SPONSORED BY THE

Federal Ministry of Education and Research

tNAC - Trusted Network Access Control

Ingo Bente[1] Josef von Helden[1] Joerg Vieweg[1] Marian Jungbauer[2] Norbert Pohlmann[2]

[1]Trust@FHH Research Group, University of Applied Sciences and Arts, Hanover, Germany

[2]Institute for Internet Security, University of Applied Sciences, Gelsenkirchen, Germany

tNAC trusted network access control

Introduction

- Network Access Control (NAC) approaches promise to secure the dynamic access of mobile endpoints to networks.
- In addition to an user authentication, the integrity status of the respective endpoint is measured and verified.
- NAC agents on the respective endpoints are used to obtain and communicate the integrity measurements.
- A common threat for agent based NAC approaches is malware that forges the integrity measurements, and thus by-pass any protecting measures of the NAC solution.
- This threat is known as *Lying Endpoint Problem (LEP)*.
- tNAC aims to mitigate the LEP by leveraging Trusted Computing functions in conjunction with Trusted Network Connect.

Technological Basis

TURAYA

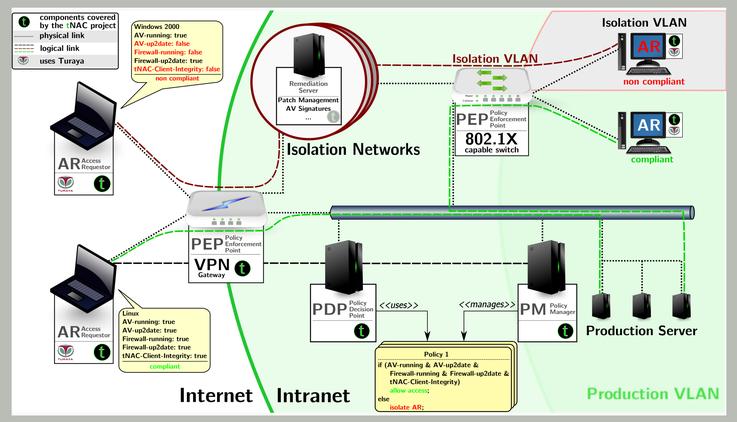
TNC@FHH

- The results of two research projects constitute the technological basis.
  - Turaya, the secure operating platform, developed within the EMSCB project.
  - TNC@FHH, the open source TNC implementation, developed at the University of Applied Sciences and Arts, Hanover.
- Turaya offers general Trusted Computing functions, including the measurement and isolation of compartments.
- TNC@FHH provides NAC functions compliant to the TNC standard, including assessment, isolation and remediation of endpoints.
- tNAC aims to integrate Turaya and TNC@FHH in such a way that Lying Endpoints are securely detected during a TNC handshake.

Features

- Compliance to TCG technologies, including TNC and TPM
- Secure detection of lying endpoints
- TPM secured assessment
- (Semi-)Automatic isolation and remediation
- User-friendly policy management

Architecture Overview



- Access Requestors: endpoints connecting to a network.
- Policy Manager: manages network operator's policies.
- Policy Decision Point: handles the TNC handshake, derives access decision based upon policies.
- Policy Enforcement Points: enforce PDP's access decision.
- Remediation Server: controls remediation of endpoints and provides appropriate resources.

TPM Support

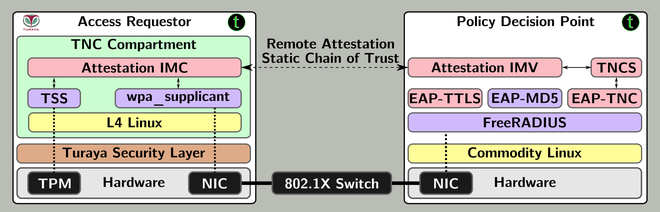


Figure: TPM support of tNAC in a 802.1X environment.

- Turaya handles integrity measurements on access requestors and extends the TPM's PCRs
- PCR values establish of a Static Chain of Trust from CRTM to single compartments
- Special attestation IMC/V pair uses these measurements within TNC handshake
- The IMC/V pair carries out a challenge/response protocol that includes a TPM_Quote of the TPM's PCRs.
- Thus, Lying Endpoints can be detected.

VPN Support

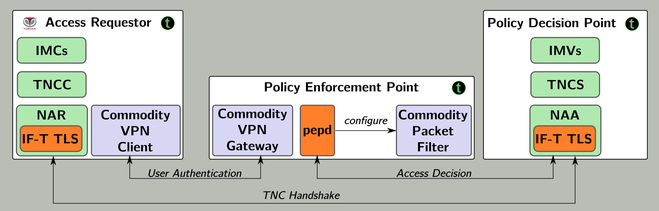


Figure: VPN support of tNAC by leveraging IF-T TLS.

- VPN support: based upon TNC's IF-T TLS specification
- TNC Handshake: tunneled over a VPN connection
- First: user authentication via a commodity VPN solution
- Second: TNC Handshake via IF-T TLS over the VPN connection
- PEP enforces access decision by configuring a packet filter (e.g. iptables)

Remediaton and Policy Management

- Remediation is supported by tNAC IMC/V pairs.
- Remediation server in isolated network environment provides necessary resources.
- Dedicated Policy Manager handles policies for TNCS and IMVs.
- Latest policies are pushed to PDP.
- IMV policies specify requirements for endpoints in order to get access.
- TNCS policies specify how evaluation results of IMVs are combined to derive an access decision.

Current Status and Future Work

- First prototype implementation finished in March 2010.
- Support for TPM based attestation, basic policy management and remediation in 802.1X networks.
- In addition, IMC/V pairs to evaluate status of Anti Virus software and opened ports are available.
- Future work
  - Implementation of VPN approach.
  - Extending policy management and remediation functions.
  - Realizing inter-compartment communication between TNC components on the access requestor.
- Final version expected for June 2011.