Access Requestor (AR)

Policy Enforcement Point (PEP)

Policy Decision Point (PDP)
Access Requestor (AR)

Policy Enforcement Point (PEP)

Policy Decision Point (PDP)
Access Requestor (AR)

Policy Enforcement Point (PEP)

Policy Decision Point (PDP)

Sensors
But How?
Open Standards for Gathering Additional Factors

- Device Health
- Location
- Behavior

Works at Application Layer or at Network Layer

- Enables Many Implementation Options

Strong Security

- Confidentiality – Sensitive Information
- Integrity – Accurate Information is Essential
Briefing on TNC
Open Architecture for Network Security
- Completely vendor-neutral
- Strong security through trusted computing

Open Standards for Network Security
- Full set of specifications available to all
- Products shipping since 2005

Developed by Trusted Computing Group (TCG)
- Industry standards group
- More than 100 member organizations

Also Approved by IETF
Network Access Control (NAC)

Coordinate Security
Access Requestor (AR)

Policy Enforcement Point (PEP)

VPN

Policy Decision Point (PDP)
Access Requestor (AR)

Policy Enforcement Point (PEP)

Policy Decision Point (PDP)

Metadata Access Point (MAP)

Sensors, Flow Controllers
Health Check

Behavior Check

User-Specific Policies

TPM-Based Integrity Check
Non-compliant System
Windows XP
✓ SP3
✓ OSHotFix 2499
✓ OSHotFix 9288
✓ AV - McAfee Virus Scan 8.0
✓ Firewall

Compliant System
Windows XP
✓ SP3
✓ OSHotFix 2499
✓ OSHotFix 9288
✓ AV - Symantec AV 10.1
✓ Firewall

Access Requestor

Policy Enforcement Point

Policy Decision Point

Remediation Network

Production Network

NAC Policy
Windows XP
• SP3
• OSHotFix 2499
• OSHotFix 9288
• AV (one of)
  • Symantec AV 10.1
  • McAfee Virus Scan 8.0
  • Firewall
NAC Policy
• No P2P file sharing
• No spamming
• No attacking others
Access Requestor

- **Guest User**
- **Mary – R&D**
- **Joe – Finance**
  - Windows XP
  - OS Hotfix 9345
  - OS Hotfix 8834
  - AV - Symantec AV 10.1
  - Firewall

---

Policy Enforcement Point

- Guest Network
- Internet Only
- R&D Network
- Finance Network

Policy Decision Point

- NAC Policy
  - Users and Roles
  - Per-Role Rules

Metadata Access Point

Sensors and Flow Controllers

---

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners. Slide #16
**Compliant System**

- BIOS
- OS
- Drivers
- Anti-Virus SW

**TPM — Trusted Platform Module**
- HW module built into most of today’s PCs
- Enables a HW Root of Trust
- Measures critical components during trusted boot
- PTS interface allows PDP to verify configuration and remediate as necessary

**NAC Policy**
- TPM enabled
  - BIOS
  - OS
  - Drivers
  - Anti-Virus SW
Access Requestor

**Policy Enforcement Point**

**Policy Decision Point**

**Metadata Access Point**

**Sensors and Flow Controllers**

---

**NAC Policy**
- Place Printers on Printer Network
- Monitor Behavior

---

Remediation Network
Access Requestor (AR)

Policy Enforcement Point (PEP)

Policy Decision Point (PDP)

Metadata Access Point (MAP)

Sensors, Flow Controllers
Solves the critical “lying endpoint problem”

TPM Measures Software in Boot Sequence

- Hash software into PCR before running it
- PCR value cannot be reset except via hard reboot

During TNC Handshake...

- PDP engages in crypto handshake with TPM
- TPM securely sends PCR value to PDP
- PDP compares to good configurations
- If not listed, endpoint is quarantined and remediated
Conveys TNC results between security domains

- Consortia, coalitions, partnerships, outsourcing, and alliances
- Large organizations

Supports

- Web SSO with health info
- Roaming with health check

How?

- SAML profiles for TNC

Applications

- Network roaming
- Coalitions, consortia
- Large organizations
IF-TNCCS-SOH Standard

- Developed by Microsoft as Statement of Health (SoH) protocol
- DONATED to TCG by Microsoft
- ADOPTED by TCG and published as a new TNC standard, IF-TNCCS-SOH

Availability

- Also built into products from other TNC vendors

Implications

- NAP servers can health check TNC clients without extra software
- NAP clients can be health checked by TNC servers without extra software
- As long as all parties implement the open IF-TNCCS-SOH standard
IETF NEA WG

- Goal: Universal Agreement on NAC Client-Server Protocols
  - Co-Chaired by Cisco employee and TNC-WG Chair

Published several TNC protocols as IETF RFCs

- PA-TNC (RFC 5792) and PB-TNC (RFC 5793)
- Equivalent to TCG’s IF-M 1.0 and IF-TNCCS 2.0
- Co-Editors from Cisco, Intel, Juniper, Microsoft, Symantec

Now working on getting IETF approval for IF-T
Lots of open source support for TNC

- University of Applied Arts and Sciences in Hannover, Germany (FHH)
  [http://trust.inform.fh-hannover.de](http://trust.inform.fh-hannover.de)
- libtnc
  [http://sourceforge.net/projects/libtnc](http://sourceforge.net/projects/libtnc)
- OpenSEA 802.1X supplicant
  [http://www.openseaalliance.org](http://www.openseaalliance.org)
- FreeRADIUS
  [http://www.freeradius.org](http://www.freeradius.org)
- omapd IF-MAP Server
  [http://code.google.com/p/omapd](http://code.google.com/p/omapd)
- strongSwan IPsec
  [http://www.strongswan.org](http://www.strongswan.org)
- Open Source TNC SDK (IF-IMV and IF-IMC)
  [http://sourceforge.net/projects/tncsdk](http://sourceforge.net/projects/tncsdk)

TCG support for these efforts

- Liaison Memberships
- Open source licensing of TNC header files
Certifies Products that Properly Implement TNC Standards

Certification Process

- Compliance testing using automated test suite from TCG
- Interoperability testing at Plugfest
- Add to list of certified products on TCG web site

Customer Benefits

- Confidence that products interoperate
- Easy to cite in procurement documents
Options for Application Enforcement with TNC
Non-compliant System
Windows XP
- SP3
- **xOSHHotFix 2499**
- **xOSHHotFix 9288**
- AV - McAfee Virus Scan 8.0
- Firewall

Compliant System
Windows XP
- SP3
- OSHHotFix 2499
- OSHHotFix 9288
- AV - Symantec AV 10.1
- Firewall

**Access Requestor**

**Policy Enforcement Point**

**Policy Decision Point**

Policy
Windows XP
- SP3
- OSHHotFix 2499
- OSHHotFix 9288
- AV (one of)
  - Symantec AV 10.1
  - McAfee Virus Scan 8.0
  - Firewall
Access Requestor (AR)

Policy Enforcement Point (PEP)

Metadata Access Point (MAP)

Sensors, Flow Controllers
TNC Web Site

Technical

http://www.trustedcomputinggroup.org/developers/trusted_network_connect

Business

http://www.trustedcomputinggroup.org/solutions/network_security

TNC–WG Co–Chairs

Steve Hanna
Distinguished Engineer, Juniper Networks
shanna@juniper.net

Paul Sangster
Chief Security Standards Officer, Symantec
Paul_Sangster@symantec.com