Trusted Computing
Overview

Use Cases

Neil Kittleson
What is Trusted Computing?

- Trusted Computing is defined as the use of a computer when there is confidence that the computer will behave as expected.
- In practice, trusted computing is dedicated hardware that:
  - Protects a unique platform identity (TPM)
  - Verifies software integrity before software is loaded (TPM)
  - Protects network integrity (TNC)
  - Protects data integrity and confidentiality (SED)
- Information assets are protected by trusted computing technology by the ability to detect tampering with software before affected software is loaded.

A hardware “Root-of-Trust” is provided by a secure hardware chip, typically a Trusted Platform Module (TPM).
Protecting Credentials
Device Identity
Secure Execution

1. System powers on and program execution verifies BIOS/FIRMWARE

2. Hypervisor measures match

3. OS & Applications are launched

2. Hypervisor measure does not match

3. Hypervisor launch can be blocked
Data Protection
Crypto Erase
Case Studies
Case Study #1 – Professional Services Firm

Who
PricewaterhouseCoopers

Problem
› Protect company networks and information resources from unauthorized access through the use of stolen certificates
› Software tools designed to prevent export of certificate private keys can be subverted by Jailbreak, a free web download
› Jailbreaking certificates violates company and regulatory policy and is often a beach of contract

Additional Requirements
› Scalable to 150,000 employees at 850 locations in 142 countries
› No additional hardware
› Work across broad spectrum of applications
› Compatible with existing PKI infrastructure
› Centrally manageable
› Low cost
Case Study #1 – Professional Services Firm (cont’)

Solution

› TPMs in nearly 100% of computing platforms
› Wave Systems management software suite to provide scalable:
  • TPM provisioning
  • Application keying material management

Benefits

› No additional hardware required
› Compatible with existing PKI infrastructure
› Cost Effectiveness (three year projection, including licenses, deployment costs, and operational costs):
  • TPM solution is half the cost of smart card
  • TPM solution is one-third the cost of USB tokens
Case Study #2 – Automotive Manufacturer

Who

› Mazda North American Operations (MNAO)
  • Responsible for R & D, sales and marketing, parts and customer service in North America

Problem

› Protect customer personal identifiable information and confidential business information on Laptops

Additional requirements

› IT burden had to be low to none
› Data protection is the highest priority
› Protection against lost or stolen laptops
Solution

› Self Encrypting Drives (SEDs) and Wave Systems SED management application
  • Centralized administration of users, credentials and access privileges
  • Policy based controls
  • Proof of Compliance
  • Simplified machine re-provisioning, data destruction and EOL best practices
  • SSO, Windows® Password Synchronization
  • Password recovery “Help Desk” capabilities

Benefits

› Protects mobile data
› “Built in” encryption minimizes setup and support costs
› Centralized management of computer security policies
› Proof of compliance for data protection regulations
Case Study #3 – Safe & Lock Company

Who
› Diebold
  • Automated Teller Machine (ATM) pioneer
  • 170,000 employees in 90 countries
  • Delivering self-service solutions and security systems for over 150 years

Problem
› ATM security is an ongoing concern
  • Aggressive, sophisticated criminals
  • $50B in ATM cash withdrawn annually
› Physical brute force attacks
  • Prevented by locks, cameras, safes
› Cyber attacks
  • Thieves hack into ATM
  • Bypass onboard computer
  • Use unauthorized computer to issue commands
  • Result: fraudulent withdrawals
Solution

› ATM on-board computer contains a TPM
› Wave management software integrated into ATM security framework
› Use TPM to generate hardware-based machine certificates within PKI infrastructure
› Unique, un-spoofable identifier for device authentication
› Also supports user certificates for service technicians

Benefits

› Hardware-level security provides stronger protection than software-only solution
› Standards-based security:
  • Ensures critical management functions
  • Provides assurance that applications run flawlessly with all TPM vendors – insulation from change
Case Study #4 – Host Integrity at Startup (HIS)

Goals:

- NSA Research initiative
- Measure and report integrity of platform from boot-up to log-in
- Detect occurrences of malware and unintended changes

Requirements

- Small pilot of 260 platforms
- Measure BIOS and pre-OS environment
- Report measurements to server for action
- Support Windows XP on Dell Optiplex 755 and higher

Implementation

- TPM Roots of Trust for Storage, Measurement and Reporting were used
- Integrated with existing infrastructure – Privacy CA worked with existing PKI infrastructure
- Non-invasive – No additional hardware necessary
- Initial focus on reporting – No additional action taken
- Inspired other pilots in Department of Defense
Next Steps
Conclusion

- Trusted computing is cyber defense technology that can be used to protect enterprise data, platforms and networks
- Trusted computing technologies are actively evolving, with new standards and new products regularly entering the market
- Major hardware manufacturers and software vendors support trusted computing off-the-shelf
- Trusted computing products can offer a cost-effective path to improved compliance and security