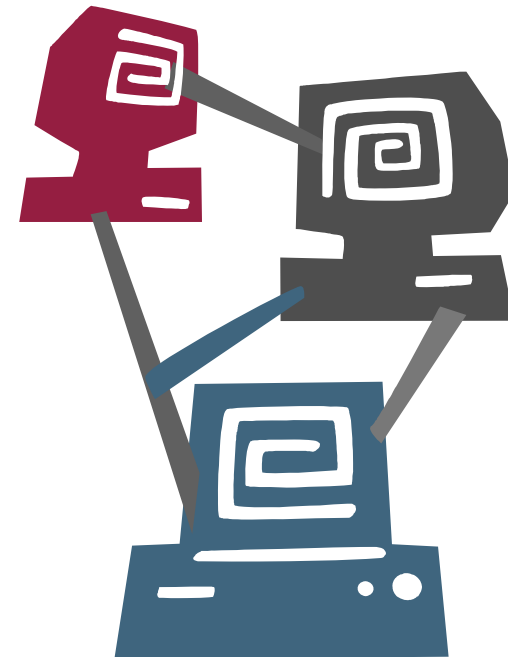
Aktuelle Probleme am Beispiel VPN

- Keine Unterscheidung zwischen vertrauenswürdigen und nicht vertrauenswürdigen Rechnersystemen möglich
- **Folgen**
 - Malware und Eindringlinge gefährden das Netzwerk
 - Netze sind nicht vertrauenswürdig
 - Kein vertrauenswürdiger Datenaustausch möglich



- **Idee:**
 - **Feststellen der Systemintegrität, durch messen der Gerätekonfiguration**
 - **Überprüfen der Konfiguration nach Vorgaben (Policies)**
 - **Vertrauenswürdige Geräte integrieren und**
 - **Nicht-vertrauenswürdige Geräte ablehnen oder isolieren (für Updates)**
- **Vorhandene Lösungen:**
 - Microsoft NAP
 - Cisco NAC
 - Juniper, StillSecure, ...

→ **Heutige NAC-Lösungen besitzen zwei große Einschränkungen ...**



Network Access Control (NAC)

→ kritische Betrachtung (1/2)

1. Standardisierung

- **Alle Lösungen sind inkompatibel zueinander**
- **Erste Bestrebungen**
 - Clientseitige Kompatibilität von Cisco und Microsoft
 - Microsoft stellt sein Client-Server-Protokoll „SoH“ zur Verfügung
 - „Kleine“ Lösungen werden zu den „Großen“ kompatibel
 - z.B.: StillSecure Safe Access laut Hersteller zu Microsoft NAP und Cisco NAC
- **Zwei Standardisierungs-Ansätze**
 - **Internet Engineering Task Force (IETF): Network Endpoint Assessment (NEA)**
 - **Trusted Computing Group (TCG): Trusted Network Connect (TNC)**

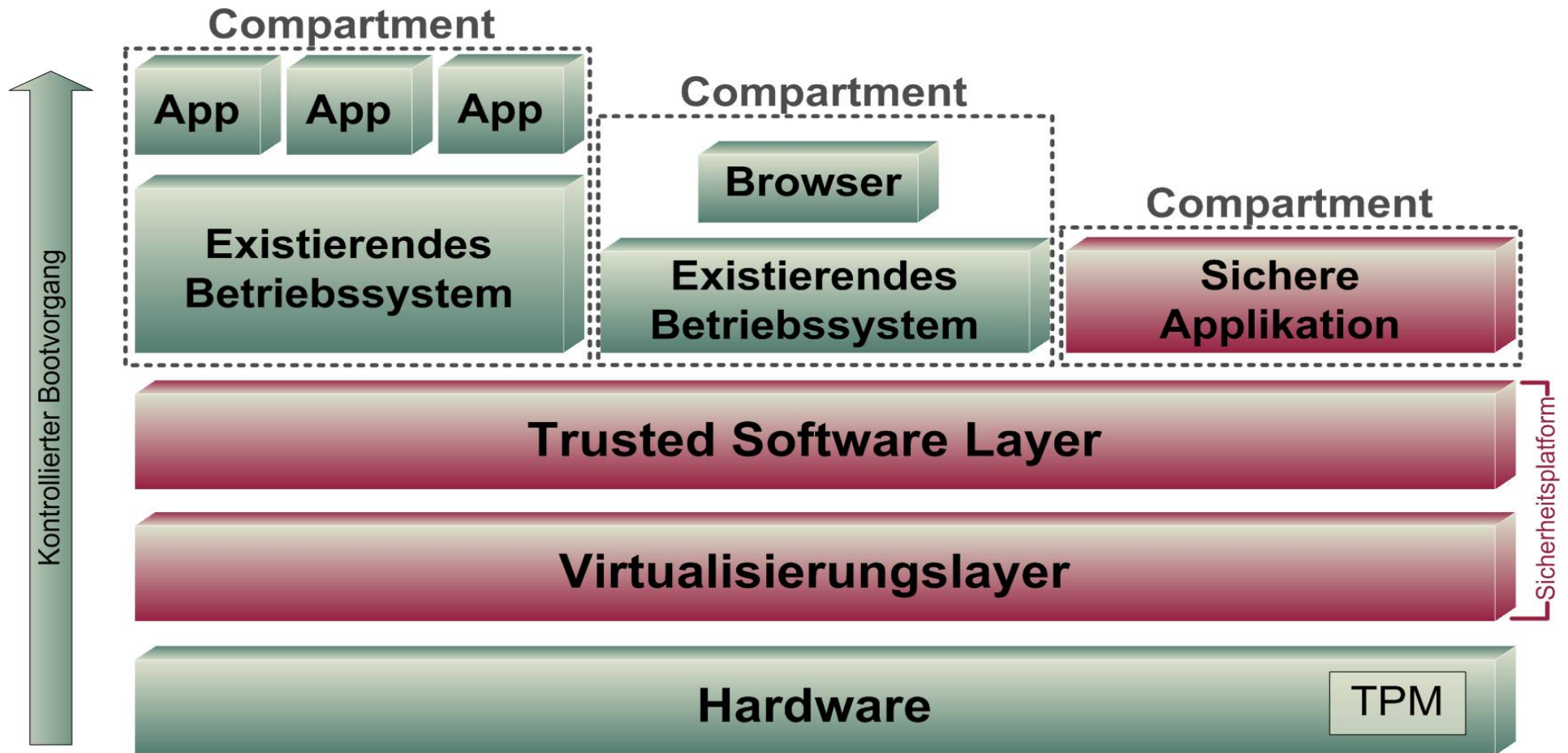
2. Vertrauenswürdigkeit / Sicherheit

- Mögliche Kompromittierung
 - gemessener Komponenten (z. B. Virens Scanner)
 - der NAC-Komponenten selbst
 - Anhand von Cisco NAC auf der Black Hat Konferenz 2007 vorgeführt
 - Problem: heutige Betriebssysteme
 - keine Isolation möglich
- **Lösungsansatz: Integration in eine Sicherheitsplattform**



Sicherheitsplattform

→ Übersicht

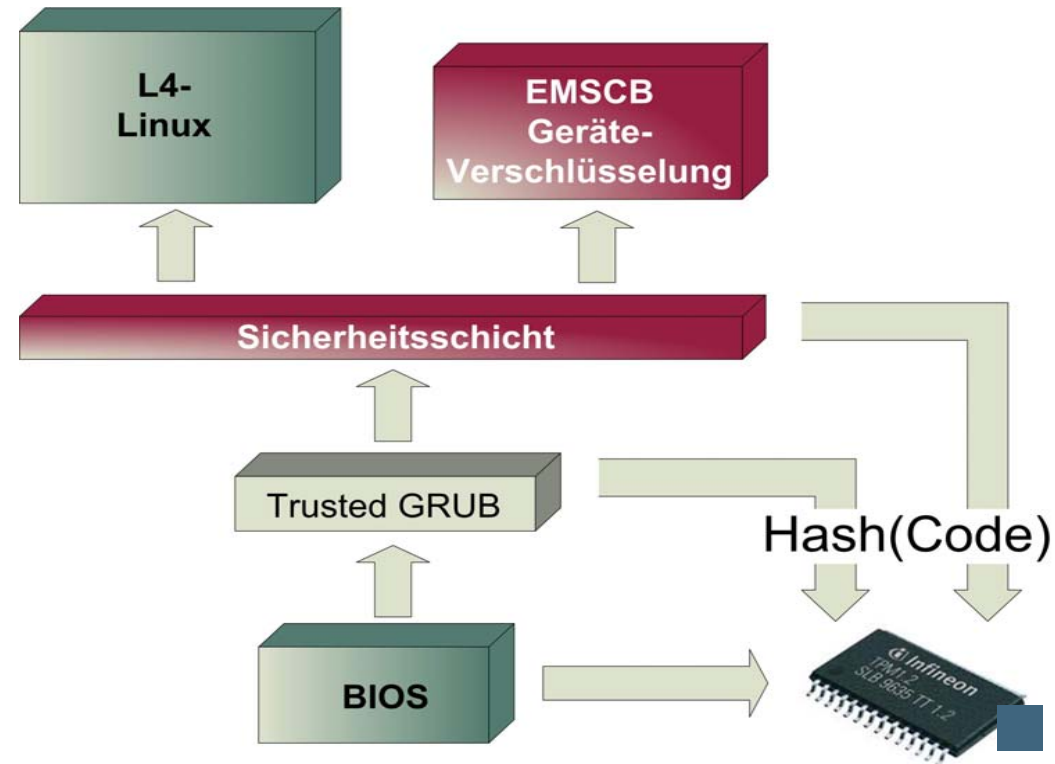


Sicherheitsplattform → Chain of Trust

- **Erweitern des Bootloaders um Funktionen von Trusted Computing**
 - Messen der Integrität von Komponenten *vor* deren Ausführung
 - Ablegen der Integritätswerte in Registern eines Sicherheitsmodules, z. B. Trusted Platform Module (TPM)

- **Kontrollierter Bootvorgang:**

- Bildet die **Wurzel** der Sicherheitsplattform
- Misst alle Komponenten



Trusted Network Connect (TNC)

→ Einführung

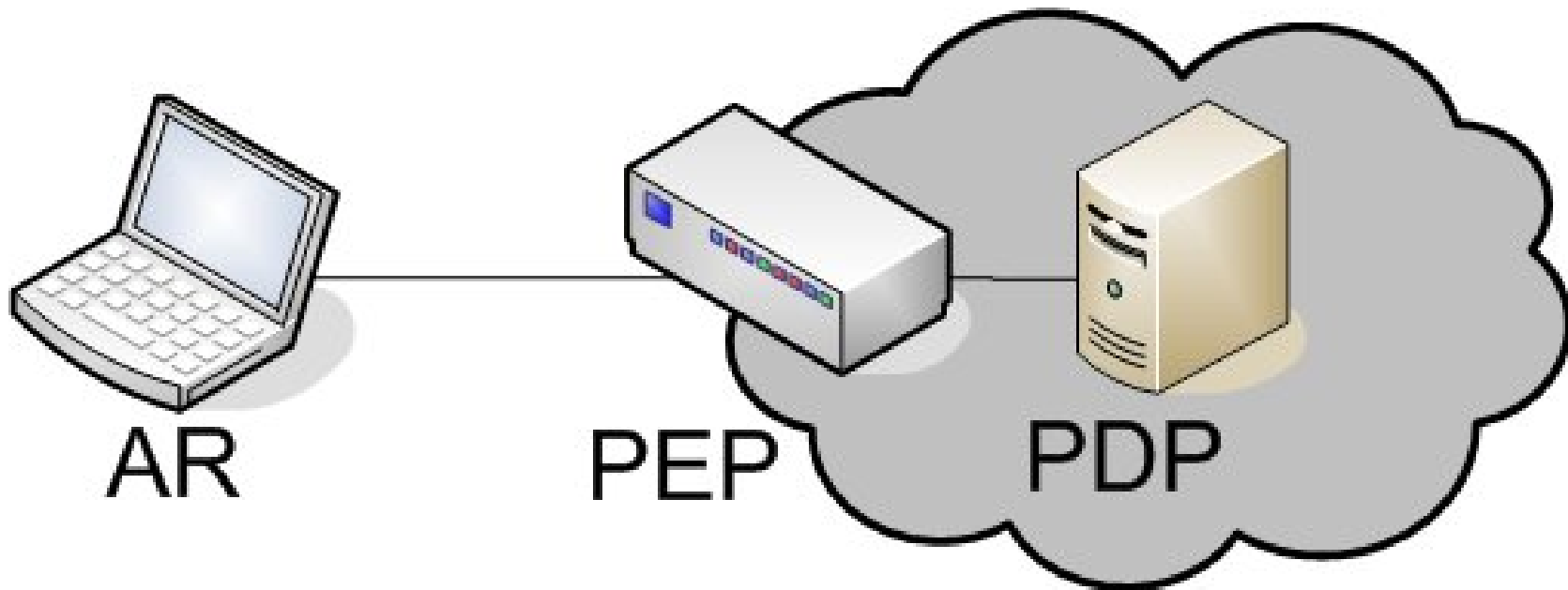
- „Trusted Network Connect“ Spezifikation ist von der TCG
- Ziel: Entwicklung eines Industrie-Standards im NAC Bereich
- Eigenschaften:
 - Offene Spezifikation (aktuell: Version 1.2)
 - Offen für alle Plattformen und Hersteller
 - Unterstützt Sicherheitsmodule, wie TPM, MTM ...
 - z. B. zum Signieren von Messwerten
 - Nutzt vorhandene Techniken:
 - Netzwerkzugriff: 802.1x, VPN & PPP
 - Nachrichtentransport: EAP TLS & HTTPS
 - Authentifizierung: Radius Server & Diameter



Trusted Network Connect (TNC)

→ Komponenten & Topologie

- Access Requestor (AR)
- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)



AR bei TNC ebenfalls agentenbasiert: Vertrauenswürdigkeit erst in Verbindung mit Sicherheitsplattform

- **Zunehmende Vernetzung**
- **Bedrohungen im mobilen Umfeld nehmen zu**
 - Steigender Bedarf an vertrauenswürdigen Netzwerkverbindungen
- **Vorhandene Lösungen (z.B. VPN) sind derzeit nicht ausreichend**
- **NAC erlaubt es, Gerätekonfigurationen zu prüfen**
 - Erhöht das Level an Vertrauen



- **Vorhandene NAC Lösungen sind bisher eingeschränkt verwendbar**
- **TNC bietet Antworten auf die größten Einschränkungen**
 - 1. Standardisierung:
 - TNC ist offen; wichtig im heterogenen Umfeld der mobilen Geräte
 - 2. Vertrauenswürdigkeit / Sicherheit:
 - Unterstützung von Sicherheitsmodulen
 - Dank des offenen Standards einfache Integration in Sicherheitsplattformen
- wichtige technische Herausforderung ist die Entwicklung von sicheren Hard- und Softwarelösungen für mobile Geräte



Mit Trusted Computing zur mobilen Sicherheit der Zukunft

Vielen Dank für Ihre Aufmerksamkeit Fragen ?

**Antworten auch nach dem Vortrag:
Gemeinschaftsstand Nordrhein-Westfalen
Halle 9, Stand C16**

Malte Hesse

Hesse (at) internet-sicherheit.de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen

