

Trusted Network Access Control

→ Vertrauenswürdige Netzwerkverbindungen

Marian Jungbauer

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

if(is)
internet-sicherheit.

tNAC
trusted network access control

Das Netzwerk wie es sein sollte

Sei höflich zu allen, aber freundschaftlich mit wenigen;
und diese wenigen sollen sich bewähren, ehe du ihnen Vertrauen
schenkst.

George Washington

Netzwerke heute

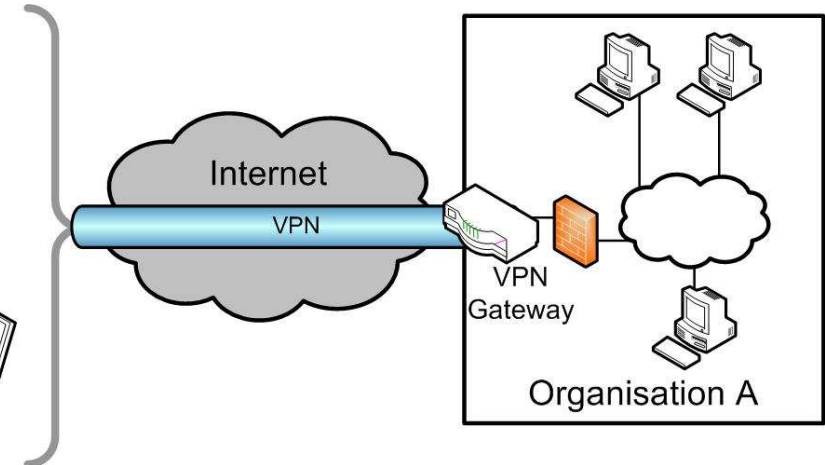
Sei offen zu allen und freundschaftlich mit vielen;
und diese vielen müssen sich nicht bewähren, ehe du ihnen
Vertrauen schenkst.

Einleitung

→ Aktuelle Netzwerke

- **Netzwerkzugriff meist geschützt durch**

- Nutzer-Authentifizierung
- Firewalls,
- VPNs, ...



- **Aber**

- **Keine Überprüfung von angeschlossenen Rechnersystemen**
- Keine Unterscheidung zwischen **vertrauenswürdigen** und **nicht vertrauenswürdigen** Rechnersystemen

- **Konsequenzen**

- Heutige Netzwerkverbindungen sind **nicht vertrauenswürdig**
→ **Keine vertrauenswürdige Kommunikation möglich**

Einleitung

→ Zunehmende Probleme

- **Zunehmende Vernetzung**

- In und zwischen Unternehmen
- Weltweit

→ Nutzung öffentlicher Netzwerke (Internet)

- **Steigende Nutzung sicherheitskritischer Anwendungen**

- Steigender Bedarf an vertrauenswürdiger Kommunikation
- B2B, Online-Banking, uvm.

- **Angestellte „tragen“ Sicherheitsrisiken in die Firmen**

- Außendienst (direkt oder über VPN)
- Mitarbeiter die Familienmitgliedern Zugriff auf Notebooks erlauben
- **Umgehung** etablierter **Sicherheitsmechanismen** (Firewalls, ...)

Einleitung

→ Bedarf neuer Sicherheitstechnologien



- **Bedarf neuer Technologien, die**
 - Zugriffsentscheidungen **so früh wie möglich** und **abhängig vom Zustand** der Rechnersysteme treffen
 - **Vertrauenswürdigen** Rechnersystemen Zugriff **gewähren**, und
 - Zugriff über **nicht vertrauenswürdige** Systeme **ablehnen**

Ansatz

Network Access Control (NAC)

- Einleitung
- **Network Access Control**
- tNAC
- Zusammenfassung

Network Access Control

→ Functions (1/2)



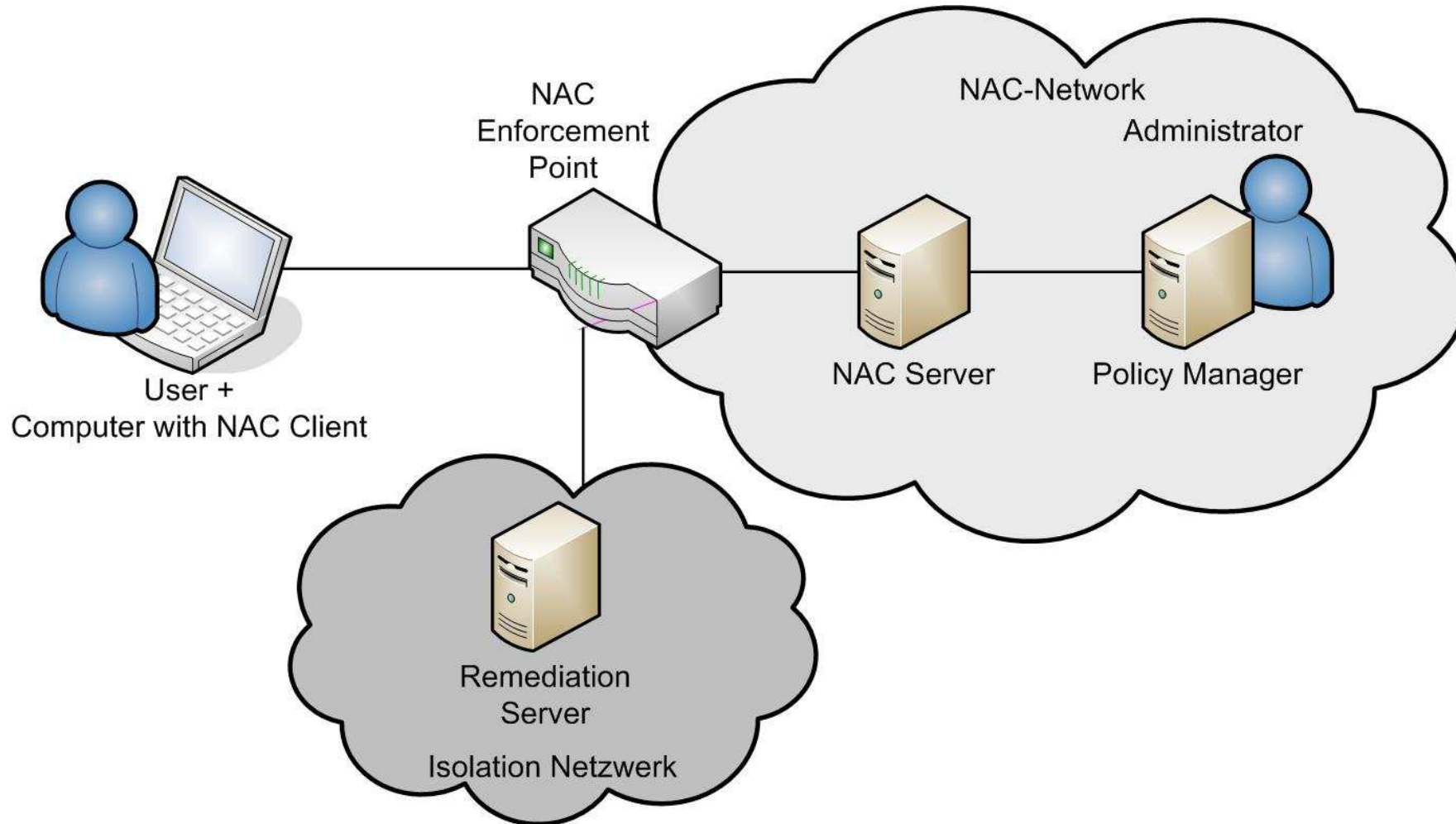
- **Nutzer-Authentifizierung** (z.B. über Passwörter oder Zertifikate)
 - z.B. VPN and IEEE 802.1X

- **Überprüfung der Konfiguration**
 - Messung der Konfiguration **vor** dem Netzwerk-Zugriff
 - z.B. Messwerte über Anti-Virus-Scanner und Personal Firewall
 - Vergleich der Messwerte mit Anforderungen (Policies) des Netzwerks
- **Überprüfung der Integrität von Rechnersystemen**
 - Regelmäßige Messung zugelassener Systeme

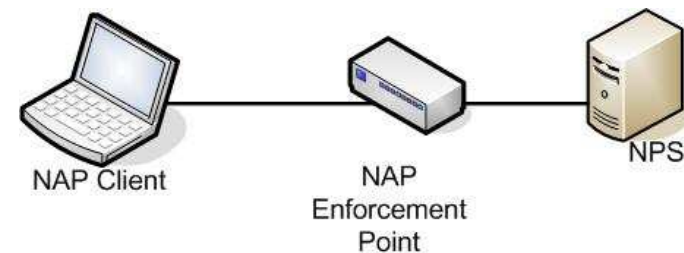
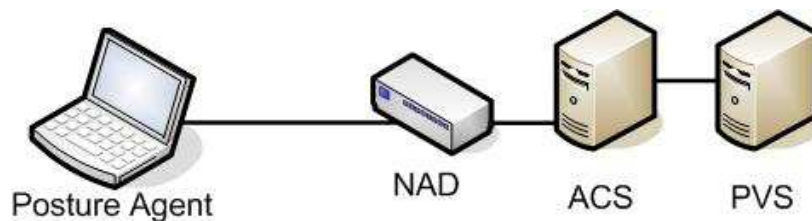
- **Policy Enforcement**
 - Durchsetzen der Policies bei nicht-konformen Rechnersystemen

Network Access Control

→ Topologie



- NAC Lösungen sind bereits verfügbar
- Die bekanntesten
 - Cisco Network Admission Control (Cisco NAC)
 - Microsoft Network Access Protection (NAP)
- Und viele weitere
 - Juniper Unified Access Control
 - StillSecure Safe Access
 - ...

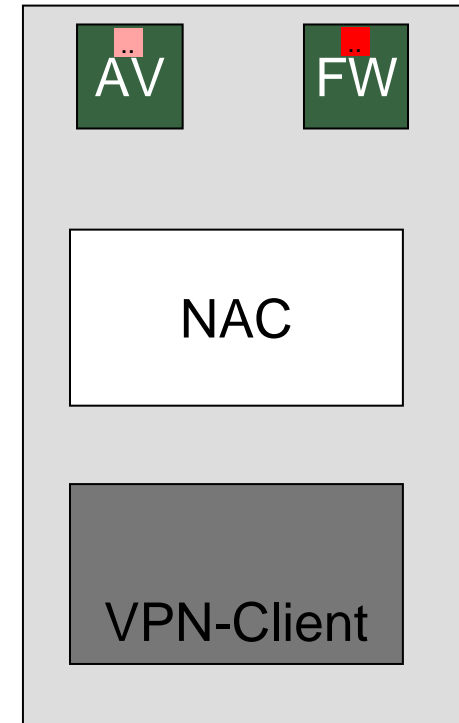


Network Access Control

→ Einschränkungen aktueller Lösungen (1/2)

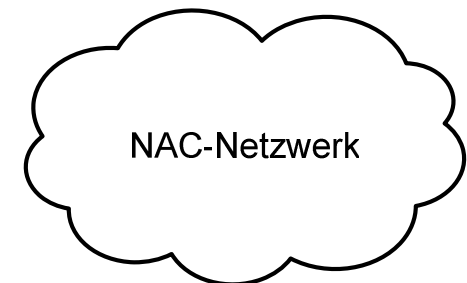
Fehlendes Vertrauen in die Messwerte “lying endpoint problem”

- Grund: Herkömmliche Betriebssysteme ohne Isolation der Komponenten
- Messwerte können kompromittiert werden
- NAC-Komponenten ebenfalls
 - Gezeigt auf der BlackHat-Konferenz 2007
- Paradoxon: Mehr Vertrauen über Messwerte denen aber nicht vertraut werden kann!?



Fehlendes Vertrauen in NAC-Netzwerke

- Nutzer können gemessene Daten nicht kontrollieren
- Mögliche Datenschutz-Probleme



Network Access Control

→ Einschränkungen aktueller Lösungen (1/2)



- **No Standards / No compatibility by design / No platform independence**
 - Unterstützung für alle wichtigen Betriebssysteme ist essentiell
 - Aktuelle NAC Lösungen unterstützen zumeist Microsoft Produkte
 - Alle Lösungen sind meist per Design nicht kompatibel zueinander

- **Zwei Standardisierungsansätze**
 - **Trusted Computing Group: Trusted Network Connect (TNC)**
 - IETF: Network Endpoint Assessment (NEA)

Agenda

- **Einleitung**
- **Network Access Control**
- **tNAC**
- **Zusammenfassung**

▪ Forschungsprojekt

- www.tnac-project.org
- Gestartet im Juli 2008, Laufzeit: 3 Jahre

▪ Konsortium

- FH Gelsenkirchen, if(is)
- FH Hannover
- Datus AG
- Sirrix AG
- Steria Mummert Consulting AG



▪ Gefördert vom Bundesministerium für Bildung und Forschung (BMBF)

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

- **Entwicklung einer vertrauenswürdigen NAC Lösung**
 - TNC kompatibel mit TPM Unterstützung
- **Analyse der Anforderungen und Effektivität von tNAC**
 - im Anwendungsfall bei den Partnern
- **Erfahrungen in den Spezifikations-Prozess der TCG einbringen**
- **Management**
 - Entwicklung von Management-Komponenten für tNAC
 - Policy-Manager
 - Management-Console

- **Basis: Verbindung zweier Forschungsprojekte**

- **Turaya**

- Open Source Sicherheitsplattform
- Strenge Isolation von sicherheitskritischen Prozessen



- **TNC@FHH**

- Open Source Implementierung von Trusted Network Connect (TNC)
- Entwickelt an der FH Hannover
- Ziel: Implementierung aller Kern-Komponenten von TNC
- Aktuell keine TPM Unterstützung

Agenda

- **Einleitung**
- **Network Access Control**
- **tNAC**
- **Zusammenfassung**

- **Steigender Bedarf an vertrauenswürdiger Kommunikation**
 - Aktuelle Netzwerke können dies nicht bieten

- **Das NAC Konzept scheint ein guter Ansatz zu sein**
 - Existierende Lösungen können aber keine Vertrauenswürdigkeit bieten
 - durch den Einsatz auf herkömmlichen Betriebssystemstrukturen

- **TNC ist offen und unterstützt die Verwendung eines TPMs**
 - benötigt aber immer noch ein Vertrauenswürdiges Betriebssystem

- **Das tNAC Projekt will diese Einschränkungen lösen**
 - durch eine Integration in eine Sicherheitsplattform
 - durch Offenheit

Trusted Network Access Control

Vielen Dank für die Aufmerksamkeit

Besuchen Sie uns auf unserem Stand! Halle 9 Stand D06

Marian Jungbauer

Jungbauer {at} internet-sicherheit . de

Institut für Internet-Sicherheit

Fachhochschule Gelsenkirchen

<https://www.internet-sicherheit.de>

