etiss
european
trusted infrastructure
summer school

Trusted Network Connect (TNC)

4th European Trusted Infrastructure Summer School
August / September 2009

Josef von Helden

University of Applied Sciences and Arts, Hanover

josef.vonhelden@fh-hannover.de

Ingo Bente

Jörg Vieweg

Content

- **Introduction**
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- Trust@FHH
  - TNC@FHH
  - tNAC
  - IF-MAP@FHH
- Conclusion

Introduction: Motivation

- Changing network structures
  - from static and homogeneous to dynamic and heterogeneous
  - mobile endpoints connect to and communicate with various networks
    - employees using their notebooks at home and at work
    - guest devices, e.g. consultants, students, …
- Hackers adapting their strategies
  - attacking the weakest IT component of a network: endpoints
  - stay hidden, waiting for crucial moments e.g.
    - spy on passwords,
    - eavesdrop on transactions,
    - doing evil work with the user’s privileges after his/her successful authentication to a service

Introduction: IT security today

- More or less isolated security solutions for specific problems, e.g.
  - firewalls to protect the corporate network against attacks from the outside
  - virus scan engines to find malicious code
  - filter software against spam
  - IDS for alerting in case of suspicion of intrusion
- Seems to be not sufficient to counter present and future attacks, due to
  - changing network structures (s.a.)
  - changing attacks and attacker‘s profiles:
    from script kiddies to cybercrime professionals
  - hardness to track network wide security incidents

Introduction: Vision ...

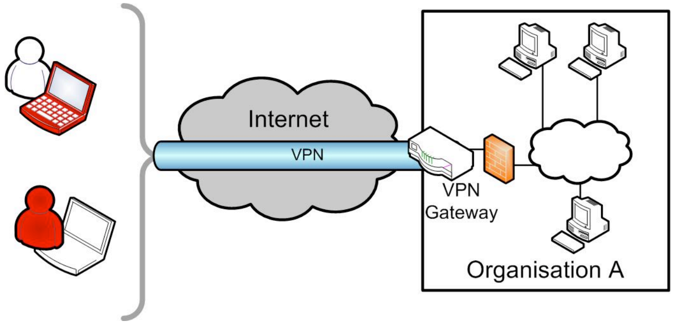
- ... of a modern, effective IT security architecture
- Features
  - distributed
    - with respect to the higher importance of endpoint security
    - security begins at the edge of the network
    - checking of endpoints (integrity and authenticity) before joining the network and periodically thereafter
  - integrated
    - „Security goes inline“: Integration into network devices (eg. switches, access points)
  - cooperative
    - interaction of technologies und tools
  - open / interoperable
    - open specification and standards allow communication between entities from different vendors
  - (centrally) manageble
- Trusted Network Connect (TNC) can play a major role towards such a modern, effective IT security architecture

Content

- Introduction
- **Network Access Control (NAC)**
- Trusted Network Connect (TNC)
- Trust@FHH
  - TNC@FHH
  - tNAC
  - IF-MAP@FHH
- Conclusion

NAC: Threats

- Compromised endpoints are a threat to any network they are connecting to
- Traditional security mechanisms like firewalls, IDS, VPNs, user authentication do not protect against those threats

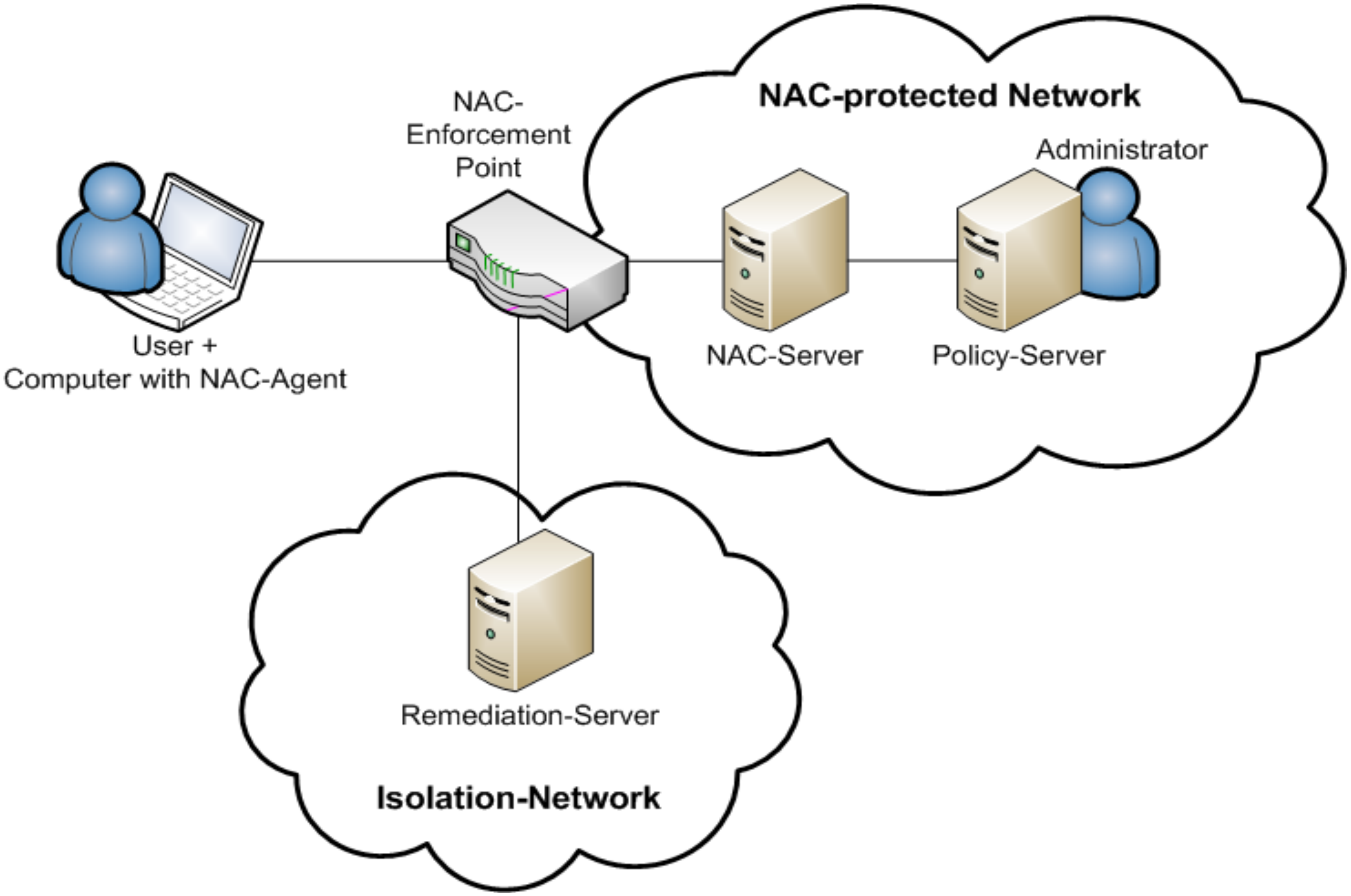


☞Network Access Control (NAC)

NAC: Basic Functionalities

- User Authentication, e.g.
  - based on passwords or certificates
  - via VPN and IEEE 802.1X
- Integrity check of the computer system
  - configuration measurement before network access
    - e.g. installed software like antivirus scanner and firewall
  - compare measurements to policies of the network to access
  - re-assess accepted computer systems in regular intervals
- Policy Enforcement
  - enforce policy decisions
  - give non-compliant computer systems the chance for remediation

NAC: Typical Topology



NAC: Solutions

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

NAC: Requirements

- NAC solutions meet the basic requirements for checking the integrity status of endpoints “by definition”.
- To gain significant benefit (at least) two important requirements have to be fulfilled
  - interoperability
    - enabling multi-vendor support
    - enabling customer’s choice of security solutions and infrastructure
  - unforgeability
    - i.e. the network (resp. a security server in the network) can really trust in the integrity information provided by the endpoint (countering the “lying endpoint problem”)

NAC: Limitations of Current Solutions

- Today, no available NAC solution meets the requirements of interoperability and unforgeability
  - Cisco's NAC and Microsoft's NAP are both proprietary by design
    - interoperability approaches
      - Microsoft opened their NAP-Client-Server-Protocol „SoH“
      - Cisco takes part in IETF WG “Network Endpoint Assessment“
  - NAC-components themselves can get compromised
    - e.g. shown on Cisco CTA at BlackHat conference 2007
- In general: unforgeability presumes having

  (a) a hardware based root of trust which

  (b) also is standardised to meet interoperability

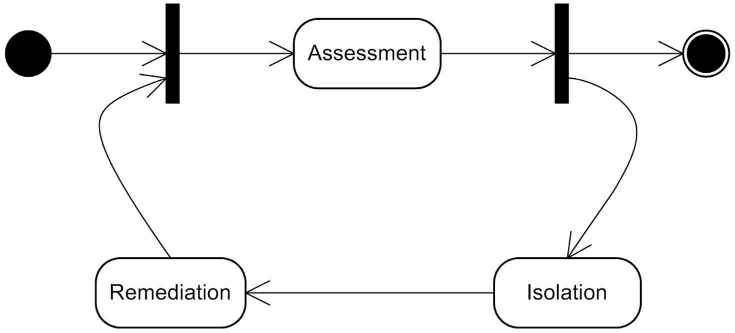
☞ Trusted Network Connect (TNC)

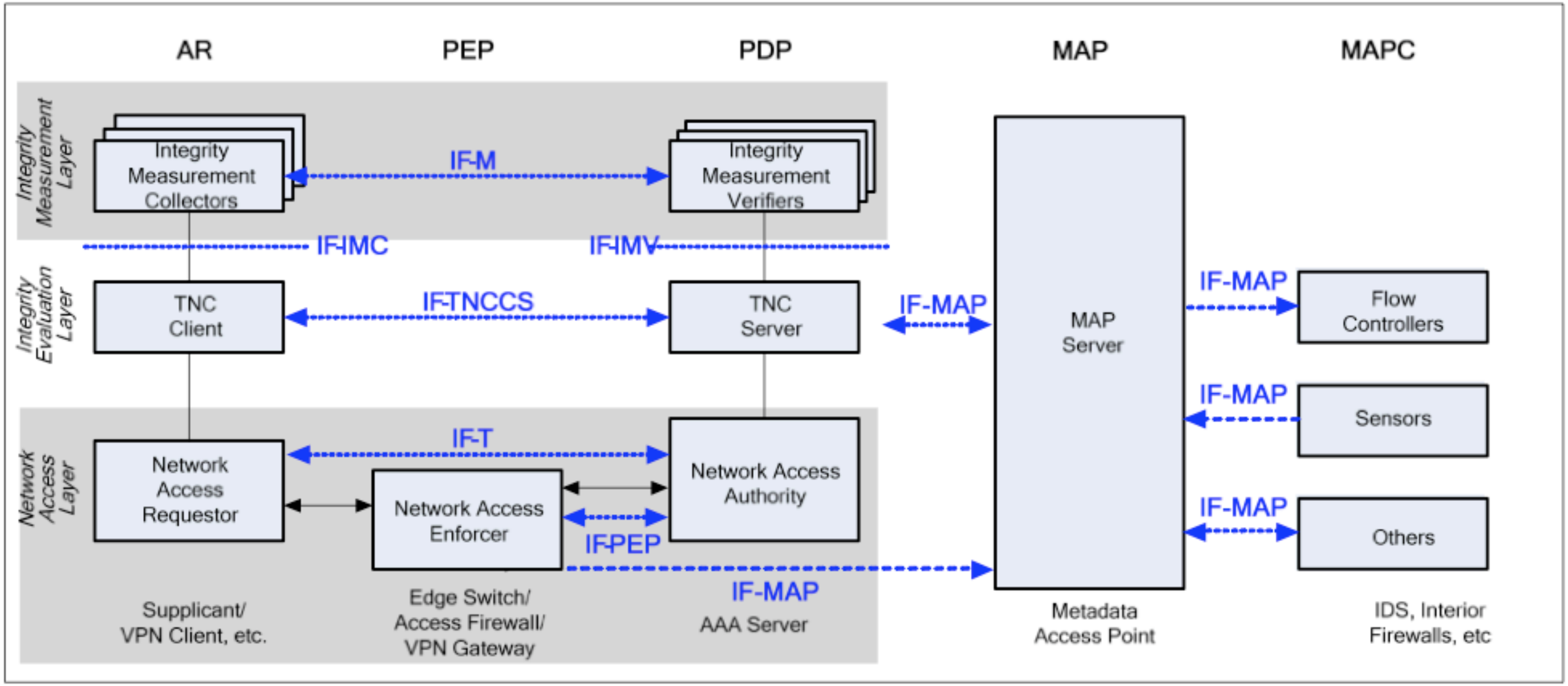
Content

- Introduction
- Network Access Control (NAC)
- **Trusted Network Connect (TNC)**
- Trust@FHH
  - TNC@FHH
  - tNAC
  - IF-MAP@FHH
- Conclusion

TNC: Overview

- Open Architecture for NAC
  - specified by the TNC Subgroup of the TCG
  - all specifications are publicly 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





[TNC Architecture for Interoperability Specification version 1.4 revision 4]

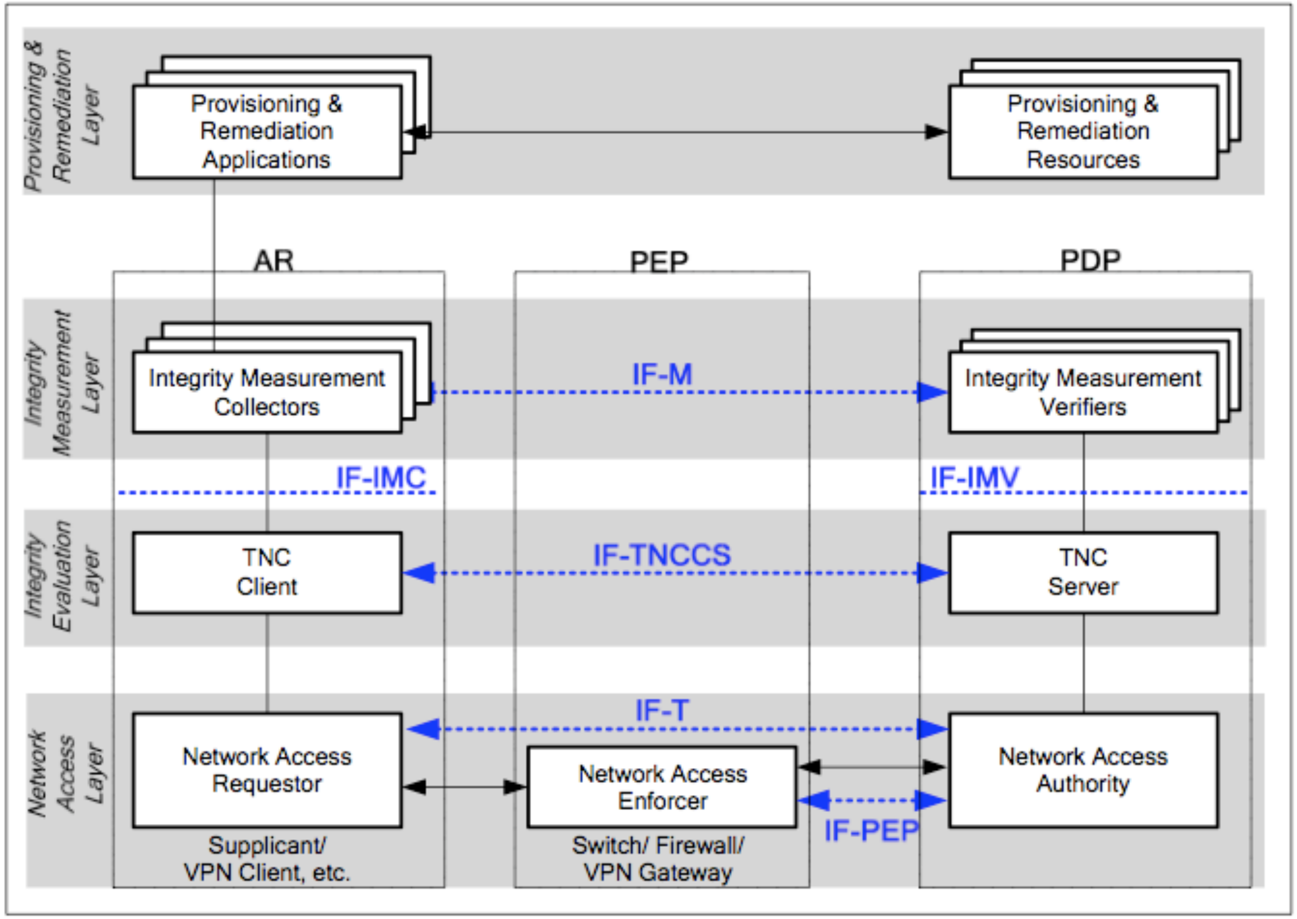
TNC: Required Roles

- Access Requestor (AR)
  - requests access to a protected network
    - typically the endpoint, e.g. notebook, desktop, ...
- Policy Decision Point (PDP)
  - performing the decision-making regarding the AR’s request, in light of the access policies.
    - typically a network server

TNC: Optional Roles

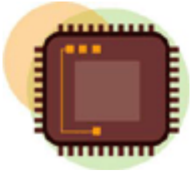
- Policy Enforcement Point (PEP)
  - enforces the decisions of the PDP regarding network access
    - typically a switch, access point or VPN gateway
- Metadata Access Point (MAP)
  - store and provide state information about ARs
    - device bindings, user bindings, registered address bindings, authentication status, endpoint policy compliance status, endpoint behavior, authorization status, ...
- MAP Client (MAPC)
  - publish to, or consume from, the MAP state information about ARs

TNC: Provisioning and Remediation Layer


Provisioning & Remediation Layer
Provisioning & Remediation Applications
Provisioning & Remediation Resources
AR
PEP
PDP
Integrity Measurement Layer
Integrity Measurement Collectors
IF-M
Integrity Measurement Verifiers
IF-IMC
IF-IMV
Integrity Evaluation Layer
TNC Client
IF-TNCCS
TNC Server
Network Access Layer
IF-T
Network Access Requestor
Network Access Enforcer
Network Access Authority
IF-PEP
Supplicant/ VPN Client, etc.
Switch/ Firewall/ VPN Gateway

[TNC Architecture for Interoperability Specification version 1.4 revision 4]

TNC: TPM support



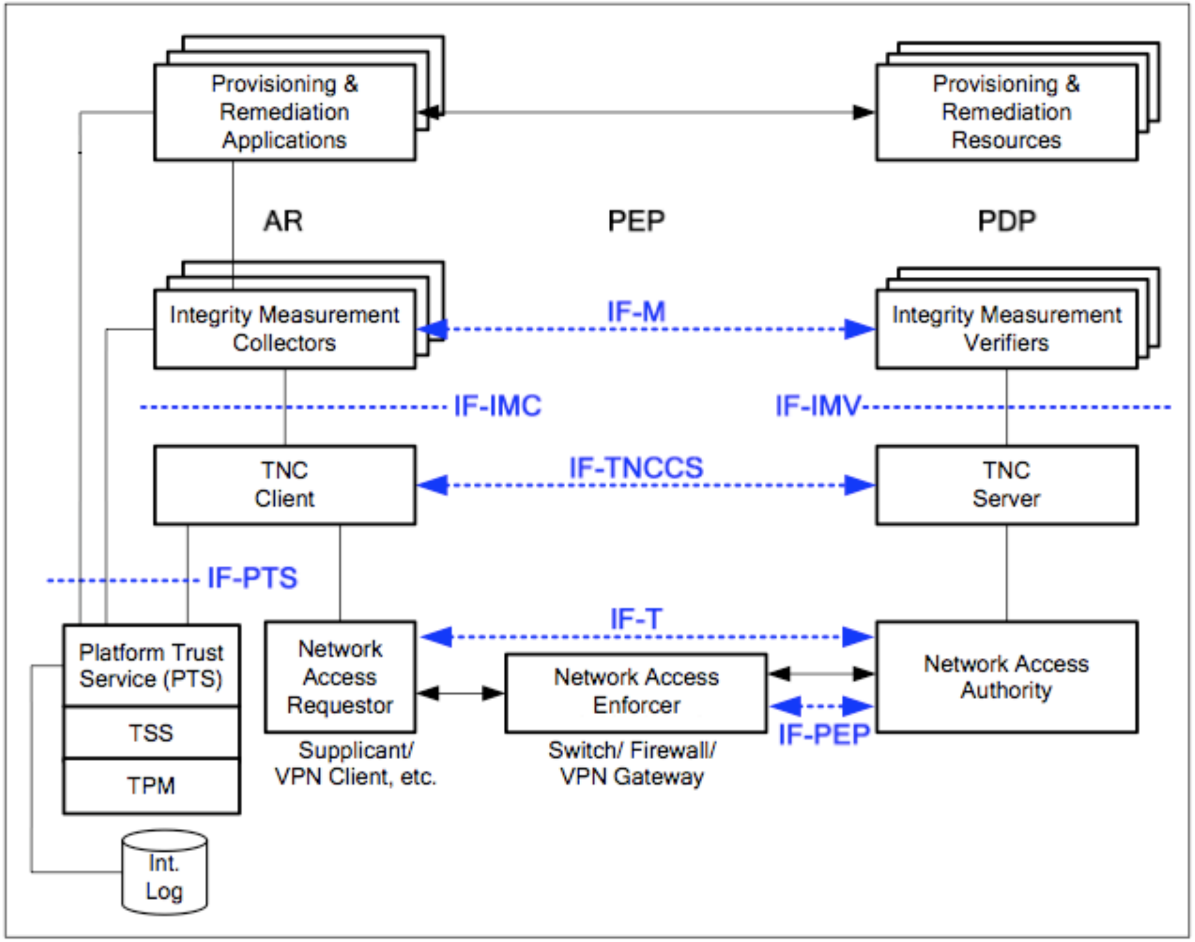
- One main advantage of TNC compared to other NAC solutions
  - supports use of the TPM during TNC Handshake
  - promising approach to solve the „lying endpoint problem“
  - goal: Ensure integrity of TNC subsystem located on the AR
- Idea: Use TPM capabilities during TNC Handshake
  - create integrity reports
    - including signed PCR values
  - 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!

TNC: 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

TNC: TPM extended architecture


Provisioning & Remediation Applications
Provisioning & Remediation Resources
AR
PEP
PDP
Integrity Measurement Collectors
IF-M
Integrity Measurement Verifiers
IF-IMC
IF-IMV
TNC Client
IF-TNCCS
TNC Server
IF-PTS
IF-T
Platform Trust Service (PTS)
TSS
TPM
Network Access Requestor
Network Access Enforcer
Network Access Authority
IF-PEP
Supplicant/ VPN Client, etc.
Switch/ Firewall/ VPN Gateway
Int. Log

[TNC Architecture for Interoperability Specification version 1.4 revision 4]

TNC: Reflecting Interoperability / Unforgeability

- Interoperability
  - generally:
    - fulfilled, because all specifications are publicly available
  - in reality:
    - some experiences with TNC@FHH (see below …)
- Unforgeability
  - generally:
    - fulfilled because TPM support is integrated in the design of the architecture
  - in reality:
    - futher reasearch and devolopment needed
      (see tNAC slides below…)

Content

- Introduction
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- **Trust@FHH**
  - TNC@FHH
  - tNAC
  - IF-MAP@FHH
- Conclusion

Trust@FHH

- Research group at the University of Applied Sciences and Arts in Hanover, Germany
  - research in the area of Trusted Computing, focusing on Trusted Network Connect
- Projects
  - TNC@FHH: open source implementation of the TNC architecture
  - tNAC: research project sponsored by the Federal Ministry of Education and Research
  - IF-MAP@FHH: open source implementation of MAP/MAPC
- More information: trust.inform.fh-hannover.de

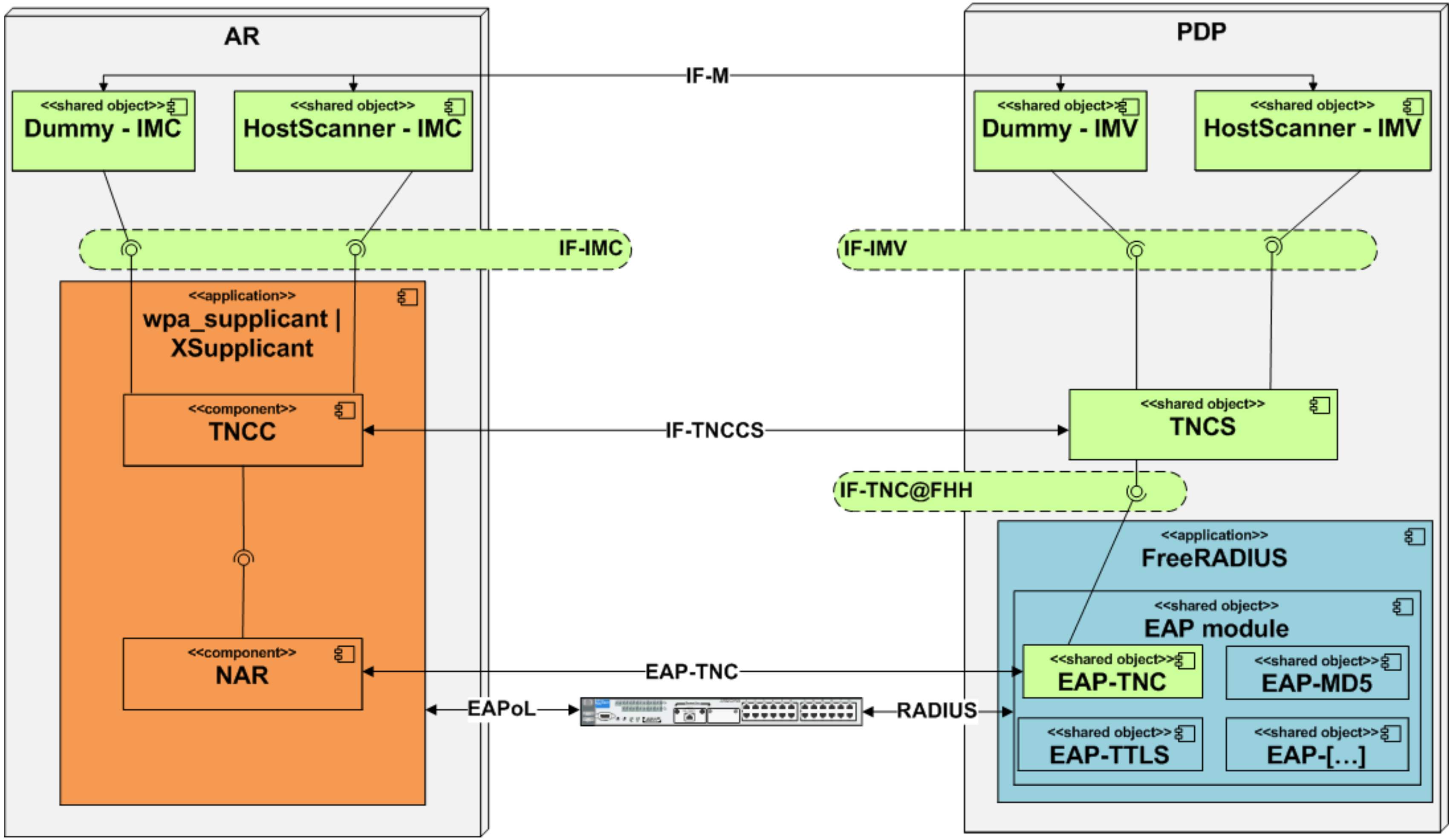
Content

- Introduction
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- Trust@FHH
  - **TNC@FHH**
  - tNAC
  - IF-MAP@FHH
- Conclusion

TNC@FHH: Features

- TNC Server running as an extension of FreeRADIUS
- Several IMC/IMV pairs
- IMC/IMV development framework
- Basic policy management
- Verified interoperability with other TNC implementations (Xsupplicant, wpa_supplicant, libtnc)
  - TNC plugfests 2008 and 2009
- Implemented in C++
- Completely open source

TNC@FHH: Architecture



TNC@FHH: Interoperability

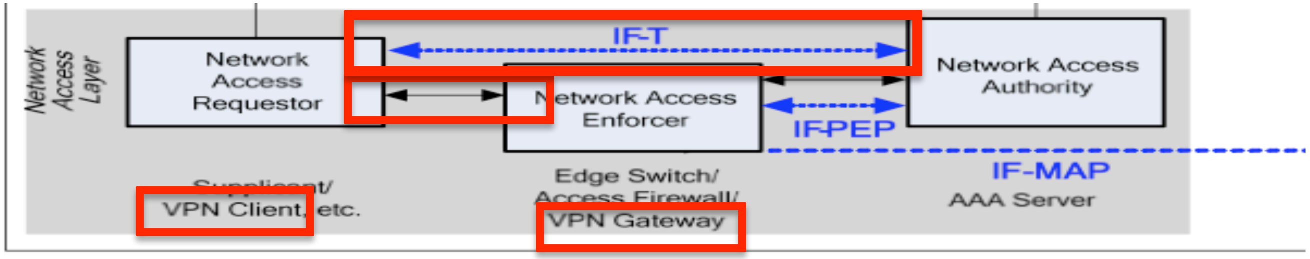
- Results from TNC plugfests in 2008 and 2009
  - different TNC implementations (mainly open source) worked together (almost) without additional effort
  - high degree of interoperability
  - high quality of the TNC specifications
- TNC support by commercial products
  - only few commercial products support parts of the TNC specification
    - IF-IMC / IF-IMV to integrate IMC/IMV-pairs from different vendors
    - IF-PEP to support various PEPs
  - especially IF-TNCCS is at most supported as SOH-Version only
- TNC compliance program is under progress

TNC@FHH *in progress*

- VPN meets TNC
- Privacy enhancements
- Interoperability with MS NAP (IF-TNCCS-SOH)
- Tools: tncsim

TNC@FHH *in progress*: VPN meets TNC (1)

- Objective
  - enabling TNC assessment through VPN connections
- Challenge
  - TNC assessment needs to be carried within the protocol used during the joining process
  - in case of VPN:
    - no 802.1x between AR and PEP
    - AR has an IP address assigned, so is reachable using TCP/IP by other systems



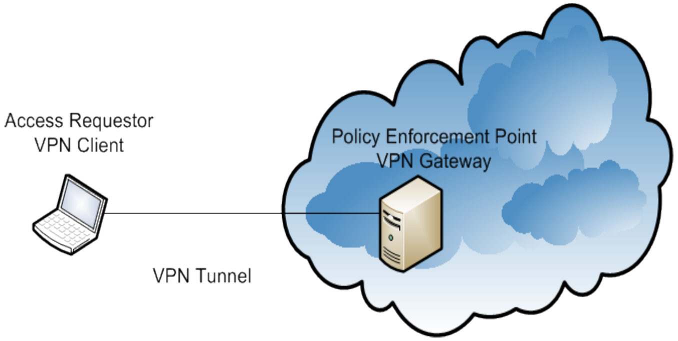
TNC@FHH *in progress*: VPN meets TNC (2)

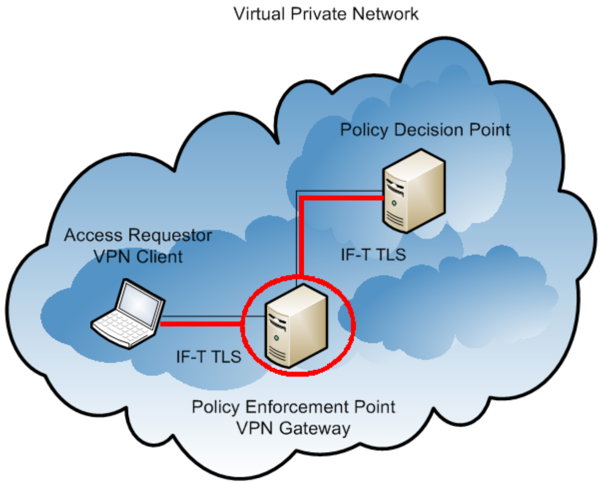
- Common approach: enhancement of VPN software
  - high development effort (if possible at all)
  - support of IKEv2 and Multiple Authentication Exchanges (RFC 4739) is mandatory -> K.O. for mostly all present VPN solutions

- Our approach: TNC through VPN tunnel
  - generic approach works for (almost) every VPN software
  - VPN and TNC software only loosely coupled
  - no adaption of VPN software needed

TNC@FHH *in progress*: VPN meets TNC (3)

- Phase 1:
  - establish VPN tunnel
  - allow communication between AR and PDP only (e.g. through ACLs)
- Phase 2
  - TNC handshake through VPN tunnel using *IF-T binding to TLS*
  - on success: allow general communication of AR using IF-PEP

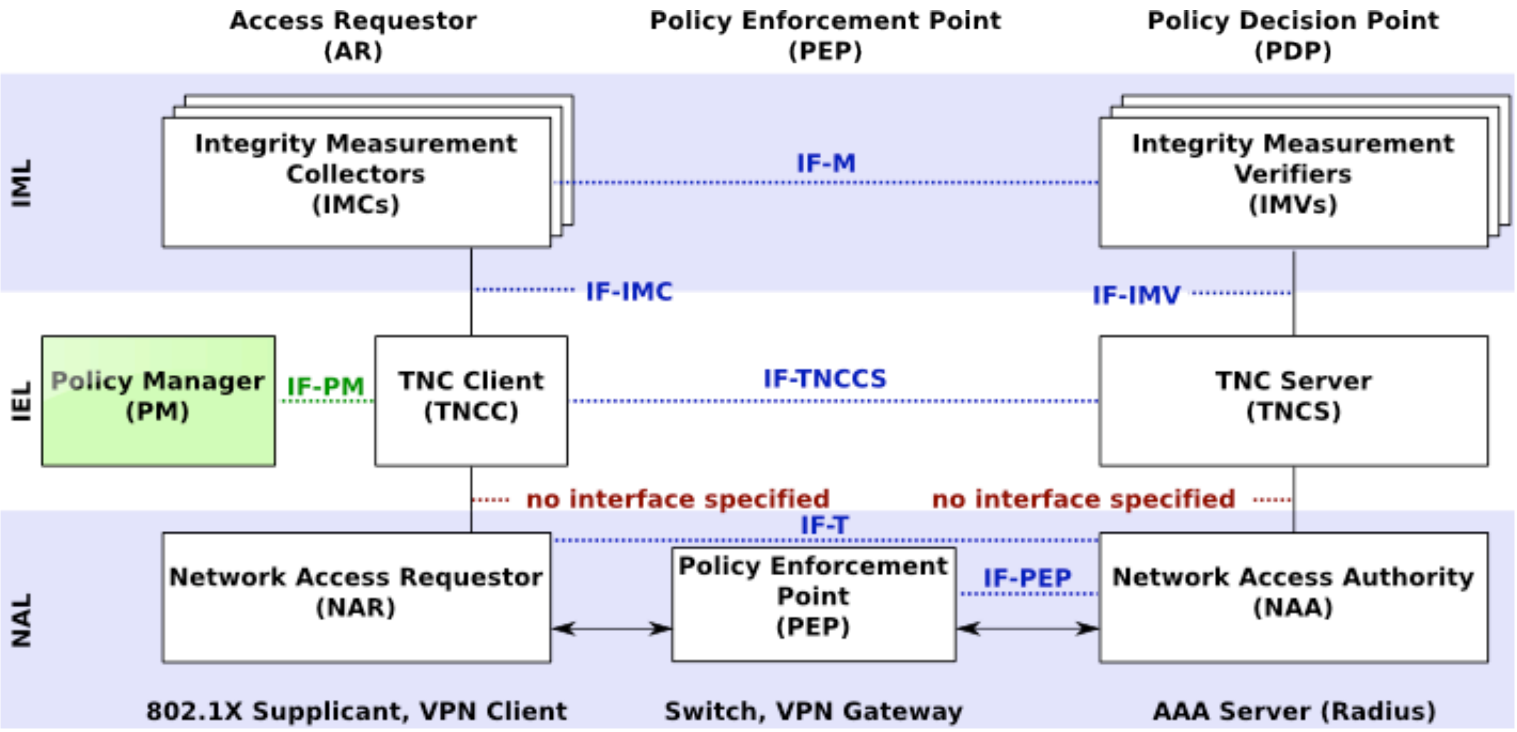




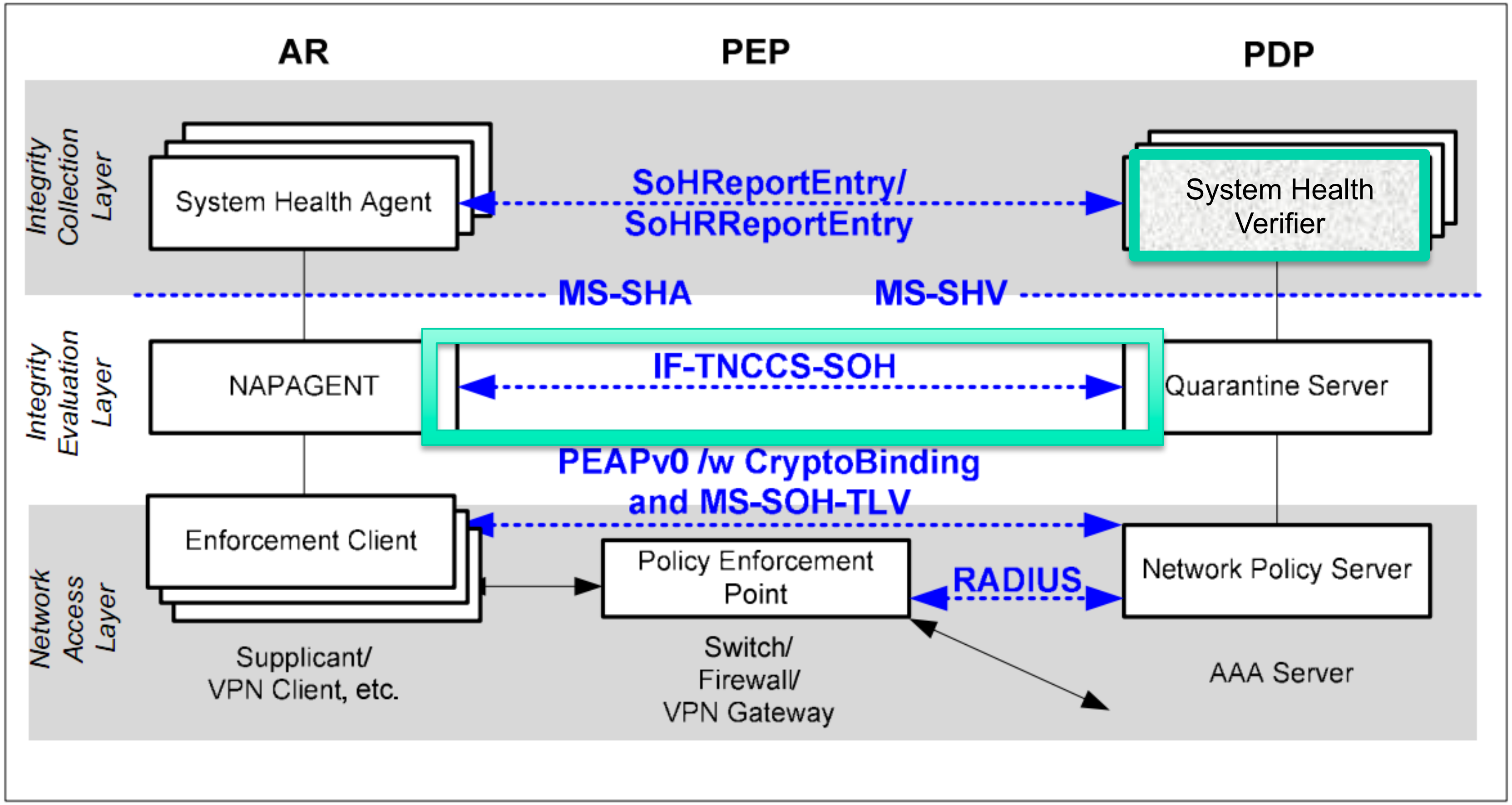
TNC@FHH *in progress*: Privacy enh. (1)

- Problem
  - user has little control over what information is shared during TNC assessment
  - network may ask for information the user considers privacy / security sensitive
  - not acceptable in an environment with multiple trust domains
- Our approach
  - client-side policies based upon IF-M
  - user can specify
    - which information is allowed to be shared
    - depending on the network he is connecting to
  - requires only little modifications to TNC architecture ...

TNC@FHH *in progress*: Privacy enh. (2)


Access Requestor (AR)
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
IML
Integrity Measurement Collectors (IMCs)
IF-M
Integrity Measurement Verifiers (IMVs)
IF-IMC
IF-IMV
IEL
Policy Manager (PM)
IF-PM
TNC Client (TNCC)
IF-TNCCS
TNC Server (TNCS)
no interface specified
no interface specified
IF-T
NAL
Network Access Requestor (NAR)
Policy Enforcement Point (PEP)
IF-PEP
Network Access Authority (NAA)
802.1X Supplicant, VPN Client
Switch, VPN Gateway
AAA Server (Radius)

TNC@FHH *in progress*: IF-TNCCS-SOH (1)



[TNC IF-TNCCS: Protocol Bindings for SoH version 1.0 revision 0.08, May 2007]

TNC@FHH *in progress*: IF-TNCCS-SOH (2)

- Issues
  - no compatability between IF-TNCCS-SoH and standard IF-TNCCS, e.g.
    - Type-Length-Value (TLV) vs. XML
    - only a single exchange of fixed size vs. multiple exchanges and no packet size restriction
  - even without using IMCs (SHAs) measurement of platform properties is possible
    - using Microsofts System Statement of Health (SSoH) message type
    - SSoH measures pre-defined properties, e.g. OS-Version, OS-Patchlevel

TNC@FHH *in progress*: IF-TNCCS-SOH (3)

- Our approach
  - version field of the IF-TNCCS packet specifies used version (IF-TNCCS or IF_TNCCS-SoH)
  - specialised IMV
    - „Standalone“: no appropriate IMC required
    - parses incoming SSoH-messages and responds accordingly (with a SSoHR-message)
    - uses the pre-defined Microsoft Type-Values

TNC@FHH tools: tncsim

- tncsim allows to test TNC components
  - locally on one machine
  - without setting up a test LAN (PEP, PDP on the same machine)
  - AR can be on the same or another machine in the network
- Supports different TNC implementations
  - TNC@FHH
  - libtnc
  - wpa_supplicant
  - Xsupplicant
- Makes development work **a lot** easier

Content

- Introduction
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- Trust@FHH
  - TNC@FHH
  - **tNAC**
  - IF-MAP@FHH
- Conclusion

tNAC: the project

- Research Project:
  - started on July, 1st 2008
  - scheduled for 3 years
- Consortium consisting of
  - University of Applied Sciences and Arts Hanover
  - University of Applied Sciences Gelsenkirchen
  - Ruhr-University Bochum
  - Datus AG
  - Sirrix AG
  - Steria Mummert Consulting AG
  - and some other companies
- Sponsored by the
  Federal Ministry of Education and Research

SPONSORED BY THE
Federal Ministry
of Education
and Research

tNAC: Objectives

- Develop a Trusted Network Access Control Solution
  - TNC compatible NAC solution with full TPM support
- Analyse requirements & evaluate effectiveness of tNAC
  - based upon real world scenarios
- 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

tNAC: Turaya and TNC@FHH

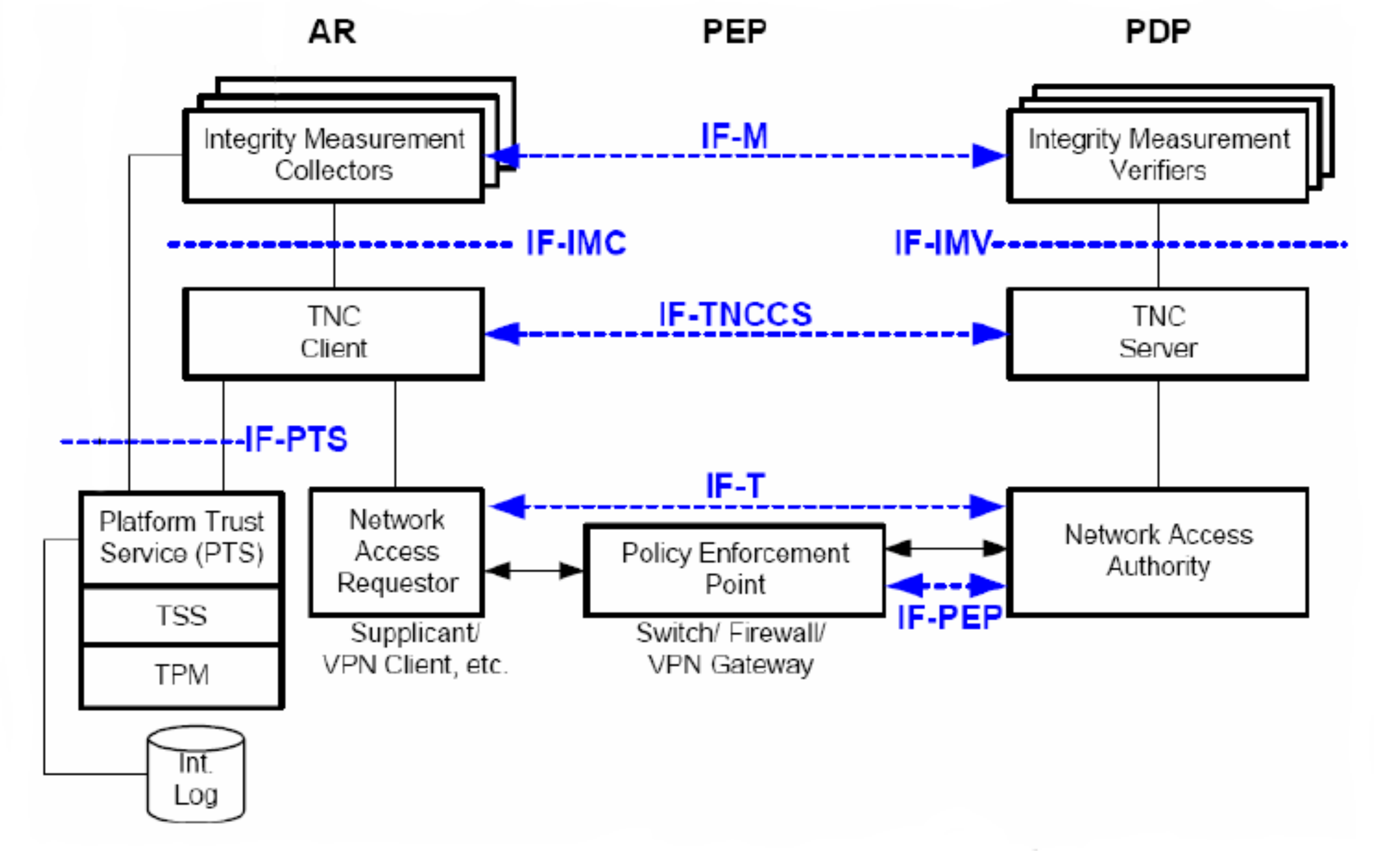
- Combine results of two research projects
- Turaya
  - open source security platform
  - developed by the former EMSCB-Project
  - supports strong isolation of security critical processes in "compartments"
- TNC@FHH
  - open source based implementation of TNC
  - developed at University of Sciences, Hanover
  - implements all core TNC components/layers/interfaces
  - no TPM support … yet

tNAC:
Adoption of TNC in real world scenarios

- security benefit of a TNC solution is evident and desired (by companies)
- several handicaps prevent the adoption today, especially
  - high complexity of policy definition and enforcement
  - efforts and investments required for integration of TNC into the existing IT infrastructure
  - today's impossibility to achieve unforgeability
    - mainly due to the lack of TPM support in standard operating systems
  - missing overall view of network security state
    - lack of cooperation between various security tools

tNAC: coming back to unforgeability…

- … remember the TPM extended architecture



tNAC: PTS features

- Creates integrity reports
  - makes them available to IMCs / TNCC
  - enables them to be used during TNC Handshake
  - ensures that they are rendered in an standardised 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 ?

tNAC: PTS & The Chain of Trust

- PTS must be part of the Chain of Trust
  - measure PTS before execution
  - not supported by „normal“ OS
    - need for a Trusted OS
- PTS responsible for measuring (at least) TNC components
  - TNC components become part of Chain of Trust, too
- Benefit
  - Chain of Trust up to Application Level
    - especially including TNC components on the AR
  - integrity of TNC subsystem can be ensured
    - no lying endpoint problem anymore
- How are integrity reports communicated between AR and PDP ?

tNAC: PTS IMC/IMV

- Special IMC/IMV pair
  - What ?
    - responsible for communicating integrity reports
    - PTS-IMC interfaces with PTS to obtain integrity reports
    - communicates them to PTS-IMV during TNC handshake
    - PTS-IMV evaluates received integrity reports
  - How ?
    - open issue
    - IF-M protocol between IMC/IMV generally implementation specific
    - TCG expects to standardise widely useful IF-M protocols
      - like IF-M between PTS-IMC/IMV
      - essential for interoperability between a PTS-IMC and a PTS-IMV from different vendors

tNAC: Establishing TNC Subsystem Integrity

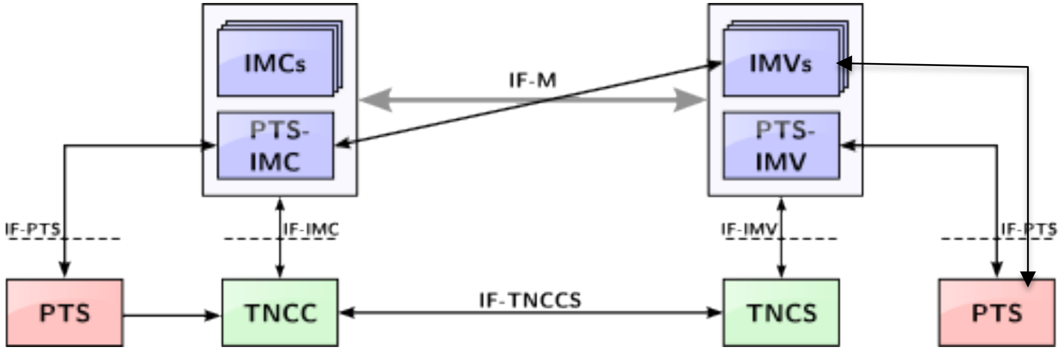
- Collection of Integrity Data
  - Pre-OS Boot
    - Starting from RTM : BIOS, OS-Loader, OS-Image
  - Pre-PTS Startup
    - OS must measure PTS (including TSS)
  - PTS Operation
    - Measure TNC components (NAR, TNCC, PTS-IMC, further IMCs)
    - Render measurements in interoperable format
  - PTS-IMC Collection
    - Obtain Integrity report containing Chain of Trust from PTS
- Reporting to PTS-IMV via IF-M
  - PTS-IMV evaluates integrity report
  - Provides access decision – along with all other IMVs

tNAC: Further Integrity Checks

- Motivation
  - check integrity of further applications on the AR
  - E.g. Anti Virus, Firewall … in addition to its configuration
- (At least) two possible approaches
  - Application specific IMC/IMV pair interacting with PTS
    - IMC/IMV pair measures configuration and integrity
    - needs to interact with PTS … standardised but quite advanced
    - What about standardised IF-M?
  - PTS-IMC/IMV measures further integrity aspects
    - IF-M must support that PTS-IMV requests integrity checks of arbitrary components
    - no need for application specific IMC/IMV pair to care about PTS
    - very complex process of decision making

tNAC *in progress*: PTS-IMC/IMV approach

- Cross over communication
  - any IMV can request integrity measurements from an AR
  - only the PTS-IMC issues the necessary measurements
  - all measurements are encapsulated in one Integrity Report
  - all IMVs verify their specific part of the IR with the PTS



IF-MAP@FHH *in progress*: MAP Server

- Started in September 2008 (project of master students)
- Work in progress
- Current status
  - implementation based upon Java Web Services
    - (SOAP/HTTP, WSDL, Apache CXF)
  - most functions of IF-MAP API are implemented
    - establishing a session
    - publish / subscribe
    - basic search operations
- so far no real MAP clients
  - SOAP UI was used to generate test messages

IF-MAP@FHH *in progress*: MAP Clients

- Project of bachelor students will start in September 2009
  - 14 students
  - scheduled for 12 months
- Objectives
  - improve implementation of existing MAP server
    - Especially regarding data model / search operations
  - develop reasonable MAP clients
    - Snort
    - iptables
    - dhcp
    - nagios
    - TNC@FHH

Content

- Introduction
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- TNC@FHH
- tNAC
- **Conclusion**

Conclusion (1/3)

- TNC has some very important features to act as part of a modern, effective IT security architecture
  - distributed and integrated (general NAC features)
  - interoperable
    - due to its openness
  - unforgeable (by design)
    - thus potentially very effective
  - cooperative
    - due to the MAP approach
  - (manageability is out of scope of the TNC spec)

Conclusion (2/3)

- Some issues
  - unforgeability is well designed in theory but hard to achieve in real world scenarios (need for TrustedOS, chain of trust, …)
  - (too) high complexity of measurement and remote attestation in real world scenarios
  - privacy
    - user has little control over what information is revealed to third parties
  - specification and standardisation (also beyond TCG) is still in progress
    - see also: IETF Network Endpoint Assessment (NEA) working group
  - MAP approach is a bit „hidden“ as being part of the limited area of TNC/NAC
    - MAP could have a much broader importance and relevance towards a cooperative approach in an overall security architecture

Conclusion (3/3)

- The need for solutions like TNC will grow according to
  - the increasing importance of endpoint security for the overall network security and
  - the strongly increasing security threats to endpoints.
- TCG and many others (like Trust@FHH) are working on further developments and enhancements required for a real interoperable, real trusted NAC solution and finally a modern, effective IT security architecture.

Further readings (1/2)

- Home of Trust@FHH: http://trust.inform.fh-hannover.de
- Home of FreeRADIUS: http://freeradius.org/
- Home of Project libtnc: http://sourceforge.net/projects/libtnc
- Homepage of wpa_supplicant: http://hostap.epitest.fi/wpa_supplicant/
- Homepage of XSupplicant: http://open1x.sourceforge.net/
- Home of EMSCB project: http://www.emscb.com/
- Roecher Dror-John, Thumann Michael, NACATTACK. In: Black Hat Europe 2007, http://www.blackhat.com/html/bh-europe-07/bh-eu-07-speakers.html

Further readings (2/2)

- TNC specs: http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications
  - TNC IF-IMC, Specification Version 1.2, February 2007
  - TNC IF-IMV, Specification Version 1.2, February 2007
  - TNC IF-MAP binding for SOAP, Specification Version 1.1, May 2009
  - TNC IF-PEP: Protocol Bindings for RADIUS, Specification Version 1.1, February 2007
  - TCG Infrastructure Working Group, Platform Trust Services Interface Specification (IF-PTS), Specification Version 1.0, November 2006, In: http://www.trustedcomputinggroup.org/developers/infrastructure/specifications
  - TNC IF-TNCCS: Protocol Bindings for SoH, Specification Version 1.0, May 2007
  - TNC IF-T: Protocol Bindings for Tunneled EAP Methods, Specification Version 1.1, May 2007
  - TNC IF-T: Binding to TLS, Specification Version 1.0, May 2009
  - TNC IF-TNCCS, Specification Version 1.2, May 2009
  - TNC Architecture for Interoperability, Specification Version 1.4, May 2009