

Trusted Network Access Control

→ Experiences from Adoption

Joerg Vieweg
joerg.vieweg@fh-hannover.de
Trust@FHH Research Group
University of Applied Sciences and Arts Hanover
<https://trust.inform.fh-hannover.de>



- **Introduction**
- **Network Access Control**
- **Trusted Network Connect**
- **Projects**
- **Summary**

Introduction

→ Motivation

Current Situation

- **Networking steadily increases**
 - in and between companies
 - public networks (e.g. internet)
- **Critical Applications**
 - B2B transactions, home banking and many more
- **Critical Infrastructure**
 - Communications-Networks itself
 - public power grid

Current Situation

- **Threats**

- software vulnerabilities (e.g. buffer overflows)
- Viruses, Malware
- ...

- **Problem**

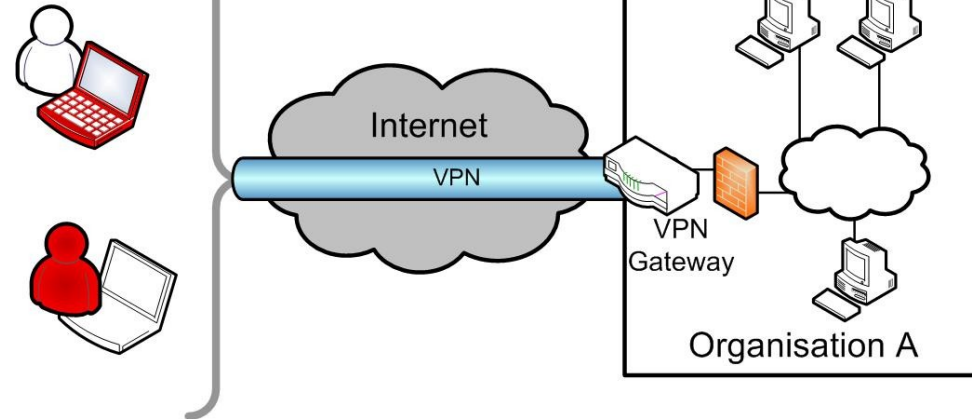
- Countermeasures protect Network against threats from „outside“
- what about threats which are „carried“ into the network
 - e.g. employee who uses notebook also at home or as field worker

Introduction

→ Current security technologies

- **Network access protected mainly by**

- User authentication
- Firewalls,
- VPNs, ...



- **But**

- No integrity checks of connecting or connected computer systems
- No differentiation between trustworthy and not trustworthy computer systems

- **Consequences**

- Connecting device may be a threat for the otherwise protected network

Introduction

→ Need for new approaches

- There's a need for new technologies which
 - make an access decision before a device get (full) network access
 - permit access to computer systems with trusted configuration
 - deny access to computer systems with untrusted configuration

Approach

Network Access Control (NAC)

- **Introduction**
- **Network Access Control**
- **Trusted Network Connect**
- **Projects**
- **Summary**

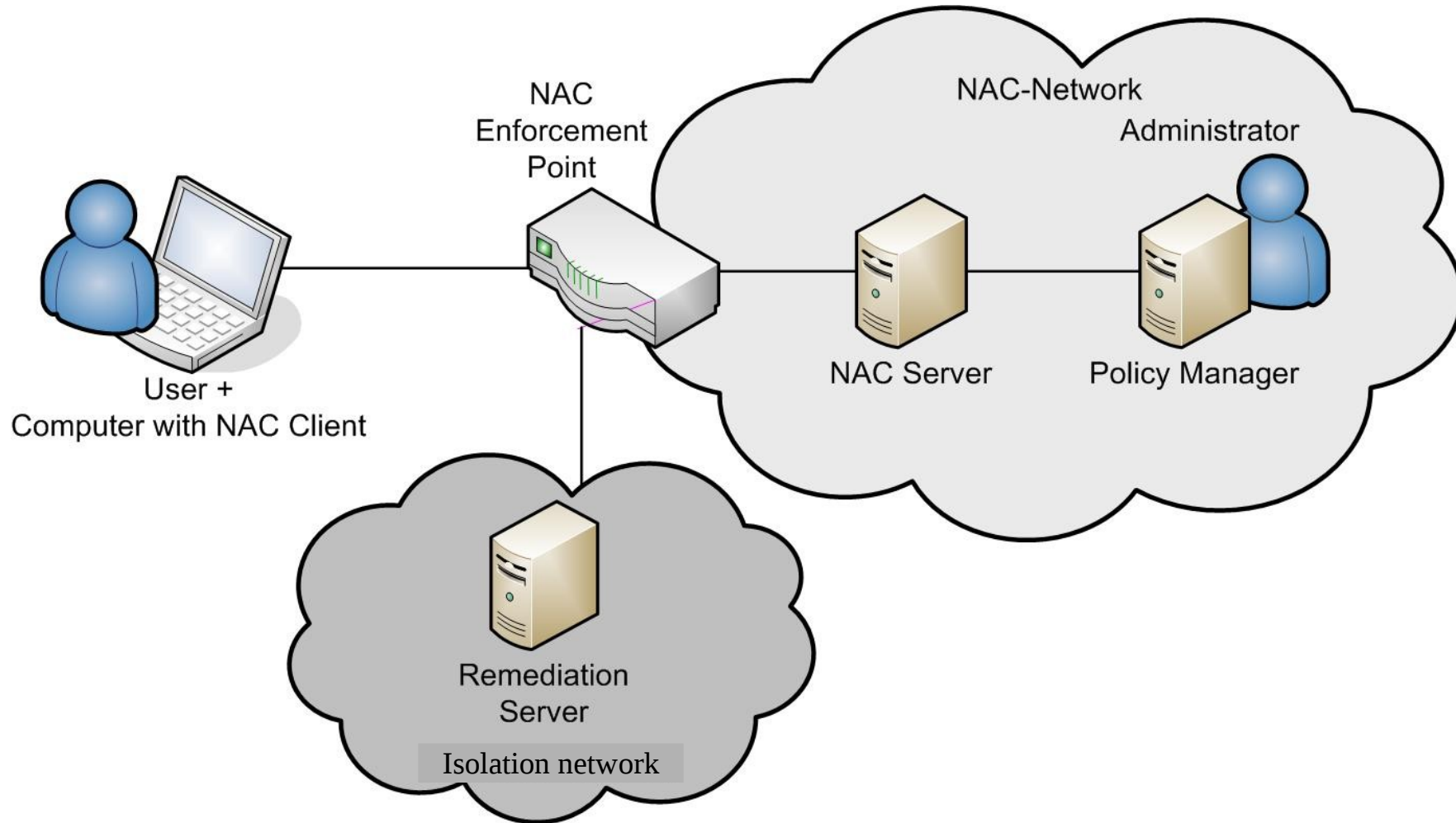
Network Access Control

→ Functions (1/2)

- **User Authentication**
 - User Authentication (e.g. password or certificates)
 - e.g. VPN and IEEE 802.1X
- **Configuration Assessment**
 - Configuration measurement **before** network access is granted
 - e.g. installed software like antivirus scanner and Firewall
 - Compare measurements to policies of the network to access
 - ➔ **Integrity check of the computer system**
 - Re-assess accepted computer systems in regular intervals
- **Policy Enforcement**
 - Enforce policies to non-compliant computer systems

Network Access Control

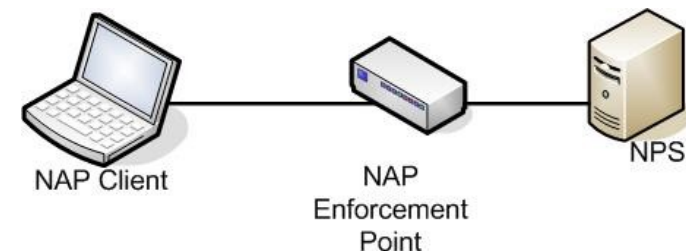
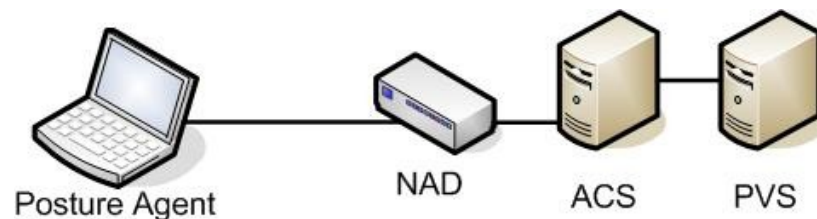
→ Topology



Network Access Control

→ Solutions

- NAC solutions already available on the market
- The most prominent:
 - Cisco Network Admission Control (Cisco NAC)
 - Microsoft Network Access Protection (NAP)
- And many more:
 - Juniper Unified Access Control
 - StillSecure Safe Access
 - ...



Network Access Control

→ Limitations of current solutions (1/3)

Lack of trust in the measurements

The “lying endpoint problem”

- Caused by current OS without isolation of components
- Measured components can get compromised
- NAC-components can get compromised too
 - Shown on Cisco CTA at BlackHat conference 2007
- Achieve more trustworthiness based on measurements which are not trustworthy?

Lack of trust in NAC enabled networks

- User can't control collected data
- Possible privacy issues

Network Access Control

→ Limitations of current solutions (2/3)

- **No Standards, no compatibility by design**
- **First approaches**
 - Client sided compatibility of Cisco NAC and NAP
 - Microsoft opened their NAP-Client-Server-Protocol „SoH“
 - Compatibility of „smaller“ solutions to Cisco NAC, NAP or TNC
 - e.g. StillSecure Safe Access
- **Two (but one) approaches for standardization**
 - **TCG: Trusted Network Connect (TNC)**
 - IETF: Network Endpoint Assessment (NEA) – using TNC as outline
 - Goal: Standardize the Client-Server-Protokolls

Network Access Control

→ Limitations of current solutions (3/3)

- **Platform independence**
 - Support for every common OS is essential
 - Current NAC solutions support primarily Microsoft products

- **Political challenges**

“Who defines what is considered as being trustworthy?”

 - Vendors of NAC and/or security solutions?
 - Network operator?
 - Third Party?
 - All together?

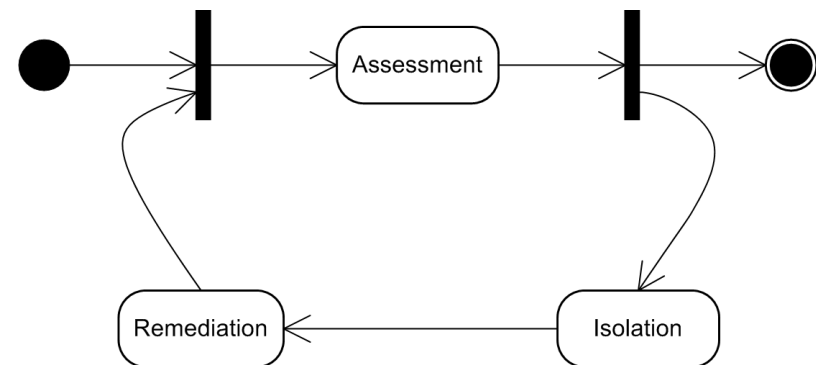
- **Einführung**
- **Network Access Control**
- **Trusted Network Connect**
- **Projects**
- **Summary**

- **Open Architecture for NAC**
 - Specified by the TNC Subgroup of the TCG
 - All specifications are publically available
 - Enables multi-vendor interoperability
 - Supports existing technologies (802.1X, EAP)



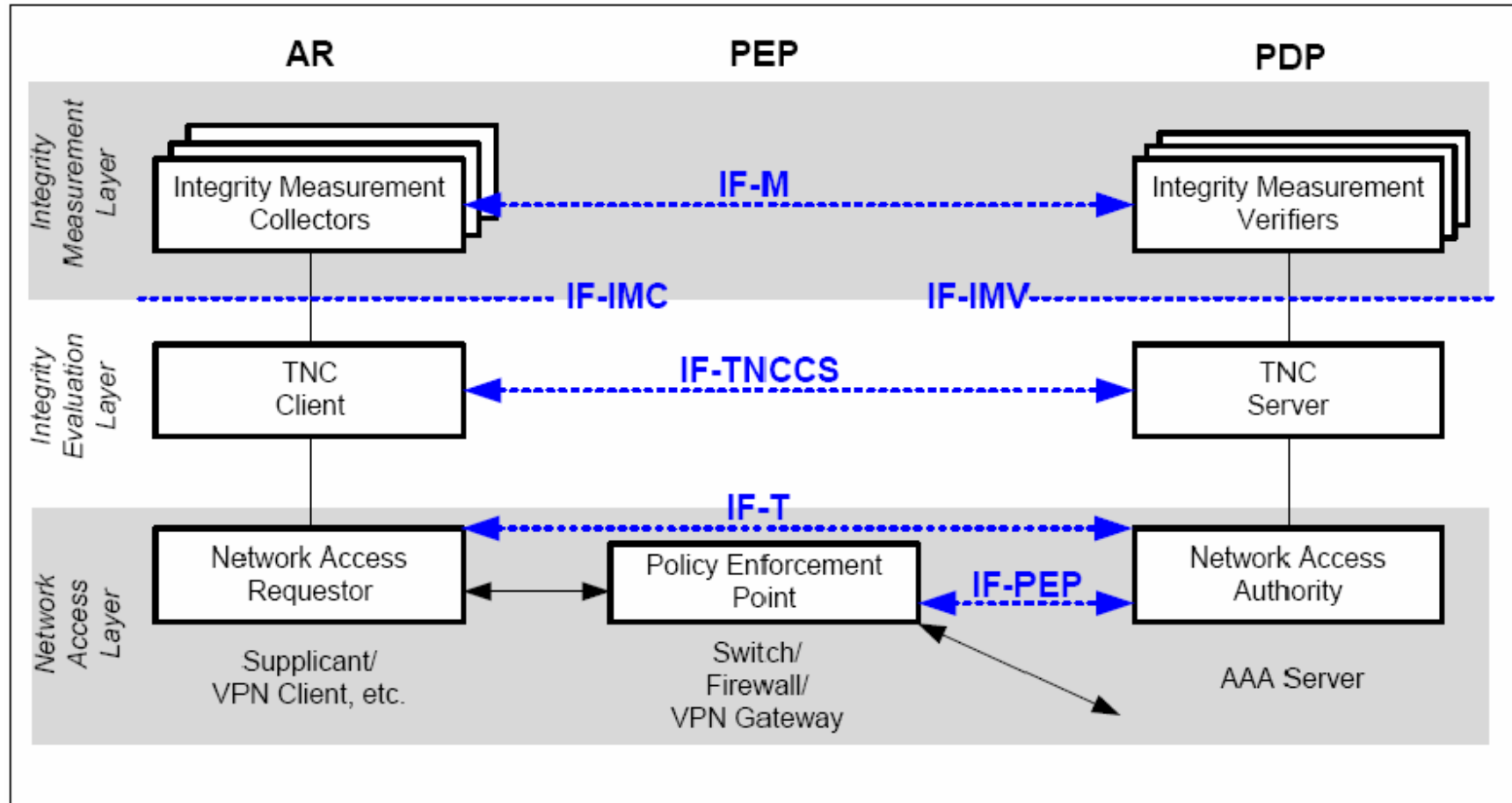
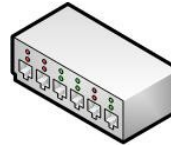
- **TNC Handshake consists of 3 phases**

- **Assessment**
 - TNC Platform Authentication
 - Identity + integrity of platform
- **Isolation**
 - Quarantine non-healthy endpoints
- **Remediation**
 - Fix problems and make endpoint healthy again



Trusted Network Connect

→ Basic Architecture

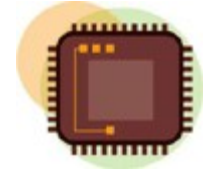


[TNC Architecture for Interoperability Specification version 1.3 revision 6]

Trusted Network Connect

→ TPM Support

- **One main advantage of TNC compared to other NAC solutions**
 - Supports use of the TPM during TNC Handshake
 - Promising approach to solve the „lying endpoint problem“
 - Goal: Ensure integrity of TNC subsystem located on the AR
- **Idea: Use TPM capabilities during TNC Handshake**
 - Create integrity reports (signed)
 - AR sends integrity report to PDP
 - PDP compares received values to known good reference values
 - PDP can verify integrity of TNC subsystem
- **AR cannot successfully lie about its current integrity state!**



Trusted Network Connect

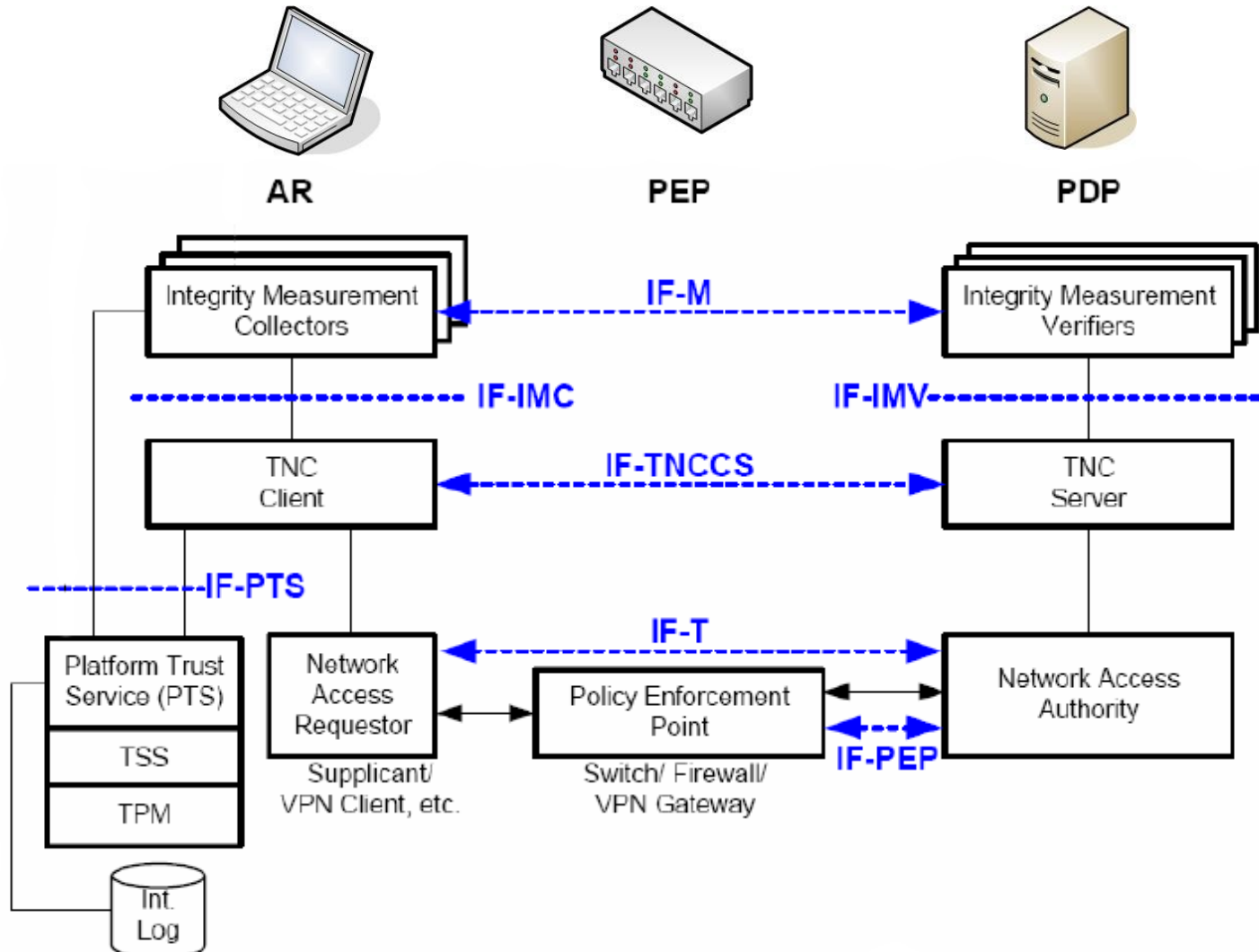
→ TPM Support - additional components

- **PTS (Platform Trust Services)**
 - System service on the AR
 - Exposes Trusted Platform capabilities to TNC components

- **Further components**
 - TPM (Trusted Platform Module)
 - Implements Trusted Platform's capabilities
 - TSS (Trusted Software Stack)
 - Exposes high level interface to TPM for applications
 - IML (Integrity Measurement Log)
 - Stores list of integrity measurements on AR

Trusted Network Connect

→ TPM Extended Architecture



[TNC Architecture for Interoperability Specification version 1.3 revision 6]

- **Creates integrity reports**
 - Makes them available to IMCs / TNCC
 - Enables them to be used during TNC Handshake
 - Ensures that they are rendered in an standardized format
 - TCG Schema Specifications

- **Measures integrity status of ...**
 - TNC components
 - On disk & in memory measurements
 - Appends measurements to IML

- **Why should one trust the PTS ?**
 - Part of the so called Chain of Trust

Trusted Network Connect

→ Chain of Trust

- **Transitive measurement chain**
 - started at the Root of Trust for Measurement (Trust Anchor)
 - components are measured before they are started
 - measurement values are safely stored
 - result is a integrity statement about the platform
 - compromising of components can be detected when checking integrity value against known good values
- PTS part of the Chain of Trust

Trusted Network Connect

→ Further Integrity Checks

- **Motivation**
 - Check integrity of further applications on the AR
 - E.g. Anti Virus, Firewall ... in addition to its configuration
- **Application specific IMC/IMV pair interacting with PTS**
 - IMC/IMV pair measures configuration and integrity
 - Needs to interact with PTS ... standardized but quite involved
 - What about standardized IF-M?

- **Introduction**
- **Network Access Control**
- **Trusted Network Connect**
- **Projects**
- **Summary**

Projects

→ Introduction

- Currently, three projects with trust@fhh research group involvement
 - TNC@FHH
 - IFMAP@FHH
 - tNAC

- TNC@FHH
 - Open source based implementation of TNC
 - Developed at University of Applied Sciences and Arts Hannover
 - Implements all core TNC components/layers/interfaces
 - No TPM support ... yet
 - Been tested within several TNC Environments
 - No AR component
 - relies on standalone products
 - wpa_supplicant
 - XSupplicant
 - only support for 802.1X... yet
 - used within the tNAC-Project

- **Research Project:**
 - Started on July, 1st 2008
 - Scheduled for 3 years
- **Consortium consisting of**
 - University of Applied Sciences Gelsenkirchen
 - University of Applied Sciences and Arts Hannover
 - Ruhr-Universität Bochum
 - Datus AG
 - Sirrix AG
 - Steria Mummert Consulting AG
- **Sponsored by the Federal Ministry of Education and Research**

SPONSORED BY THE

Federal Ministry
of Education
and Research

www.bmbwf.de

- **Develop a Trusted Network Access Control Solution**
 - TNC compatible NAC solution with full TPM support

- **Integration of a security Platform**
 - Turaya (EMSCB)

- **Participate in TCG's specification process**
 - Contribution to IF-M between PTS-IMC/IMV

- **Management**
 - Keep (t)NAC manageable (Policy-Manager, Management-Console)
 - Focus on usability as well as technology

- **Another Project, besides the direct TNC-Context:**
 - IFMAP@FHH
- **Implements TCG's IF-MAP specification**
 - Server component:
 - MAP: Metadata Access Point
 - Component which collects network-related information and makes those information available for use
 - Client components
 - possess context-related information (e.g. firewall knows sth. about blocked traffic)
 - send (publish) those information to the MAP Server
 - receive (subscribe) information from the MAP Server for further use (e.g. firewall responding to threats detected by the IDS)

Agenda

- **Introduction**
- **Network Access Control**
- **Trusted Network Connect**
- **Projects**
- **Summary**

Summary

- **Endpoint becoming critical point**
- **Lack of trust against the Endpoint**
- **NAC concept seems to be a good approach**
- **Current solutions can't achieve the promised trust level**
- **TNC is open and supports the utilization of the TPM**
 - may need more work...
- **Several OSS Projects showing that Trusted Computing and OS works together**

Trusted Network Access Control

Thank You

Joerg Vieweg

joerg.vieweg@fh-hannover.de

Trust@FHH Research Group

University of Applied Sciences and Arts Hanover

<https://trust.inform.fh-hannover.de>

