Agenda

- Challenges of Trusted Computing
- Capabilities of a Trusted Computing Platform
- Establishing Endpoint Integrity
- Connecting a Trusted Platform to a Network
- Summary

RSA Conference 2005

TRUSTED COMPUTING GROUP

2

Challenges of Trusted Computing

- Increase Assurances that the Computing Environment is Safe
  - Virus and worm contamination
  - Root kits
  - Spyware and adware threats to privacy
- Identifying the Platform as an Endpoint is Ambiguous
  - Network security protocols authenticate using keys / passwords but trust that these tokens are protected by the endpoint platform
  - Many controllers, busses and peripherals make up a typical platform opportunities for compromise are large
- Protection of Data, Privacy and Control
  - Infosec policy often must accompany data as it moves through different computing environments

RSA Conference 2005

TRUSTED COMPUTING GROUP

3

Technical Challenges

- Code and logic may not behave according to the user's wishes
  - From whence did it originate?
  - How to determine its behavior without doing damage?
- Computers are distributed fractal environments
  - Where does one "platform" end and another begin?
    - Micro-architecture components are connected via traces & leads
    - Chipsets and peripherals are connected via busses and interconnects
    - Platforms are connected via networks and inter-networks
- Private information once lost can never be returned
  - When is it safe to cede control?

RSA Conference 2005

TRUSTED COMPUTING GROUP

4

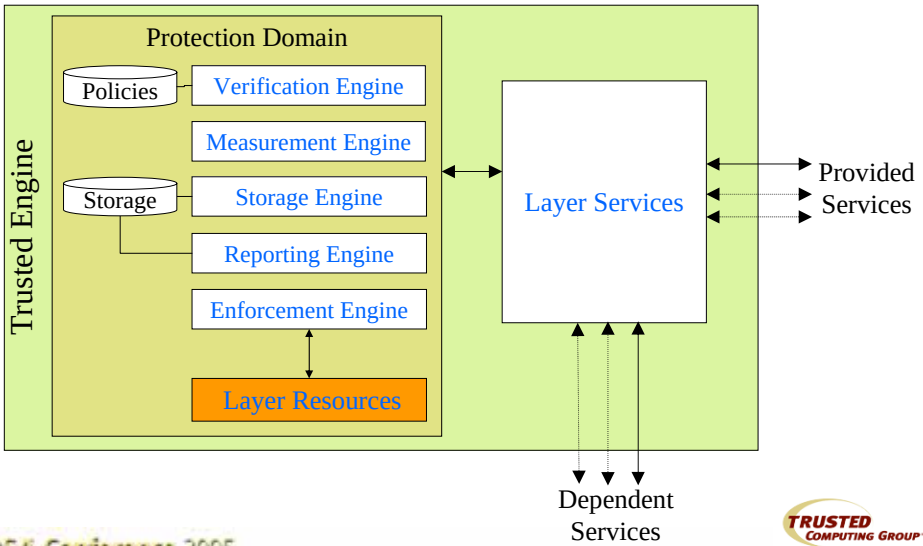
Solutions to Technical Challenges

- Some Suggestions
  - Collect measurements indicating the state / origin of code / logic
  - Save measurements in protected storage
  - Instrument the platform with the ability to report its identity / state
  - Incorporate into access control decisions the verification of measurement
  - Provide access control to resources
  - Harden computing environments
    - Through hardware and firmware isolation
      - Virtual Machines
      - Dedicated cores / partitioned hardware
    - Tamper-resistant packaging
      - TPM / smartcards

RSA Conference 2005

5

Capabilities of a Trusted Computing Platform



RSA Conference 2005

6

Trust Engine Versatility

- Engines may be Distributed or Combined as Needed
  - Example: Trusted Boot
    - Trusted boot service implements Measurement and Storage engines as part of the boot sequence
    - The system may execute infected or unauthorized code but a Verification engine on a network gateway could detect this
  - Example: Secure Boot
    - A secure boot service implements Measurement and Reporting engines that deliver results in advance to a Verification engine
    - The Verification engine evaluates measurements according to a policy to determine proper boot sequence
    - If the sequence is in error, an Enforcement engine is employed to terminate the boot process

RSA Conference 2005

TRUSTED COMPUTING GROUP™

7

Establishing Endpoint Integrity

- Collection
  - An enumeration and scanning process is needed to capture platform state
    - Controllers and processors are enumerated to determine if all present should be
    - Executing code (or may be executed) is scanned to determine its present state
- Identity
  - Each component (device, platform, software package) can be identified by its Manufacturer, Model and Version (MMV)
    - If the code or logic has a vulnerability it may be “identified” using the MMV
  - Reporting Engines have cryptographic keys that may be used to authenticate the reporting engine that by extension identifies the platform.
- Origin
  - Trusted engines rely on the reputation of the manufacturer as the basis for that trust
    - Credentials issued by manufacturers containing reference measurements and quality assertions establishes the origin

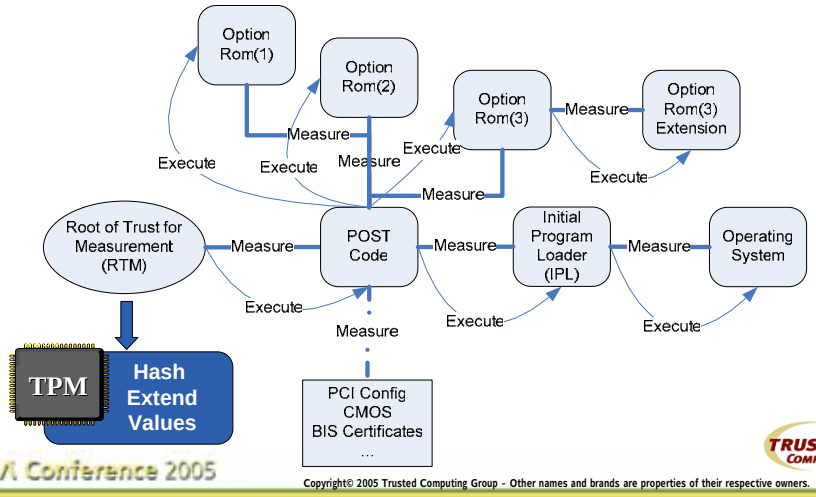
RSA Conference 2005

TRUSTED COMPUTING GROUP™

8

Pre-Boot Integrity Collection

- Example: PC Platform Pre-boot Collection Sequence

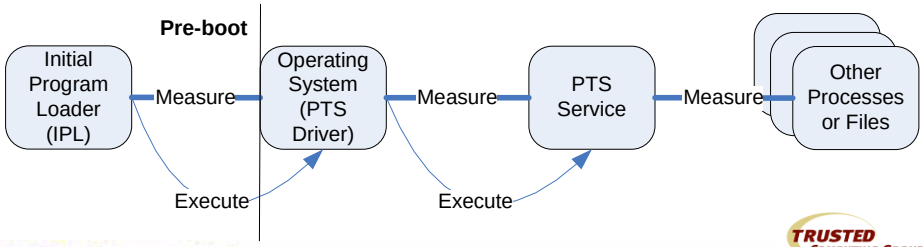


Collecting Measurements Post Boot

- A Platform Trust Service can be used to Measure Applications
  - Files
    - Read files from disk; compute a measurement
  - Processes
    - Ring 3 - DLL injection to read another processes memory
    - Ring 0 – Access pages in memory / DMA accesses
- All Measurements must have a Reference Measurement
  - They may be obtained from clean room collection directly from the platform
  - They may be obtained from manufacturers
    - Signature databases
    - Driver signing
    - TCG Credentials

A Platform Trust Service

- Integrity of the PTS is Established
  - Pre-boot by measuring PTS drivers included in OS image
  - Post-boot by measuring PTS process memory pages
- PTS may Measure other Processes and Files
  - Determined by policy or triggered by request



RSA Conference 2005

TRUSTED COMPUTING GROUP

11

Countering Threats

- A PTS Process may be the Target of an Attacker
  - Virus or worm modifies PTS while it executes
  - Driver attacks
  - Root kits
- PTS Survival Strategies
  - PTS driver periodically (randomly) re-measures PTS pages
    - Attacker must anticipate and “dodge” periodic scans
  - PTS is restarted from known good image from disk
  - PTS code is measured by another processor
  - Root kit defense remains a challenge
- Periodic Assessment of Platform State
  - Such as at network connection time

RSA Conference 2005

TRUSTED COMPUTING GROUP

12

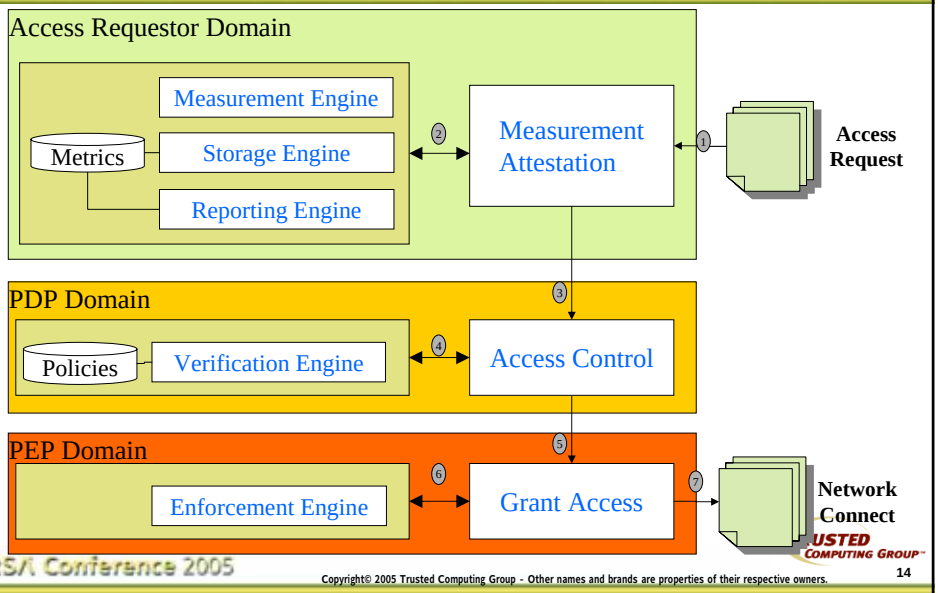
Steps of a Trusted Network Connection

- Find out the condition of the platform
- Communicate platform state when connecting
- Decide what level of access is acceptable
- Restrict the environment in accordance with access rights
- Remediation may be required to reconcile denied access

RSA Conference 2005

13

Trust Engine Decomposition for TNC

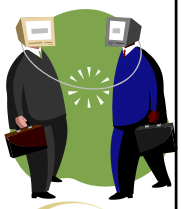


RSA Conference 2005

14

Connecting a Trusted Platform to a Network

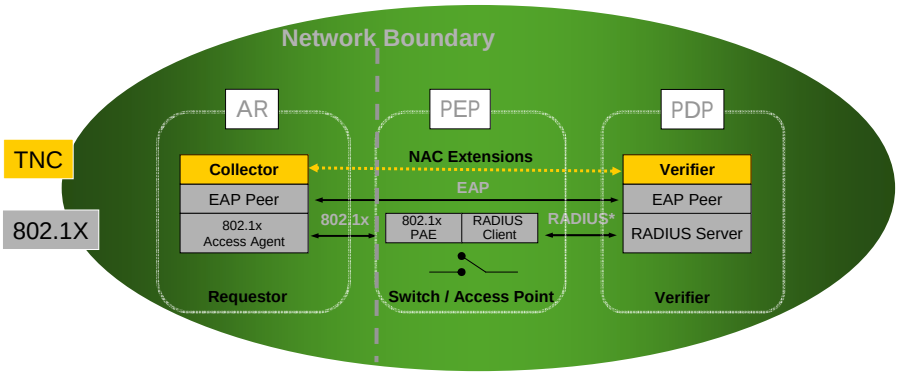
- Platform Measurements Establish Endpoint Integrity
- Integrity Values can be Reported to a Policy Decision Point (PDP) at Network Connect Time
  - 802.1X EAP methods
  - Extensions to TLS / SSL
- PDP Evaluates the Report and Determines the Response
  - Allow
  - Deny
  - Quarantine
  - Remediate



RSA Conference 2005

15

TNC with 802.1X at Link Layer

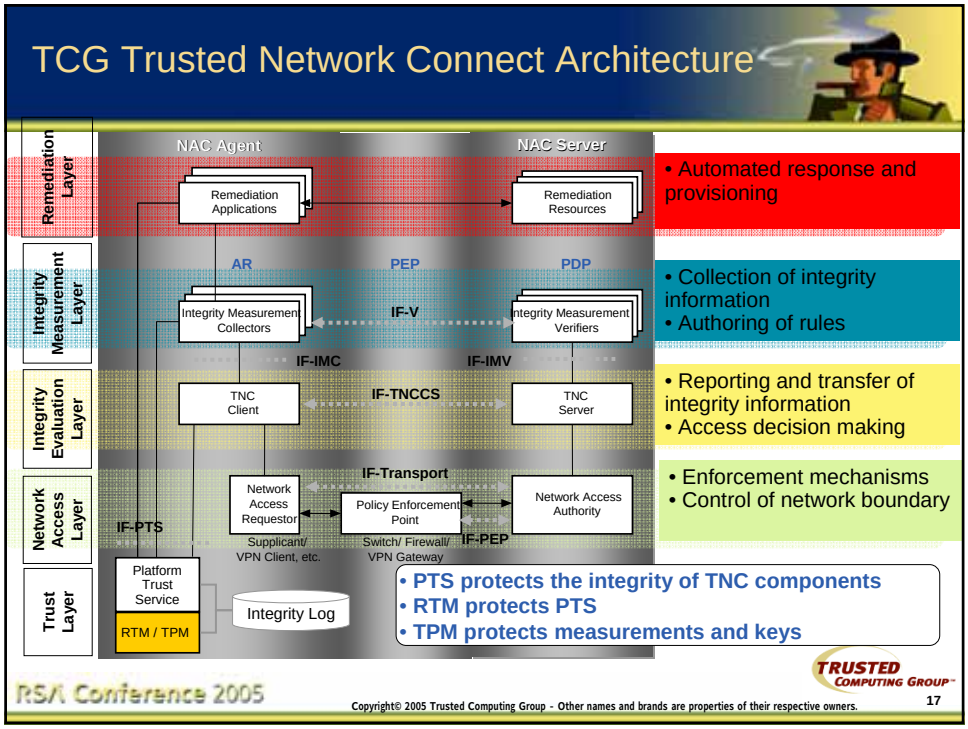


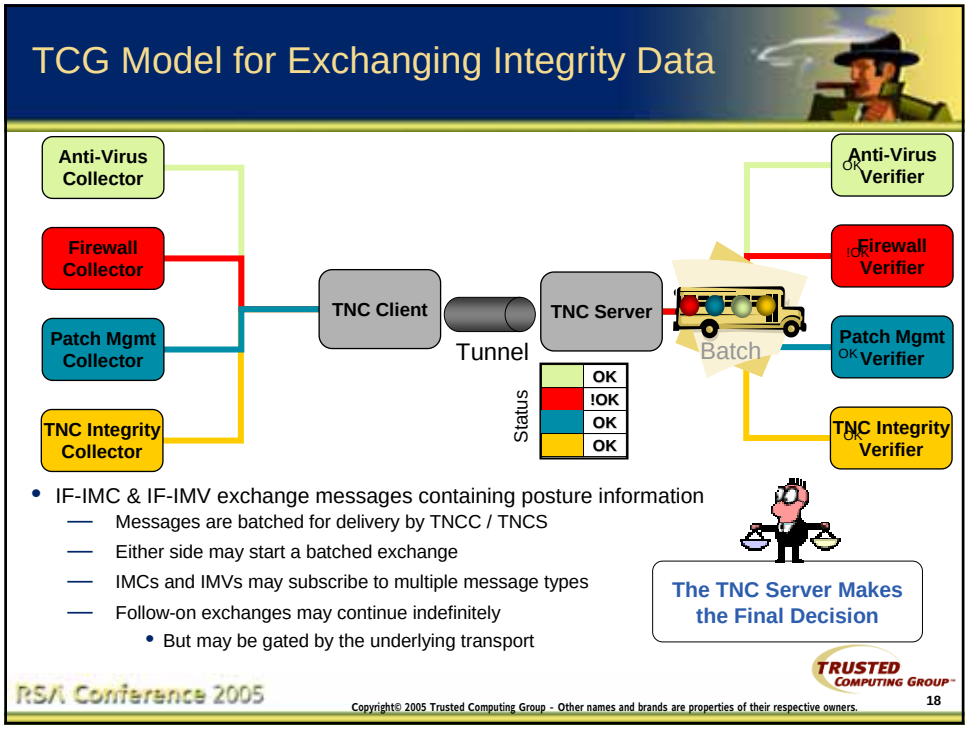
Verifier & **Collector** exchange posture information over EAP tunnel using EAP inner methods, AVPs or TLVs

AR – Access Requester
AVP – Attribute Value Pair
EAP – Extensible Authentication Protocol
PAE – Port Access Entity
PDP – Policy Decision Point
PEP – Policy Enforcement Point
NAC – Network Access Control
TLV – Tag Length Value

RSA Conference 2005

16


TCG Trusted Network Connect Architecture
Remediation Layer
Integrity Measurement Layer
Integrity Evaluation Layer
Network Access Layer
Trust Layer
NAC Agent
NAC Server
Remediation Applications
Remediation Resources
AR
PEP
PDP
Integrity Measurement Collectors
IF-V
Integrity Measurement Verifiers
IF-IMC
IF-IMV
TNC Client
IF-TNCCS
TNC Server
IF-Transport
Network Access Requestor
Policy Enforcement Point
Network Access Authority
IF-PTS
Supplicant/ VPN Client, etc.
Switch/ Firewall/ VPN Gateway
IF-PEP
Platform Trust Service
RTM / TPM
Integrity Log
• Automated response and provisioning
• Collection of integrity information
• Authoring of rules
• Reporting and transfer of integrity information
• Access decision making
• Enforcement mechanisms
• Control of network boundary
• PTS protects the integrity of TNC components
• RTM protects PTS
• TPM protects measurements and keys
RSA Conference 2005
Copyright© 2005 Trusted Computing Group - Other names and brands are properties of their respective owners.
17


TCG Model for Exchanging Integrity Data
Anti-Virus Collector
Firewall Collector
Patch Mgmt Collector
TNC Integrity Collector
TNC Client
Tunnel
TNC Server
Batch
Status
OK
!OK
OK
OK
Anti-Virus Verifier
Firewall Verifier
Patch Mgmt Verifier
TNC Integrity Verifier
• IF-IMC & IF-IMV exchange messages containing posture information
— Messages are batched for delivery by TNCC / TNCS
— Either side may start a batched exchange
— IMCs and IMVs may subscribe to multiple message types
— Follow-on exchanges may continue indefinitely
• But may be gated by the underlying transport
The TNC Server Makes the Final Decision
RSA Conference 2005
Copyright© 2005 Trusted Computing Group - Other names and brands are properties of their respective owners.
18

Integrity Report

- Integrity Report is a History
  - Operational state change; by measuring code before it executes
  - Configuration settings; at the time of measurement
  - Sequence of operations; by virtue of TPM hash operation
  - Digitally signed by TPM Attestation Identity Key (AIK)

- Integrity Report is also a Description of the Endpoint
  - Measurement engines enumerate installed software and devices
    - Vendor, Model, Version, Patch Level
      - Cryptographic hash of code
- Integrity Reports may Indicate Presence of Measurement Agent
  - Heartbeat messages; sent in regular intervals
    - Encrypted nonce with hash of non-mutating state

RSA Conference 2005

19

Evaluation of Integrity Reports

- Setup: A Policy Describing Expected Results Is a Prerequisite
  - Reference hash and extend values for repeatable measurements
    - "Normal" boot sequence will be repeatable
    - Versioning means code changes are frozen
  - Heartbeat schedule and nonces
  - Authentication keys and trust anchors

- A Policy is Defined as part of Platform Deployment
  - Policy authoring is the transformation of reference values into rules
  - Rules languages such as XRML, XACML and SAML helpful
- Reference Values Should Come from an Authoritative Source
  - Manufacturer – to detect modification due to stolen or open source
  - Evaluation labs – who make assertions of quality and conformance
  - Platform Owner – the entity taking the risk!

RSA Conference 2005

20

Summary

- Trusted Computing Faces Many Challenges
  - Lack of assurance that environments are safe and remain safe
  - Ambiguous “endpoint” structure that is fractal and distributed
  - Data protection mechanisms that balance privacy with need to know
- Trusted Computing Platforms should Support Five basic Engines
  - Measurement, Storage, Reporting, Verification and Enforcement
  - Engines should be isolated and hardened to prevent compromises
- Endpoint Integrity is Key to Establishing Trust
  - Collecting history of boot integrity, operational integrity and installed software
  - Reporting and detecting evidence of unauthorized changes
  - Controlling changes through robust configuration and systems management
- Network Operators can Improve Trust by Enforcing Compliance at Network Connect
  - Define profiles for acceptable configurations
  - Verify compliance at time of connection and periodically thereafter
- The Trusted Computing Group Specifications and Architecture Help Achieve the Goal

RSA Conference 2005

21

Questions?

- Contact Information
  - The Trusted Computing Group
    - www.trustedcomputinggroup.org
    - admin@trustedcomputinggroup.org
  - Infrastructure Working Group Co-Chairs
    - Ned Smith / Intel
      - ned.smith@intel.com
    - Thomas Hardjono / Verisign
      - thomas.hardjono@verisign.com

RSA Conference 2005

22