Trusted Network Connect (TNC)

Josef von Helden
josef.vonhelden@inform.fh-hannover.de

Martin Schmiedel
Daniel Wuttke

First European Summer School on Trusted Infrastructure Technologies
September 2006

Agenda

- Motivation
- IT Security today...
  ... a dead end street?
- Vision of a modern IT security architecture
- Trusted Network Connect
  - overview
  - features, entities, architecture, ...
  - TNC implementation at FHH
  - TNC with TPM
  - (some) challenges and questions
- Conclusion
- References

Motivation

- organisational conditions call for action, e.g. Sarbanes Oxley Act (SOX), Basel II Accord
- new and more sophisticated IT-based attacks...
- ... example...
  - an attacker wants to compromise a server...
    ... which is behind a hard to break firewall ...
  - thus, take the more clever approach:
    - first, compromise the client (much easier)...
      ... and stay hidden on the client...
    - wait for the client to authenticate itself to the server
    - (mis)use the authenticated connection for attacking the server
      ... and still stay hidden ...

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
  - …

... a dead-end street?

- The internal network has to be more opened, due to strong increase of the need for electronic business with partners.
  - decreases the effectiveness of central firewall systems
- Growing need for public zones in LANs including the acceptance and integration of foreign endpoints
  - consultants, students, guests, ...
  - endpoints are often under user‘s control
- New computing paradigms, e.g. Grid computing
  - raising new security issues
- Sophisticated attacks target at client software to (e.g.) compromise servers over the Web (s.a.)
- It‘s hard to track network wide security incidents.

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
    - open specification and standards allow communication between entities from different vendors
  - central, integrated management

Benefits

- “distributed” incl. endpoints
  - strong prevention against malware attacks
- “integrated”
  - comprehensive coverage for network endpoints regardless of access type, network infrastructure, and communications protocol
  - flexible handling of non-compliant endpoints
- “cooperative”
  - detection of complex attacks by bringing together events and alarms from different sites
- “open”
  - multi-vendor compatibility and interoperability
    - leverages existing network infrastructure
- „central, integrated management“
  - enterprise-wide deployment
  - enforcement of a uniform security policy for different levels (user, group, access point, ...)

How to prepare for the future?

- Don‘t focus security on the central firewall system between internal and external networks exclusively, but...
- ... take into account distributed security measures at the edge of your network.
- Integrate endpoint security (integrity / authenticity checking) into security architecture, based on a uniform security policy.
- Prefer open standards against proprietary solutions.

Trusted Network Connect (TNC)
Overview

- an **open, non-proprietary** standard that enables the application and enforcement of security requirements for endpoints connecting to the corporate network
  - enables customer choice of security solutions and infrastructure
  - adopts existing standards whenever possible
  - received thorough and open technical review
  - support for multi-vendor interoperability
- more than 60 participating companies
  - include those with expertise in firewalls and anti-virus products; switches, routers and hubs; systems management; and operating systems

TNC: Features (1)

- Platform Authentication
  - Platform Credential Verification
  - Integrity Check Handshake
- Endpoint Policy Compliance (Authorisation)
  - establishing a level of ‘trust’
  - examples:
    - ensuring the presence, status, and software version of mandated applications
    - completeness of virus-signature databases, intrusion detection and prevention system applications
    - the patch level of the endpoint’s operating system and applications
  - input to the authorisation decision for gaining access to the network

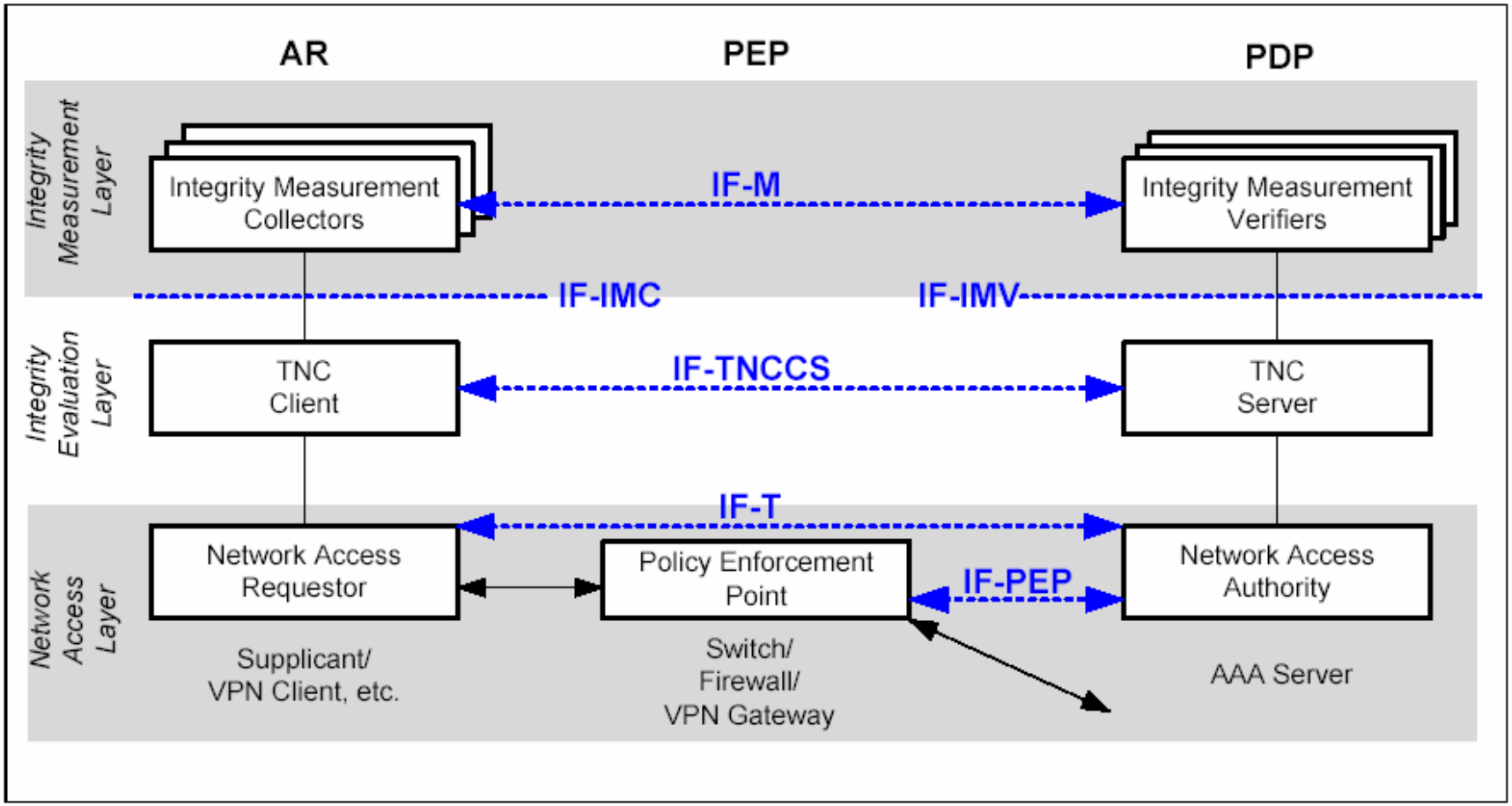
TNC: Features (2)

- Access Policy
  - endpoint machine and/or its user authenticates and discloses their security posture before connecting to the network
  - leveraging a number of existing and emerging standards, products, or techniques
- Assessment, Isolation and Remediation
  - systems not meeting security policy requirements can be isolated or quarantined
  - remediation (if possible), e.g.upgrading software or virus signature database

TNC: Entities

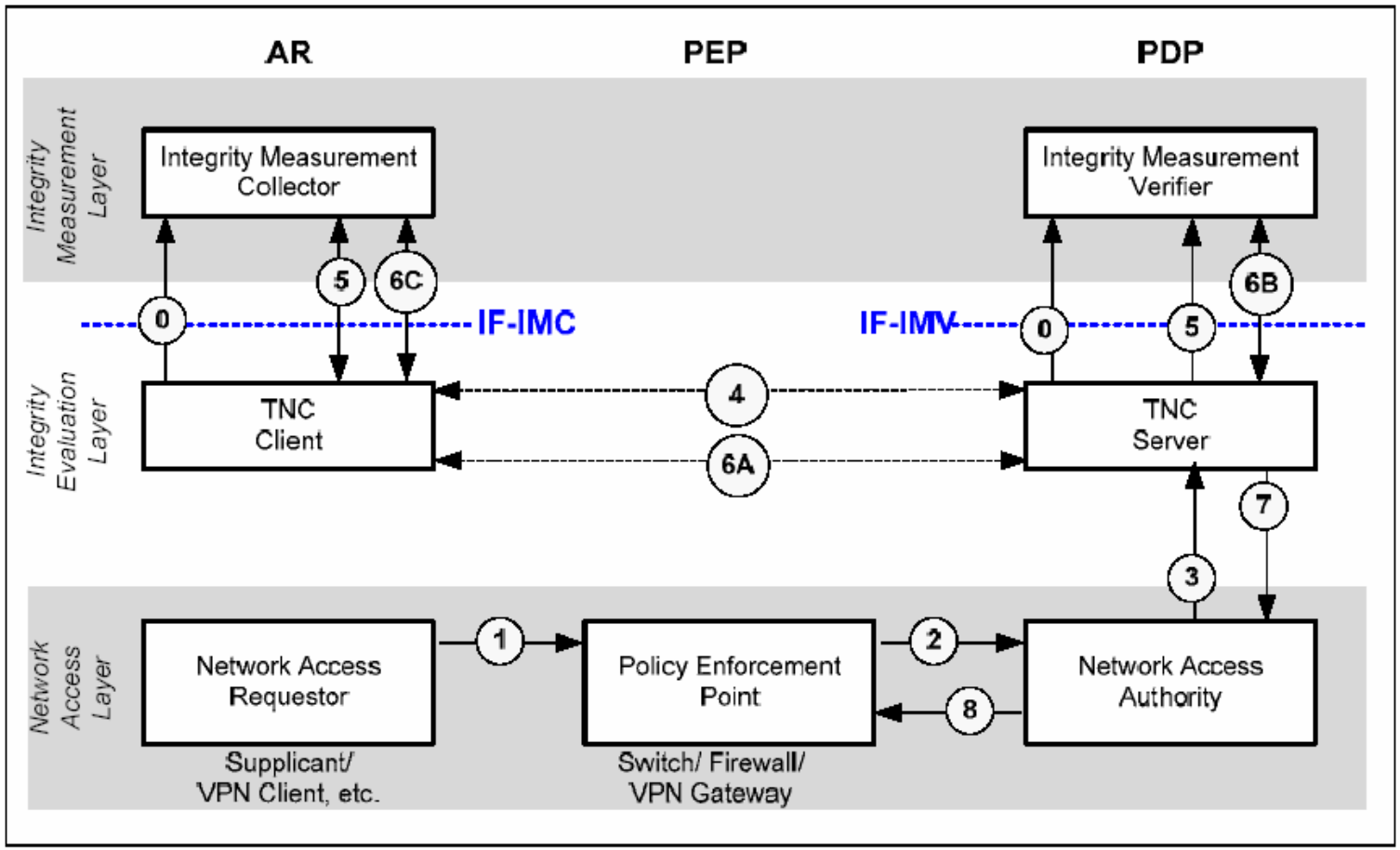
- Access Requestor (AR)
  - requests access to a protected network
    - typically the endpoint, e.g. notebook, desktop, ...
- Policy Decision Point (PDP)
  - performing the decision-making regarding the AR's request, in light of the access policies.
    - typically a network server
- Policy Enforcement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

TNC: Architecture



Quelle: TCG Trusted Network Connect, TNC Architecture for Interoperability, Specification Version 1.1, Revision 2, 1 May 2006

TNC: Basic Message Flow



Quelle: TCG Trusted Network Connect, TNC Architecture for Interoperability, Specification Version 1.1, Revision 2, 1 May 2006

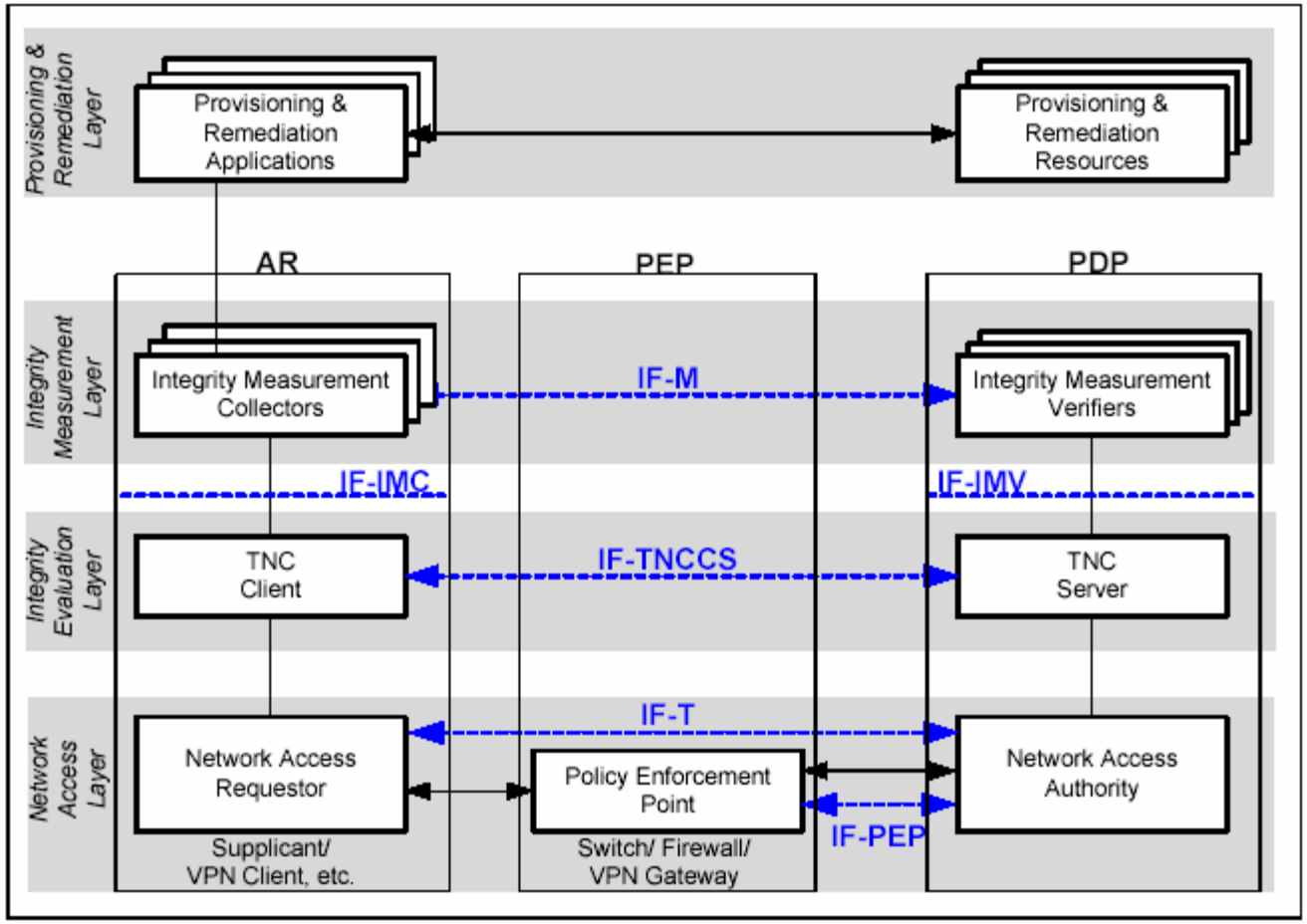
TNC: Assessment, Isolation, Remediation (1)

- Assessment phase
  - IMVs perform the verification of the AR following the policies and if necessary delivers remediation instructions to the IMCs
- Isolation phase
  - if AR
    - is authenticated and recognised to have some privileges but
    - has not passed the integrity-verification by the IMV
  - then PDP
    - may return instructions to the PEP to redirect the AR to an isolation environment where the AR can obtain integrity-related updates.

TNC:
Assessment, Isolation, Remediation (2)

- Remediation phase
  - AR obtaining corrections to its current platform configuration and other policy-specific parameters
  - bringing it inline with the PDP's requirements for network-access

TNC: Provisioning and Remediation Layer



Quelle: TCG Trusted Network Connect, TNC Architecture for Interoperability, Specification Version 1.1, Revision 2, 1 May 2006

TNC:
Provisioning and Remediation Entities

- Provisioning & Remediation Applications (PRA)
  - communicates with the IMC and provides it with specific types of integrity information, e.g. latest AV signature files
  - could be implemented as part of the IMC
- Provisioning & Remediation Resources (PRR)
  - represents the various sources of integrity information needed to update the AR, e.g. enterprise servers, vendor services (e.g. FTP server), CDs/DVDs containing the update parameters

TNC: Supporting Technologies

- Network access technologies
  - 802.1x, VPN, PPP
- Message transport technologies
  - Protected EAP methods
    - EAP-TLS, EAP-TTLS, PEAP, EAP-FAST, ...
  - TLS und HTTPS
- PDP technologies
  - RADIUS
  - Diameter

TNC: Benefits (1)

- Potentially very high security risks arising from compromised endpoints will be beaten down to a minimum, e.g.
  - employees connect their mobile devices at home to the open Internet
  - resulting in malware being inadvertently downloaded onto the device
  - when connected to the corporate network, the device becomes a distributor of the malware to other devices on the enterprise network

TNC: Benefits (2)

- With TNC verifiers
  - may ascertain the security state of a given platform or device and
  - thus, have the ability to decide
    - when it is safe to extend the enterprise boundary to a connecting platform
    - based on the integrity information reported by the platform and by the proof-of-identity supplied by the platform

TNC: Implementation at FHH (1)

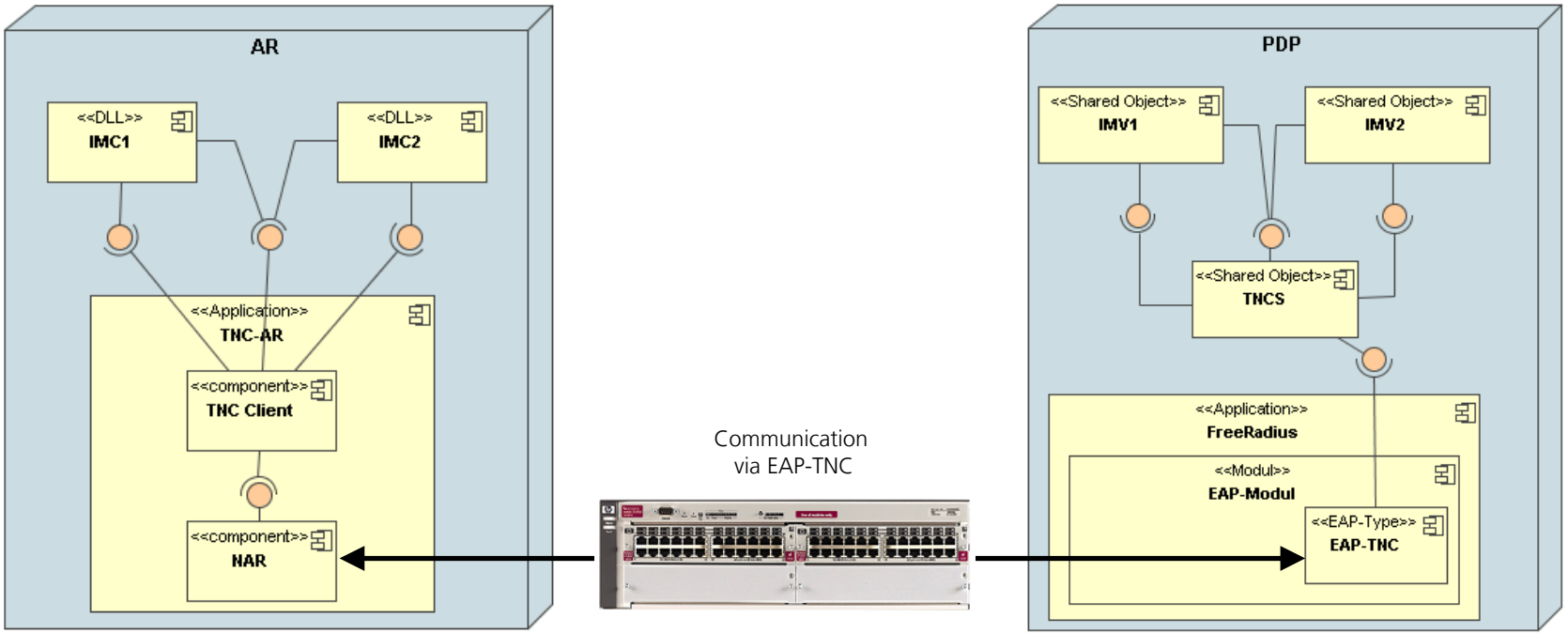
- Two master thesis, both starting Feb. 06
  - Development of client and server software for checking trustworthiness of network endpoints
    - main goal: implementation of TNCC and TNCS
  - Adapting software for automatic integrity checking of endpoints
    - main goal: implementation of IMCs and IMVs

TNC: Implementation at FHH (2)

- Technologies used for Network Access Layer:
  - 802.1x
  - Ethernet-based LAN (no WLAN)
  - RADIUS
- Technologies used during development
  - C++ as programming language
  - Eclipse with CDT-plugin as IDE
  - Xerces for parsing TNCCS-messages and IMC-IMV-messages
  - xWidgets for TNCC User Interface
  - FreeRadius server
- Platforms:
  - Windows XP: TNC Client
    - Cygwin as runtime-environment
  - SuSE Linux 9.3: TNC Server

TNC: Implementation at FHH (3)

- Architecture

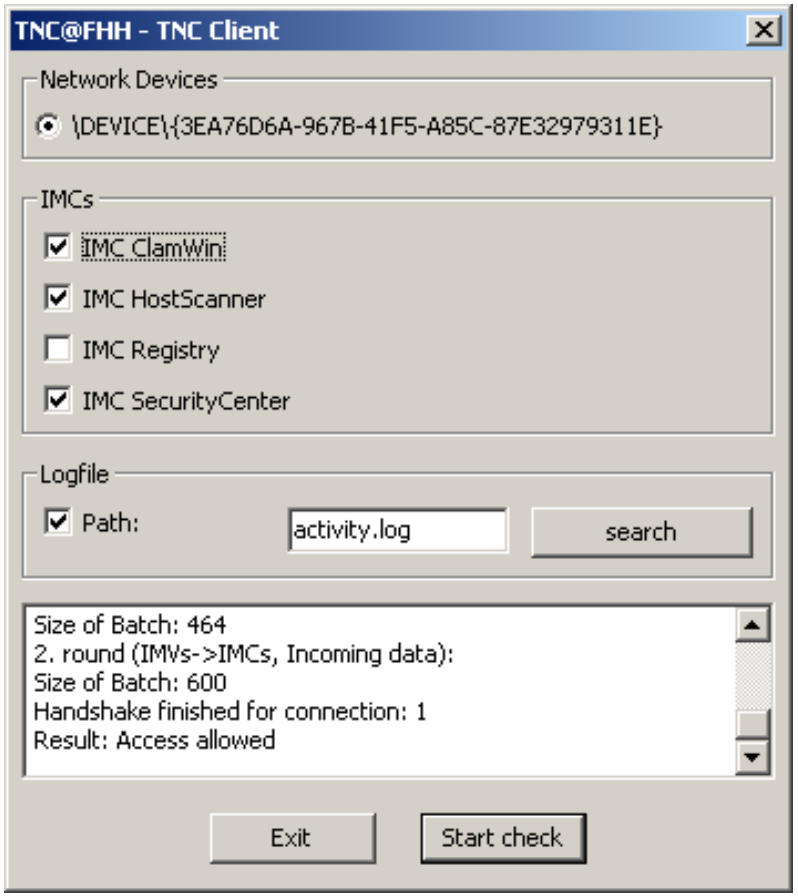


TNC: Implementation at FHH (4)

- Developed IMCs / IMVs:
  - IMCRegistry / IMVRegistry:
    - reads out Windows Registry entries
    - IMV checks whether specific security-relevant entries are present
    - Registry entries to be checked are configurable on server-side
  - IMCHostScanner / IMVHostScanner:
    - checks for open ports on Access Requestor
    - port numbers to be checked are configurable on server-side
  - IMCSecurityCenter / IMVSecurityCenter:
    - checks parameters from Windows Security Center and detects if anti-virus software and firewall are installed and up-to-date
  - IMCClamWin / IMVClamWin:
    - checks if ClamWin (open source anti-virus software) is installed and up-to-date

TNC: Implementation at FHH (5)

- TNCC User interface
  - enables transparency of actions to user
  - gives control to user about handshake



TNC: Implementation at FHH (6)

- Detailed Logging enables reproduction of actions

```
TNC Client started
IMCs loaded
IMCs initialized
Connection to PEP established
Starting initial Handshake for IMC ClamWin

**** Received Message from IMC IMC ClamWin (ID: 2, MessageType: ffff0020):
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<FHH_IMCClamWin version="1.0">
  <ClamWin installed="false"/>
</FHH_IMCClamWin>
********************************************************************************
Round finished for IMC ClamWin
1. round (IMCs->IMVs, Outgoing data):

Size of Batch: 1520
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<TNCCS-Batch BatchId="0" Recipient="TNCS„ …>
  <IMC-IMV-Message>
    <Type>FFFF0020</Type>
    <Base64>PD94bWwgdmVyc2lvbj0iMS4wI…</Base64>
 </IMC-IMV-Message>…
```

TNC: Implementation at FHH (7)

- Experiences:
  - good specification documents from TCG
  - difficult task: implementing Network Access with Windows
  - usual problems of C++ development ☺
- Limitations:
  - no encrypted EAP-TNC messages
  - no Remediation Phase (Start TNC Client once again! ☺)
  - no TPM support
  - only simple policy specification on TNC Server

TNC with TPM: Features (1)

- Protected Capabilities
  - a set of commands with exclusive permission to access „Shielded Locations“
  - examples for TPM usage in TNC
    - protect and report aggregations of integrity measurements that are stored inside the TPM’s *Platform Configuration Registers* (PCR)
    - store cryptographic keys used to authenticate reported measurements

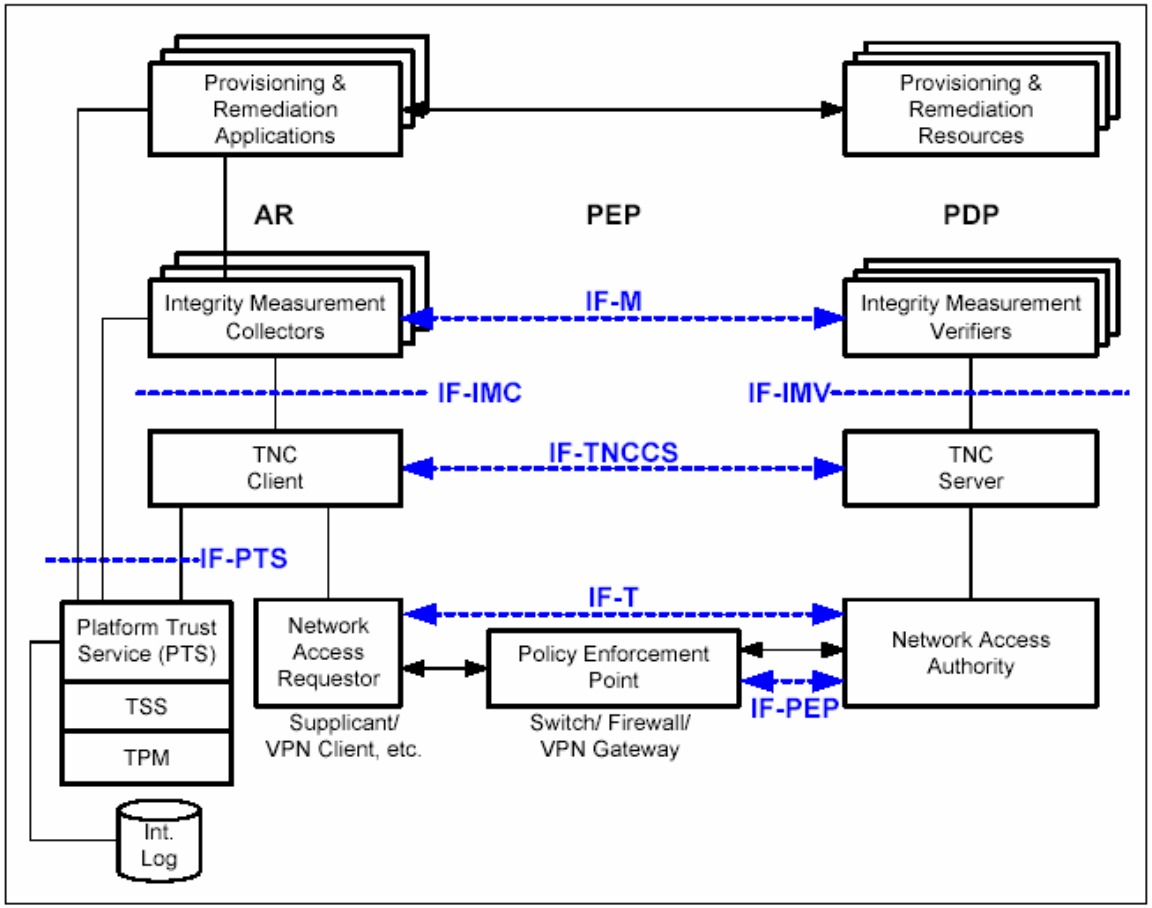
TNC with TPM: Features (2)

- Integrity Measurement and Storage
  - obtaining metrics of platform characteristics that affect the integrity (trustworthiness) of a platform
  - storing those metrics
  - putting digests of those metrics in PCRs.
- Integrity Reporting
  - attesting to the contents of integrity storage, i.e. stored measurement log
  - signed using the private key held (e.g. AIK-certificate) located in shielded locations in the TPM

TNC with TPM: Features (3)

- Attestation
  - vouching for the accuracy of information, such that a relying party can use the attestation to decide whether it trusts the remote platform
- Evaluation and Decision Making
  - allows delegation of evaluation to a 3rd party
  - outcome not limited to binary results
- Enforcement and Response
  - evaluating platform may in fact be a PEP or may return responses to another platform

TNC with TPM: Architecture



Quelle: TCG Trusted Network Connect, TNC Architecture for Interoperability, Specification Version 1.1, Revision 2, 1 May 2006

TNC with TPM: Entities

- in general the same entities as without TPM
- one additional entity: Privacy Certification Authority
  - issues AIK certificates to trusted platforms
  - trusted by both parties
  - needed if AR and PEP/PDP have different „owners“

TNC with TPM: Components

- Platform Trust Services (PTS)
  - exposes trusted platform capabilities to TNC components, including
    - protected key storage, asymmetric cryptography, random numbers, platform identity, platform configuration reporting and integrity state tracking
- TCG Software Stack (TSS)
  - enables applications to use higher level interfaces for communication with the TPM support functions, including
    - unlimited key storage (off-chip protected), key caching, higher-level interface abstraction

TNC with TPM: Benefits

- TPM provides a strong hardware-protected root-of-trust.
- This is needed to ensure malware and improperly configured software cannot report an erroneous status.
- The use of the TPM prevents a system from lying about what the platform is running so others can determine if the endpoint has the desirable integrity.

TNC: (some) challenges and questions

- How good does TNC work in real (complex) network environments?
- How can TNC environments be effectively managed and security policies be effectively enforced?
- What are benefits, side effects and impacts of TNC, regarding different operating scenarios?
- What scenarios are suited for operating TNC with / without TPM?
- What are security / privacy issues of TNC with / without TPM?

- Is TNC able to become a de facto standard?
- Does TNC really make the world more secure?
- ...

Conclusions

- A distributed, integrated, cooperative and open security architecture can leverage security significantly.
- TNC seems to be more than a well suited starting basis, due to
  - its use of the TCG Platform-Authentication approach as a critical part of achieving true trusted network connections
  - its openness and broad vendor support
- There are several challenges and questions...
  - ... some further research and development efforts seem to be required

References

- www.trustedcomputinggroup.org
  - home of the Trusted Computing Group
- www.trustedcomputinggroup.org/groups/network/
  - home of the Trusted Network Connect Sub Group (TNC-SG)
- www.trustedcomputinggroup.org/specs/TNC/
  - TNC-SG specs, e.g.
    - „TCG TNC Architecture“ Version 1.1, May 2006
    - „TCG TNC IF-IMC Specification“ Version 1.1, May 2006
    - „TCG TNC IF-IMV Specification“ Version 1.1, May 2006
    - „TCG TNC IF-TNCCS Specification“ Version 1.0, May 2006