

Trusted Network Connect

Networking Academy Day

19.04.2008

Dipl.-Inf. Stephan Gitz

<Stephan.Gitz@hs-bremen.de>

Roadmap

- ▶ Ziele der Informationssicherheit
- ▶ Herausforderungen der Informationssicherheit
- ▶ Angriffsvektoren und Gegenmaßnahmen
- ▶ Network Access Control (NAC)
- ▶ Trusted Network Connect (TNC)
- ▶ Trusted Platform Module (TPM)
- ▶ TNC im Projekt SIMOIT

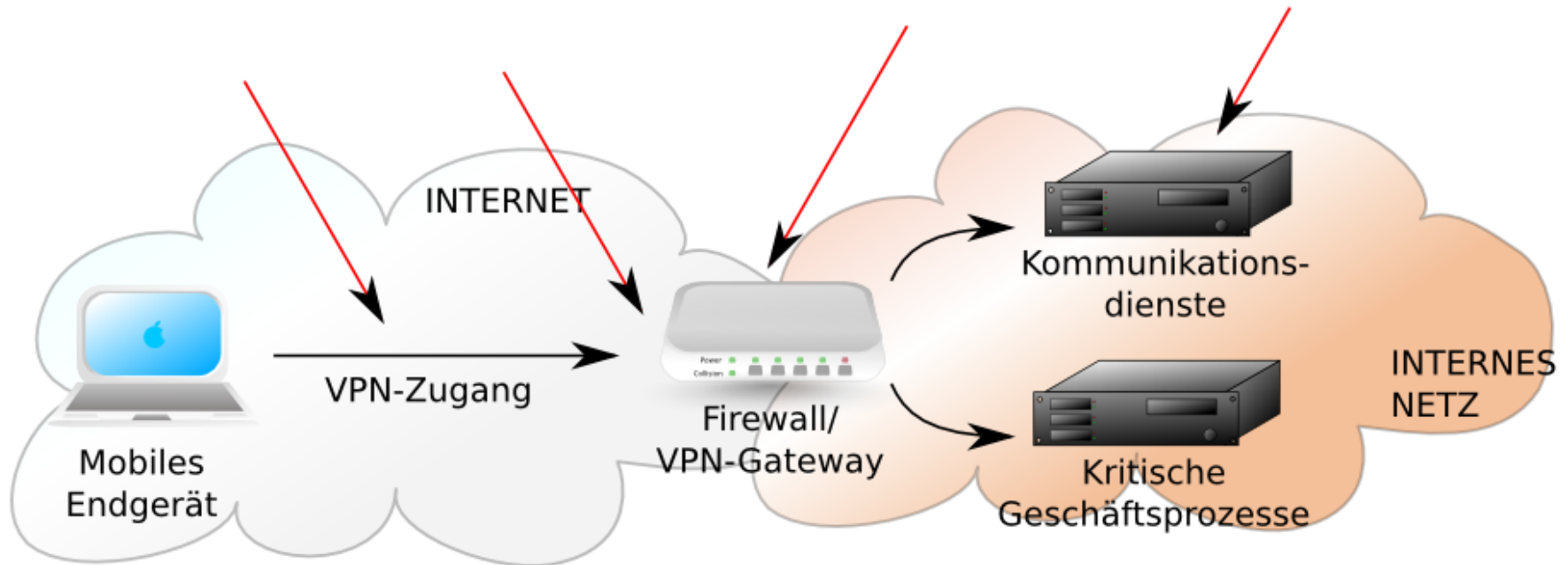
Ziel der Informationssicherheit

Das Ziel der Informationssicherheit ist es, dass die Vertraulichkeit, Verfügbarkeit und Integrität in einem ausreichendem Maße sichergestellt wird.

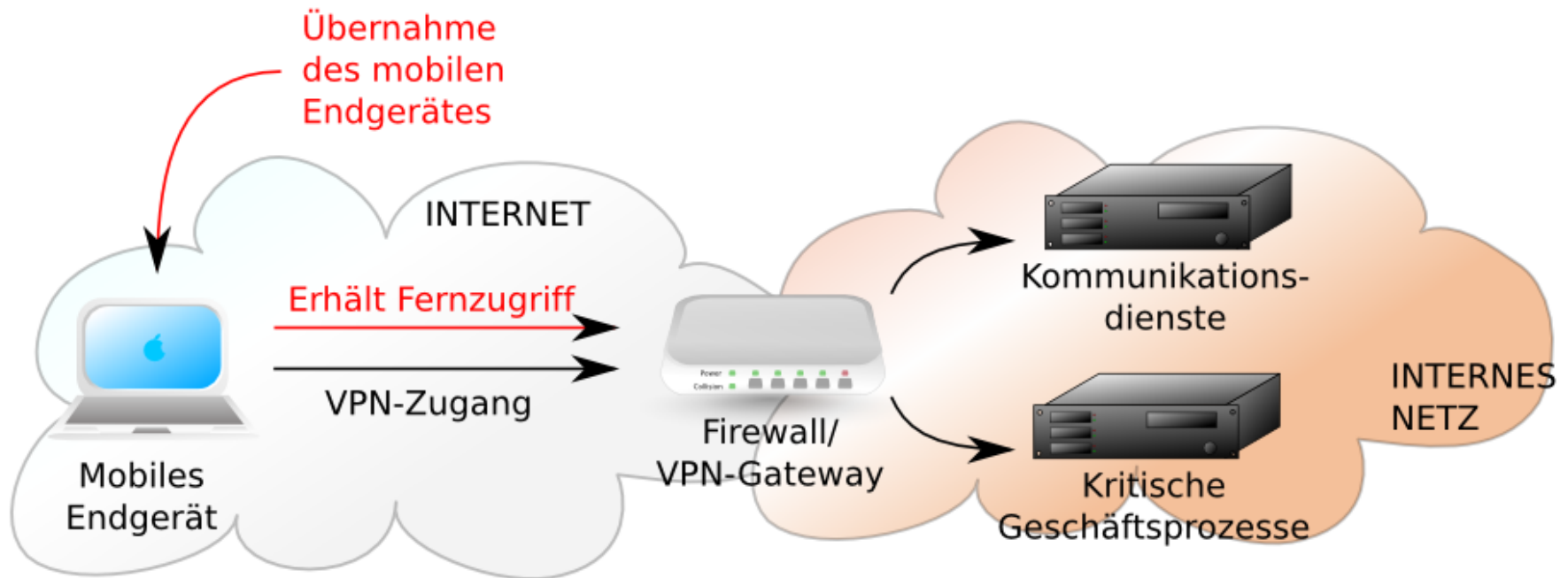
Herausforderungen der Informationssicherheit

- ▶ Immer mehr Geschäftsprozesse hängen von IT-Infrastrukturen ab
- ▶ Der Schutzbedarf der IT-Infrastrukturen steigt ständig
- ▶ Es gibt kein nichttriviales Programm ohne Fehler
- ▶ Die Komplexität der Systeme ist schwierig zu beherrschen
- ▶ vollständige Sicherheit bei vernetzten Systemen ist nicht erreichbar
- ▶ Sicherheit ist kein Produkt sondern ein Prozess

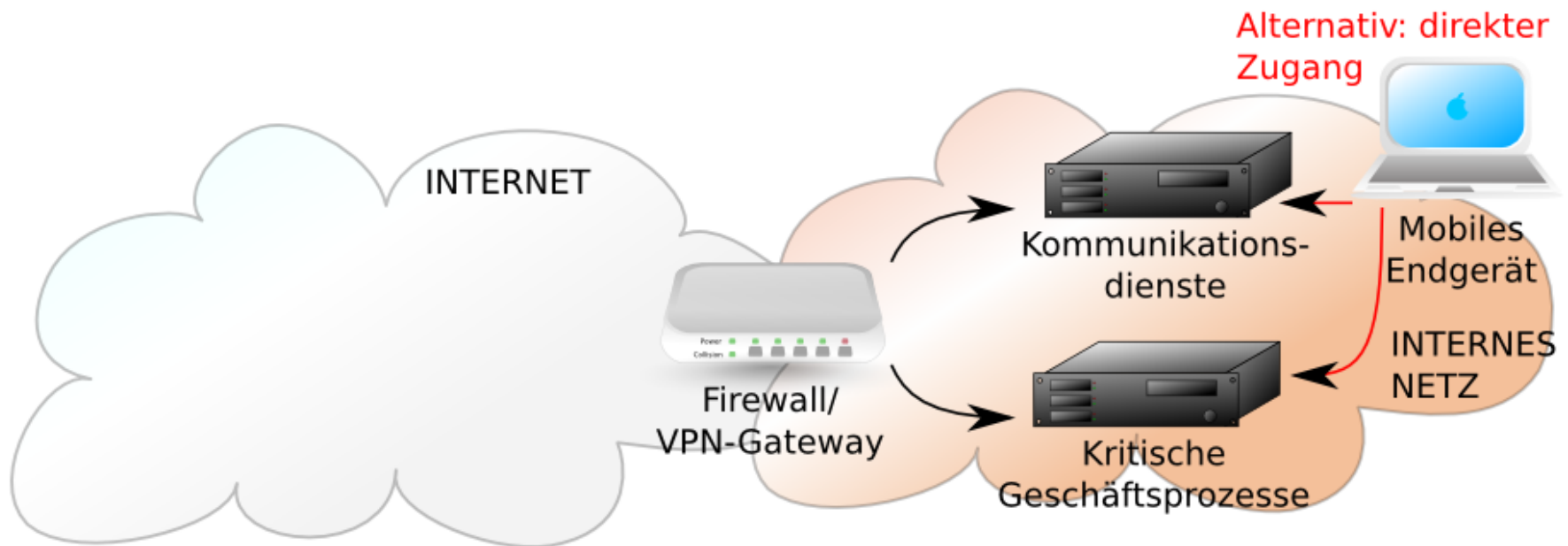
Angriffsvektoren und Gegenmaßnahmen



Angriffsvektor: Mobile Endgeräte



Angriffsvektor: Mobile Endgeräte



Network Access Control (NAC) – Ziele

- ▶ Intrusion Prevention
 - Verringertes Risiko durch Überprüfung der Geräteintegrität
 - Zugriff nur bei Erfüllung der Security Policy
 - z.B. aktuelle Softwarepakete und Anti-Virus-Definitionen
- ▶ Isolation von nicht-konformen Geräten
 - Möglichkeit, z.B. Softwarestände zu aktualisieren
- ▶ Außerdem: nicht-funktionale Ziele
 - Möglichst geringe Einschränkungen des Workflows der Mitarbeiter

NAC – Voraussetzungen

- ▶ Akzeptanz der notwendigen Maßnahmen durch die Hierarchien
- ▶ Schutzbedarfsanalyse der IT-Infrastruktur
- ▶ Erarbeitung einer Security Policy für Endgeräte
 - Erfassung der Anforderungen der Mitarbeiter
 - Entscheidungen zu zulässigen Zuständen der Endgeräte
 - Problem – Vollständigkeit
 - viele Schnittstellen, Plattformen, Anwendungen und Prozesse
- ▶ Kontinuierliche Anpassung an veränderte Unternehmensumgebungen (Change Management)

NAC – Relevante Technologien

- ▶ Network Access Protect (NAP – Microsoft)
- ▶ Network Admission Control (NAC – Cisco)
- ▶ Trusted Network Connect (TNC – TCG)
- ▶ Network Endpoint Assessment (NEA – IETF-WG)

Trusted Network Connect

- ▶ NAC-Standard der Trusted Computing Group
- ▶ Integritätsüberprüfung auf dem mobilen Gerät beim Verbinden mit einem Netz
 - Zustandsinformationen werden von Agenten auf den Endgeräten geliefert
 - TNC-Server trifft auf dieser Basis die Entscheidung über Zugriff
- ▶ Integriert in 802.1x und IPsec-VPN (d.h. IKEv2) über EAP-Tunnel
- ▶ Standard besteht aus einer Architektur und einer Reihe von Schnittstellen

TNC – Kontrollpunkte

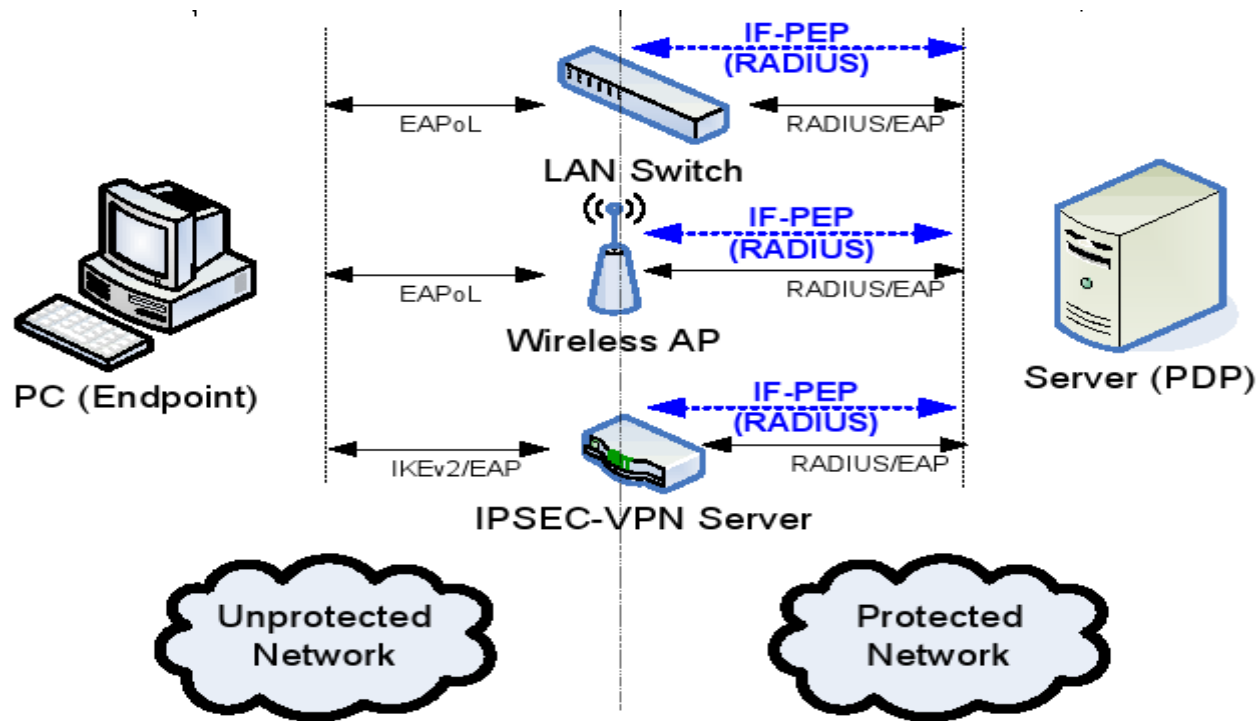
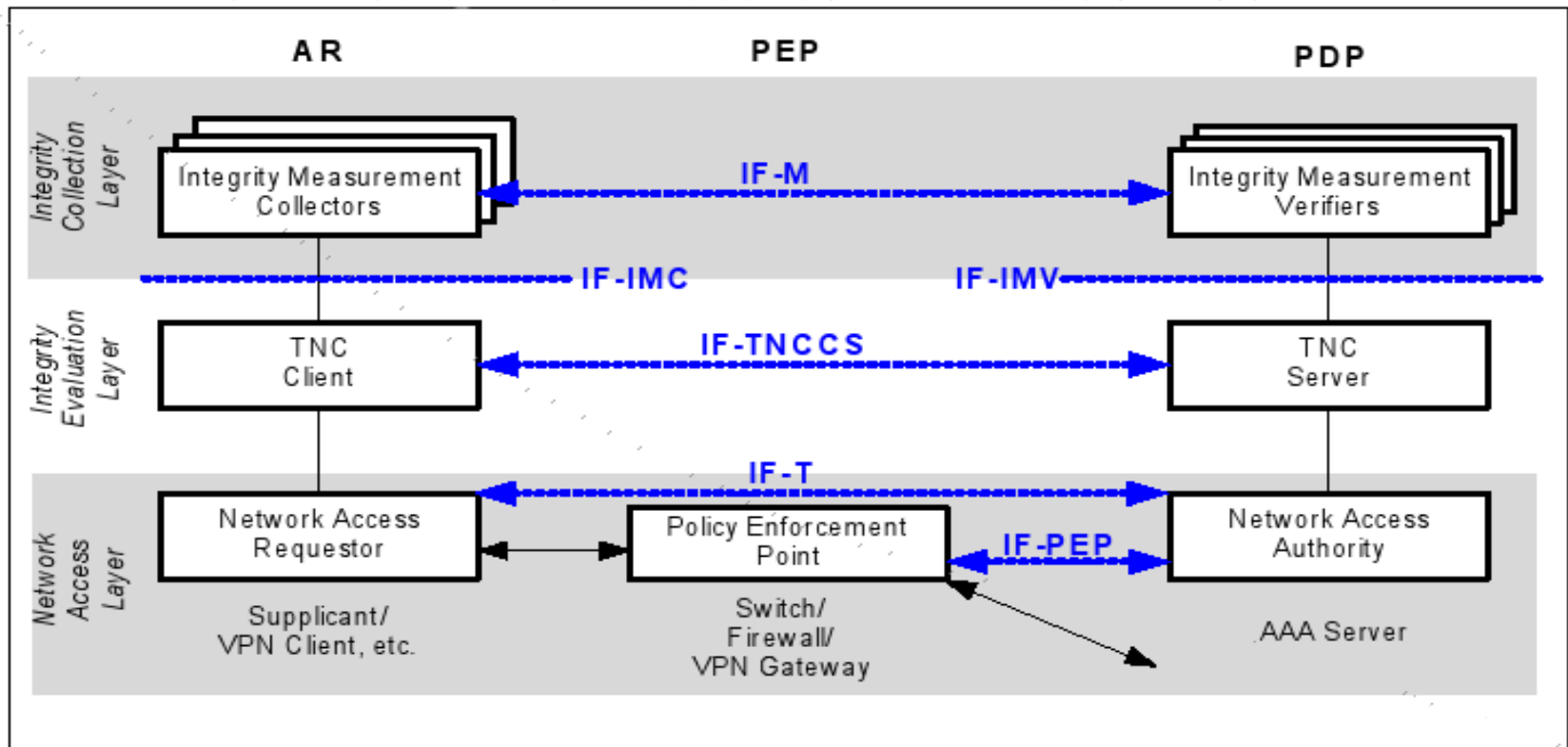


Figure 1 - Network-Based PEP in TNC Architecture

Quelle: Trusted Computing Group

TNC – Architektur



Quelle: Trusted Computing Group

TNC-Client – Vertrauenswürdigkeit

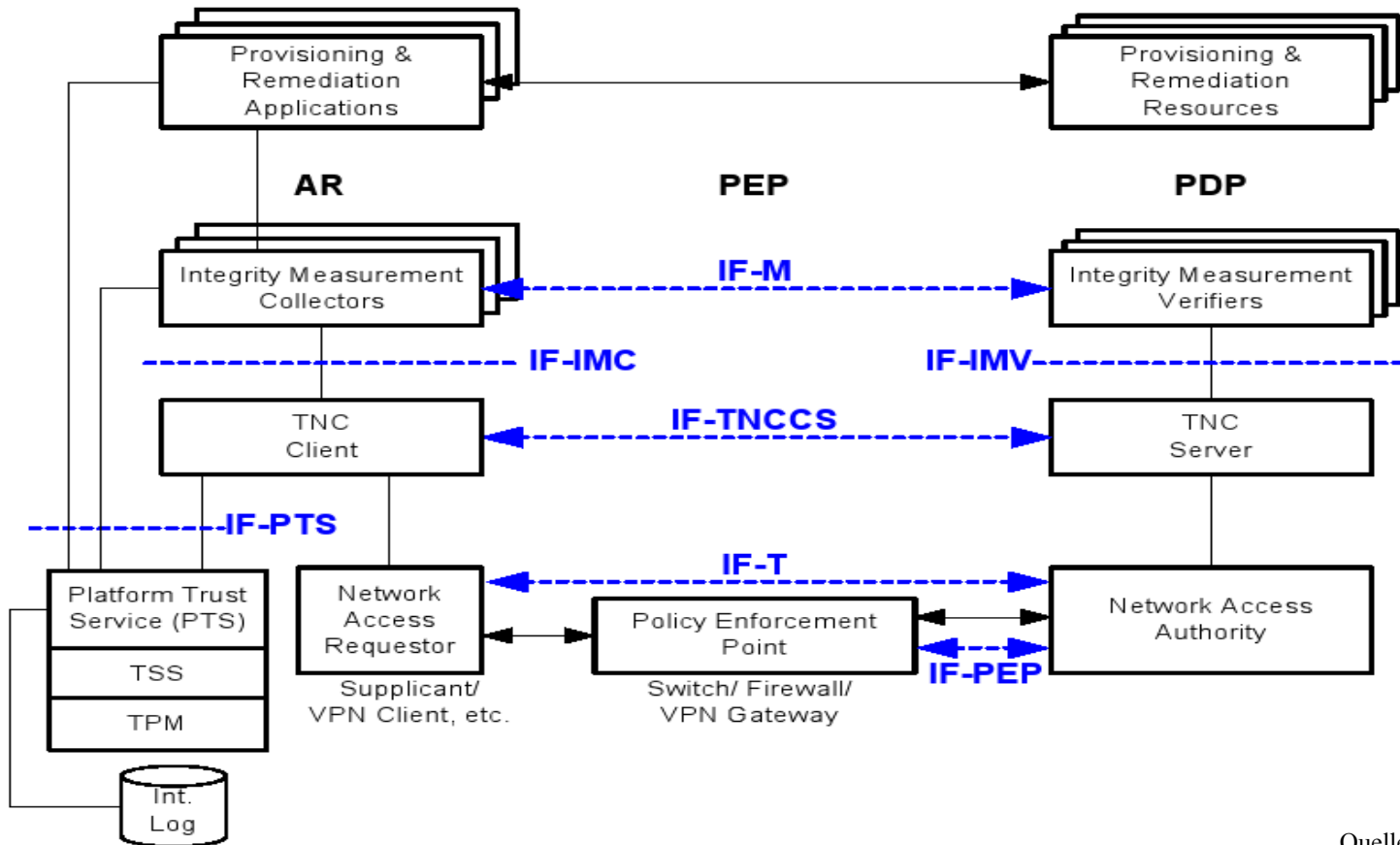
- ▶ Durch TNC wird Angriffsvektor weiter verschoben
 - z.B. Manipulation des Integrity Measurement Collectors
 - Cisco Implementation gilt seit Blackhat 2006 als kompromitiert
- ▶ Hardwareunterstützung wird benötigt um dieses Problem anzugehen
- ▶ Mögliche Lösung: Trusted Platform Module (TPM)

Trusted Platform Module (TPM)

- ▶ TPM für eine hardwarebasierte Authentisierung und Integritätsprüfung
 - Sichert einen “known good state“
 - Authentisiert das Endgerät und kann den Beweis der Integrität an Kommunikationspartner liefern

- ▶ Bildet die “Root of Trust” des Gerätes
 - Sichere Operationen und Schlüsselspeicher in Hardware
 - „Chain of Trust“ von der Hardware über das BIOS und Betriebssystem zur Applikation

TNC – TPM



Quelle: Trusted Computing Group

TNC/TPM – Aktueller Stand

▶ TNC

- Kern-Spezifikationen abgeschlossen
- Erste Produkte wie Switches, Router, VPN-Gateways unterstützen TNC
- Fehlender Schutz gegen Veränderungen der Agenten auf Endgeräten
- Microsofts Statement of health-Protokoll wurde integriert
- Bisher kaum Know-How zum Thema NAC vorhanden

▶ TPM

- Hardware-Chip in vielen Laptop-Systemen bereits vorhanden
- Bisher nur geringe Verwendung durch Anwendungen
- Mobile TPM ist am Anfang der Entwicklung

SIMOIT – Ziele

- ▶ Erhöhte Sicherheit mobiler Endgeräte mit Zugriff auf Unternehmensnetze
- ▶ Entwicklung eines Prototyps einer NAC-Umgebung, basierend auf freier Software
- ▶ Integration in reale Unternehmensumgebung
- ▶ Entwicklung notwendiger organisatorischer Konzepte
- ▶ Aufbau von Know-How im Bereich Network Access Control

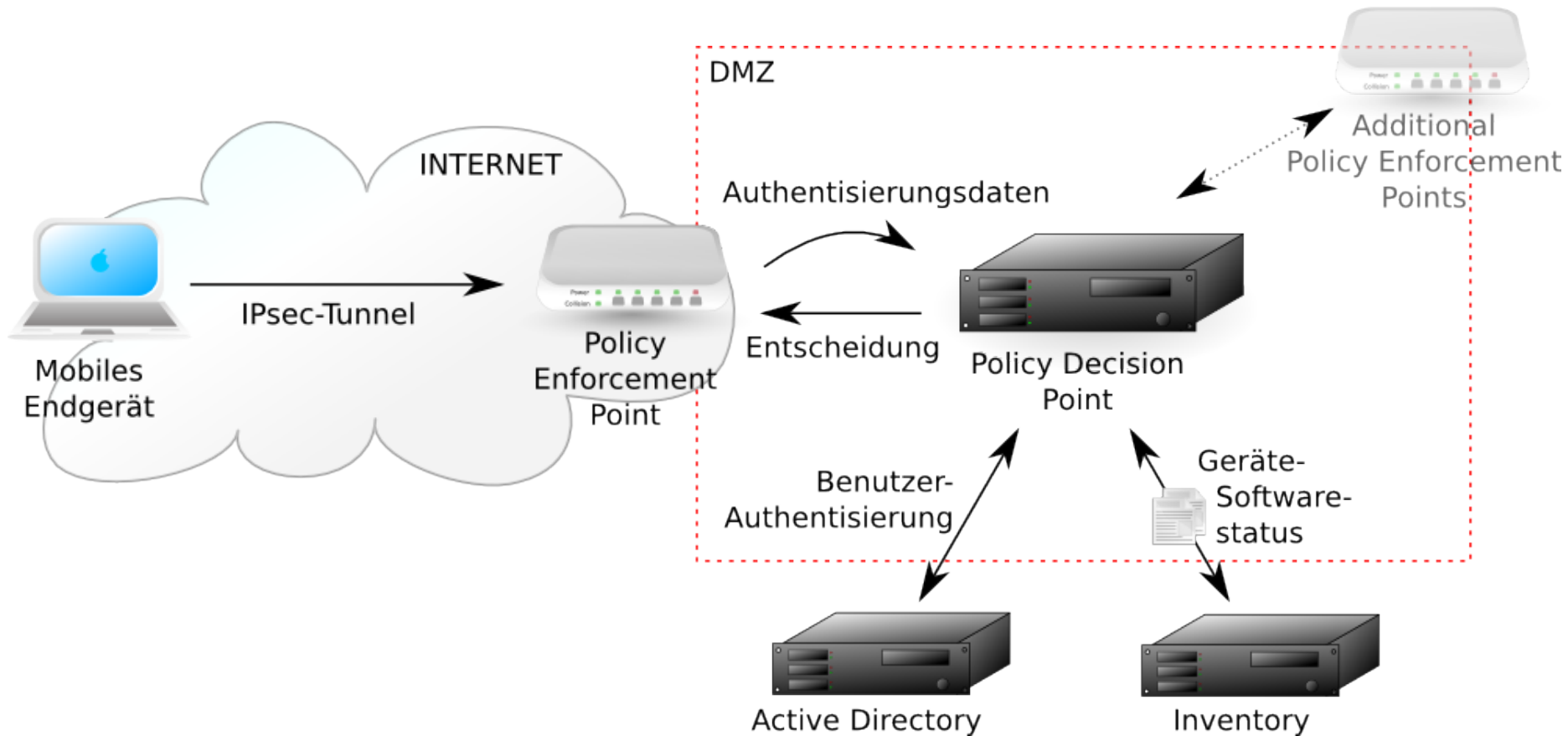
SIMOIT – Gegebenheiten

- ▶ Bisher keine IKEv2-Unterstützung im MS-Windows-IPsec
- ▶ Integration von IKEv2/EAP-fähigen VPN-Clients ist aufwendig
- ▶ Fehlende Schnittstelle zum Softwarezustand des Endgerätes
- ▶ Bisher kein Schutz der Agenten auf den Endgeräten
- ▶ Kein freier TNC-Server verfügbar

SIMOIT – Technischer Ansatz

- ▶ TNC-basiertes Network Access Control
- ▶ Umsetzung des TNC-Standards auf Serverseite
- ▶ Entscheidung über Integrität der Endgeräte aufgrund von Infrastrukturinformationen
- ▶ Einfacher Übergang auf vollständigen TNC-Standard durch Nähe zur Spezifikation

Architecture



Implementierung

- ▶ **Mobile Endgeräte**
 - Betriebssysteme: Microsoft Windows XP, Windows Mobile 6
 - VPN-Client: MS Windows IPsec Stack

- ▶ **Policy Enforcement Point**
 - VPN-Server: Openswan, xl2tpd, pppd

- ▶ **Policy Decision Point**
 - AAA: FreeRADIUS
 - TNC-Server: FreeRADIUS-Modul
 - TNC-Framework: libtnc
 - IMV für Softwareverteilung

Ausblick

- ▶ Unterstützung von standardisierten TNC Komponenten
 - Clientseitige Software Agenten
 - IKEv2/EAP-basierte VPN Authentifizierung
- ▶ Hinzufügen weiterer Integritätsprüfungen.
- ▶ Nutzung des Trusted Platform Module zum Schutz des Software-Agenten

Fazit

- ▶ Große Dynamik im NAC-Markt
- ▶ Bisher nur begrenzte Interoperabilität der existierenden Network Access Control Technologien
- ▶ Standardisierungsbemühungen der Hersteller von NAC-Lösungen

- ▶ NAC ist ein weiteres sinnvolles Werkzeug zur Absicherung der Unternehmensnetz
- ▶ Große Anforderungen an die organisatorische IT-Sicherheit für einen erfolgreichen NAC-Einsatz

Vielen Dank für Ihre Aufmerksamkeit!

Fragen, Kommentare?