Putting Trust Into The Network
Securing Your Network Through Trusted Access Control

Steve Hanna, Juniper Networks
Co-Chair, Trusted Network Connect Sub Group of Trusted Computing Group

ACSAC
December 2006
Talk Outline

• Problem Statement
• Various Solutions
• Trusted Access Control
• Q & A
Problem: Reduce Endpoint Attacks

• Motivated Attackers
  – Extortion, Identity Theft, Bank Fraud, Corporate Espionage

• Increasingly Sophisticated and Serious Attacks
  – Viruses, Worms, Spyware, Rootkits, Back Doors, Botnets
  – Zero-Day Exploits, Targeted Attacks, Rapid Infection Speed

• Exponential Growth in Malware
  – >40,000,000 Infected Machines, >35,000 Malware Varieties

• Dissolving Network Boundaries
  – Mobile workforce, partners, contractors, outsourcing

• Regulatory Requirements
Various Solutions

• More Secure Endpoints
  – AV, Personal Firewall, Patch Management
  – Better Coding Practices, Anti-Spyware, HIPS

• Stronger Network Protection
  – Firewalls, IDS, IPS, Vulnerability Scanners
  – Network Access Control (NAC)

• But Endpoints Still Get Compromised
  – And then what?
Trusted Access Control =

Trusted Platform Module +

Network Access Control
Trusted Platform Module

• Hardware Security Component
  – Key storage
  – Signing and encryption
  – Secure and Trusted Boot
  – Remote attestation

• Open Standards for Features and APIs
  – Developed by Trusted Computing Group

• Included on all new commercial laptops, increasing number of desktops and servers
Network Access Control

• Check Endpoint Health against Policy
  – At or After Network Connection
  – If Unhealthy, Quarantine and Remediate

• But what about lying endpoints?
  – Need Trusted Boot and Remote Attestation
Trusted Network Connect (TNC)

- Open Architecture for Network Access Control (NAC)
- Suite of Standards
- Developed by Trusted Computing Group
- Supports Trusted Access Control
TNC Architecture
TNC Standards
Network Access Control Use Case

Access Requestor
- Non-compliant System
  - Windows XP
  - SP2
  - xOSHHotFix 2499
  - xOSHHotFix 9288
  - AV - McAfee Virus Scan 8.0
  - Firewall

Compliant System
- Windows XP
- SP2
- OSHHotFix 2499
- OSHHotFix 9288
- AV - Symantec AV 10.1
- Firewall

Policy Enforcement Point

Policy Decision Point
- Client Rules
  - Windows XP
  - SP2
  - OSHHotFix 2499
  - OSHHotFix 9288
  - AV (one of)
    - Symantec AV 10.1
    - McAfee Virus Scan 8.0
    - Firewall
Trusted Access Control Use Case

Access Requestor
- TPM measures critical components during trusted boot
- TPM attests to measurements during Trusted Network Connect handshake
- Policy Decision Point compares measurements against good configurations

Compliant System
TPM verified
- BIOS
- OS
- Drivers
- Anti-Virus SW

Policy Enforcement Point

Policy Decision Point

Client Rules
TPM enabled
- BIOS
- OS
- Drivers
- Anti-Virus SW

Corp LAN
Trusted Network Connect (TNC) Advantages

• Open standards
  – Non-proprietary – Supports multi-vendor compatibility
  – Enables customer choice
  – Allows thorough and open technical review

• Leverages existing network infrastructure
  – Excellent Return-on-Investment (ROI)

• Strong security
  – Trusted Platform Module (TPM)
  – Solves lying endpoint problem

• Products supporting TNC standards shipping today
  – Including open source implementations
TNC Vendor Support

Access Requestor
- Endpoint
- Supplicant/VPN Client, etc.

Policy Enforcement Point
- Network Device
- FW, Switch, Router, Gateway

Policy Decision Point
- AAA Server, Radius, Diameter, IIS, etc.

Copyright © 2006 Trusted Computing Group – Other names and brands are properties of their respective owners.
Q & A