Consumerization of Trusted Computing

Dr. Michael Willett
Samsung
The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.

Member companies and individual members may use this material in presentations and literature under the following conditions:

- Any slide or slides used must be reproduced in their entirety without modification.
- The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.

This presentation is a project of the SNIA Education Committee.

Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.

The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.
ABSTRACT: Consumerization of Trusted Computing

State, Federal, and international legislation mandate the use of strong security measures to protect confidential and personal information. Businesses and governments react through due diligence by implementing security best practices. In fact, being secure in their management of information provides a competitive advantage and enhances the trust that consumers of products and services have in business/government.

The modern consumer also manages confidential and personal data, as well as sensitive applications. Net: The consumer, especially in this highly interconnected world, requires equivalent security best practices. The difference is the broad range of technical expertise in the consumer population (all of us!). The security functionality must be:

- Easy to use
- Transparent
- Robust
- Inexpensive

And, be a natural part of the computing infrastructure. Enter: Trusted computing, as defined and standardized by the Trusted Computing Group (TCG). The tenets of the TCG include: robust security functions in hardware, transparency, and integration into the computing infrastructure; a perfect match with the consumer requirements.

The TCG, an industry consortium with a broad industry, government, and international membership, has developed technical specifications for a number of trusted elements. Included are specifications for integrated platform security, network client security and trust, mobile device security, and trusted storage; all key components of the consumer computing experience.

For example, the storage specifications define the concept of Self-Encrypting Drives (SED). SEDs integrate the encryption into the drive hardware electronics, encrypting all data transparently that is written to the drive; and, with no loss in drive performance. The SED protects against loss or theft, whether a laptop or a data center drive. And, both business professionals and rank-and-file consumers lose a significant number of laptops, according to the FBI. The robust protection afforded the consumer is transparent, inexpensive, and easy to use.

Combining the performance, longevity, quietness, and ruggedness of a solid-state drive (SSD) with the SED function equips the consumer with a winning combination, all integrated into the infrastructure.

The session will provide:

- Overview of the security challenges facing the consumer
- Introduction to the tenets of the Trusted Computing Group, especially the integration of security into the computing infrastructure
- Description of the TCG/SED technology, as a relevant example of trusted computing
State, Federal, and international legislation mandate the use of strong security measures to protect confidential and personal information. Businesses and governments react through due diligence by implementing security best practices, which in their management of information provides a competitive advantage and enhances the trust that consumers of products and services have in business and government.

The modern consumer also manages confidential and sensitive data. The consumer, especially in this highly interconnected world, requires equivalent security best practices. The difference is the broad range of technical expertise in the consumer population (all of us!). The security functionality must be:

- Easy to use
- Transparent
- Robust
- Inexpensive
- And, be a natural part of the computing infrastructure.

Enter: Trusted computing, as defined and standardized by the Trusted Computing Group (TCG). The tenets of the TCG include: robust security functions in hardware, transparency, and integration into the computing infrastructure; a perfect match with the consumer requirements.

The TCG, an industry consortium with a broad industry, government, and international membership, has developed technical specifications for a number of trusted elements. Included are specifications for integrated platform security, network client security and trust, mobile device security, and trusted storage; all key components of the consumer computing experience.

For example, the storage specifications define the concept of Self-Encrypting Drives (SED). SEDs integrate the encryption into the drive hardware electronics, encrypting all data transparently that is written to the drive. SEDs protect against loss or theft, whether a laptop or a data center drive. And, both business professionals and rank-and-file consumers lose a significant number of laptops, according to the FBI. The robust protection afforded the consumer is transparent, inexpensive, and easy to use.

Combining the performance, longevity, quietness, and ruggedness of a solid-state drive (SSD) with the SED function equips the consumer with a winning combination, all integrated into the infrastructure.

The session will provide:

- Overview of the security challenges facing the consumer
- Introduction to the tenets of the Trusted Computing Group, especially the integration of security into the computing infrastructure
- Description of the TCG/SED technology, as a relevant example of trusted computing

ABSTRACT: Consumerization of Trusted Computing

Consumerization of I.T.

Easy to use
Transparent
Robust
Inexpensive

Complementary

Trusted Computing Group

Robust security in hardware
Transparency
Integration into infrastructure
How Do Standards Benefit Security?

- Using TCG standards reduces cost
  - Trusted Platform Module (TPM) is half the cost of a smart card, one-third the cost of a token – provides built-in authentication
  - TPMs are in every enterprise system now
- TCG standards cut deployment time
  - Already deployed on millions of products
  - Turn it on - no IT restart required
  - Plug and play with other available products such as Windows, Win Server, open source
- TCG enables multi-vendor interoperability
  - Standards-based products work with each other, offering users choice, lowering cost and fostering innovation
  - Plugfests ensure products work the same in different implementations
- International standardization and broad distribution drives adoption and membership in TCG
  - ISO/IEC has approved the TPM specification
Trusted Systems: Now Ubiquitous
Trusted Systems Widely Available

Estimated Growth Plan
TCG Technology

<table>
<thead>
<tr>
<th></th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>100</td>
<td>125</td>
<td>156</td>
<td>196</td>
</tr>
<tr>
<td>Embedded</td>
<td>100</td>
<td>125</td>
<td>156</td>
<td>196</td>
</tr>
<tr>
<td>PCs</td>
<td>350</td>
<td>438</td>
<td>547</td>
<td>684</td>
</tr>
</tbody>
</table>

http://www.trustedcomputinggroup.org/resources/rsa_conference_2013_tcg_overview
Authentication

**Trusted Platform Module (TPM):** Nearly every business laptop comes with an **embedded security token.** TPMs uniquely support both user and machine authentication in one token, ensuring only authorized users and authorized PCs are on the network.

<table>
<thead>
<tr>
<th>Email</th>
<th>Strengthen certificate-based email encryption with <strong>TPM key protection.</strong> Support for all X.509 certificate-based email encryption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor Authentication</td>
<td>Use the <strong>TPM for authentication to provide a first factor:</strong> &quot;something you have.&quot; An additional factor can be added for security such as a PIN or password for &quot;something you know.&quot;</td>
</tr>
<tr>
<td>VPN Access</td>
<td>A <strong>TPM can achieve a hardware level of security</strong> without the costs and hassles associated with deploying and managing smart cards or hardware tokens.</td>
</tr>
<tr>
<td>Wireless Access</td>
<td>A <strong>TPM securely can identify a user or machine and automatically integrates with the 802.1x authentication framework.</strong></td>
</tr>
</tbody>
</table>
Self-Protection – TPM

Hash -> TPM

Hash VALID

Decrypt

System Image

System Image

System Image

System Image

Hash INVALID

Decrypt

System Image

System Image

System Image

System Image

# Network Access Control (NAC) and Identify

**TNC = Trusted Network Connect**

<table>
<thead>
<tr>
<th>Guest Access</th>
<th>TNC specifications enable vendors to craft effective systems that <strong>enable guest access</strong>, without threat to the host network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Authentication</td>
<td>TNC supports <strong>authentication of users</strong> to further protect the network and to better manage who is using the network and what is happening.</td>
</tr>
<tr>
<td>Endpoint Integrity</td>
<td>TNC provides a common way to <strong>health-check clients</strong> as they attach to the network. Based on the user's own policies, these clients can be blocked from the network, quarantined, or sent to a separate network for remediation.</td>
</tr>
<tr>
<td>Clientless Endpoints</td>
<td><strong>Non-PC devices</strong> such as IP phones, cameras, physical security equipment and printers connect to the network and must be assessed for threats and vulnerabilities.</td>
</tr>
<tr>
<td>Decision Making</td>
<td>TNC's <strong>IF-MAP specifications provide a common way for security tools to communicate</strong>, resulting in data that can be shared and used at and during the network admission processes.</td>
</tr>
</tbody>
</table>
Basic NAC Architecture

- Access Requestor (AR)
- Policy Enforcement Point (PEP)
- Policy Decision Point (PDP)
Integrating Other Security Devices

Access Requestor (AR)

Policy Enforcement Point (PEP)

Policy Decision Point (PDP)

Metadata Access Point (MAP)

Sensors, Flow Controllers
Health Check

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

Production Network

Remediation Network

Policy Enforcement Point

Policy Decision Point

NAC Policy
Windows XP
- SP3
- OSHHotFix 2499
- OSHHotFix 9288
- AV (one of)
  - Symantec AV 10.1
  - McAfee Virus Scan 8.0
  - Firewall
Behavior Check

Access Requestor

Policy Enforcement Point

Policy Decision Point

Metadata Access Point

Sensors and Flow Controllers

Remediation Network

NAC Policy
• No P2P file sharing
• No spamming
• No attacking others
### Mobile Security
#### MTM = Mobile Trusted Module

#### Authentication
Many tablets have TPMs and Windows 8 for embedded security. **Mobile Trusted Module, MTM, offers a hardware root of trust in the device; supports secure transaction, safe storage of keys and certificates and assurance of integrity.**

#### Data protection
TCG offers standardized approach to encrypting storage devices where data is stored.

#### Transaction security
**TCG is aligned with Mobey Forum**¹ **to support secure mobile financial transactions.** Root of trust concept protects transactions and data.

#### BYOD security
TNC specifications enable identification and management of employee devices connecting to the corporate network.

#### Works with other mobile standards
**TCG works with the Global Platform Alliance to support its Trusted Execution Environment.** Aligned with Mobey Forum to support secure mobile financial transactions.

---


---

## Cloud Security

<table>
<thead>
<tr>
<th>End-to-end security</th>
<th>Trusted Computing standards <strong>allow cloud users to establish trust and enhance security using hardware-based roots of trust in multiple platforms</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection</td>
<td>Stored data is encrypted by on-drive hardware for data-at-rest protection</td>
</tr>
<tr>
<td>BYOD security</td>
<td>TNC architecture provides measurement of health and compliances for devices attaching to the cloud.</td>
</tr>
<tr>
<td>Multi-vendor, multi-source</td>
<td>Standards=interoperability and vendor choice</td>
</tr>
</tbody>
</table>
Data Protection

### Self-encrypting drive (SED)

Solutions, based on TCG specifications, enable integrated encryption and access control within the protected hardware of the drive.

<table>
<thead>
<tr>
<th>Encryption Performance</th>
<th>Operates at full drive speeds; scalable to large enterprises, since each drive has its own encryption engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stronger Security</td>
<td>Encryption is always on - major compliance requirement</td>
</tr>
<tr>
<td></td>
<td>Keys for encryption are generated in the drive, never leave the drive. User authentication is performed by the drive before it will unlock, independent of the operating system</td>
</tr>
<tr>
<td>Ease-of-Use</td>
<td>Much easier to use than software solutions. Encryption is transparent to both users and software; comes from the factory encrypting transparently</td>
</tr>
<tr>
<td>Cost-of-Ownership</td>
<td>No need for complex infrastructure to manage encryption keys</td>
</tr>
<tr>
<td></td>
<td>Main processor cycles not used for encryption</td>
</tr>
<tr>
<td></td>
<td>No modifications to OS, applications or tools</td>
</tr>
<tr>
<td></td>
<td>Crypto-erase provides instant repurposing / decommissioning/sanitization</td>
</tr>
</tbody>
</table>
EXAMPLE: Stored Data Protection
The Problem...

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches.

In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per record).

$6.65 Million Per Incident

http://www.privacyrights.org/ar/ChronDataBreaches.htm
The Problem...

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches.

Legal

Financial

Reputation

In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per record).

http://www.privacyrights.org/ar/ChronDataBreaches.htm

http://www.privacyrights.org/ar/ChronDataBreaches.htm
Example: California

... any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person…”

Encryption “safe harbor”
Why Encrypt Data-At-Rest?

**Threat scenario**: stored data leaves the owner’s control – lost, stolen, re-purposed, repaired, end-of-life, ...

- **Compliance**
  - 48+ U.S. states have data privacy laws with encryption “safe harbors”, which exempt encrypted data from breach notification
  - EU: Replace Data Protection Directive 95/46/EC (27 countries) requires breach notification

- Exposure of data loss is expensive ($6.65 Million on average per incident)

- Obsolete, Failed, Stolen, Misplaced…
  - Nearly ALL drives leave the security of the data center
  - The vast majority of retired drives are still readable

---

Encryption can be done in a number of places...

Host middleware
Host HBA (h/w adapter)
Application
Switch
“Bump in the wire” or proxy appliance
Array controller
Drive (HDD, SSD)
Encryption can be done in “layers”…

- Host middleware
- Host HBA (h/w adapter)
- Network Fabric
- Application
- Application Server
- Switch
- Array Controller
- “Bump in the wire” or proxy appliance
- Array controller
- Drive (HDD, SSD)
Encryption of Data At-Rest

Step-by-step Checklist

Version 2.0

9 September 2009

(available @
http://www.snia.org/forums/ssif/knowledge_center/white_papers/)
The Steps

1. Understand Drivers
2. Classify Data Assets
3. Inventory Data Assets
4. Perform Data Flow Analysis
5. Choose Points-of-Encryption
6. Design Encryption Solution
7. Begin Data Re-Alignment
8. Implement Solution
9. Activate encryption
The Steps (using SEDs)

Understand Drivers: breach laws
Classify Data Assets
Inventory Data Assets
Perform Data Flow Analysis
Choose Points-of-Encryption: drives
Design Encryption Solution: management
Begin Data Re-Alignment
Implement Solution: SED phase-in
Activate encryption: automatic

Greatly Simplified Using SEDs

- Data classification and asset inventory not required to support SEDs
- Higher layer encryption may additionally be mandated by regulations
Encryption upstream can affect other processes

- Data Compression
- Data De-duplication
- Data Loss Prevention (DLP)

Stored Data

ENCRYPTION

UPSTREAM
Trusted Storage Standardization

Trusted Computing Group

Published Storage Specifications
“Many organizations are considering drive-level security for its simplicity in helping secure sensitive data through the hardware lifecycle from initial setup, to upgrade transitions and disposal.”

Eric Ouellet
Research Vice President
Gartner
Client Security: Pre-Boot Authentication

- Transparency: Master boot record and OS are unmodified
- Protected from malicious software: Authentication occurs before OS (and any malicious software) is loaded
- The master boot record can’t be corrupted: The entire drive, including the master boot record, is encrypted

1. BIOS attempts MBR read; drive redirects to pre-boot area
2. Drive loads pre-boot OS
3. User enters authentication credentials for drive to verify
4. If authentication successful, drive loads original MBR
5. Normal operation commences
**Authentication in the Drive**

1. Correct $AK$?

   - Drive does NOT respond to Read or Write Reqs
   - Yes: Clear $AK$ decrypts $DEK$
   - No: Hash $AK$

2. $Clear AK$ decrypts $DEK$

3. $DEK$ encrypts and decrypts User Data

**Terms**

- **AK**: Authentication Key
- **DEK**: Data Encryption Key

**Notes**

- Pre-boot Authentication
- Hashed $AK$
- Encrypted $DEK$
- Clear Data
- Unlock HDD/SDD
- Encrypted User Data
- Consumerization of Trusted Computing
  © 2013 Storage Networking Industry Association. All Rights Reserved.
Crypto Erase

**Description**

- Cryptographic erase changes the drive encryption key
- Data encrypted with previous key, unintelligible when **DEcrypted** with new key

**Benefits**

- Instantaneous “rapid” erase for secure disposal or re-purposing
- Revision 1 of U.S. NIST SP800-88: *Guidelines for Media Sanitization* under way to support Crypto Erase

---

No Performance Degradation

Encryption engine speed

Matches

Port’s max speed

The encryption engine is in the drive electronics

Scales Linearly, Automatically

All data will be encrypted, with no performance degradation
IT Retires Drives Constantly

- All Drives are Eventually Retired
  - End of Life
  - Returned for Expired Lease
  - Returned for Repair / Warranty
  - Repurposed
- 50,000 drives leave data centers daily
- Exposure of data is expensive - $6.65 million on average
- 90% of retired drives are still readable (IBM study\(^1\))

Needed: A simple, efficient, secure way to make retired drive data unreadable

People make mistakes

“Because of the volume of information we handle and the fact people are involved, we have occasionally made mistakes.”

which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007


99% of Shuttle Columbia’s hard drive data recovered from crash site

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive’s platters over a two day period.

- May 7, 2008 (Computerworld)
How the Drive Retirement Process Works

Please refer to the image provided for details on the drive retirement process.

Retirement Options

- **Shredding**
  - Environmentally hazardous
  - Not always as secure as shredding, but more fun

Drive Retirement is:

- **Expensive**
- **Time-consuming**
- **Error-prone**

---


---

99% of Shuttle Columbia's hard drive data recovered from crash site

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive's platters over a two day period.

- May 7, 2008 (Computerworld)
Drive Retirement: Self-Encrypting

Self-Encrypting Drives

- Retire Drive
  - Replace
  - Repair
  - Repurpose
- Remove ALL drives
- Send even “dead” drives through Queue in secure area
- Transport Offsite
- Queue in secure area

Power Off = Locked/Encrypted = Secure

Added “insurance”: Crypto Erase

- Reduces IT operating expense
  - Eliminates the need to overwrite or destroy drive
  - Secures warranty and expired lease returns
  - Enables drives to be repurposed securely

- Provides safe harbor for most data privacy laws
Encryption key never leaves the drive. No need to track or manage …

BUT, YOU STILL MANAGE THE AUTHENTICATION KEYS (drive locking),
to protect against loss or theft (for just crypto erase, no authentication key needed)

• To recover data from a drive:
  • Only need the Authentication Key and the drive
  • Don’t need to escrow the encryption key to maintain data recoverability
  • Don’t need to track encryption key storage separate from data storage
  • Don’t need to be concerned with interoperability of encryption key storage and data
Hardware-Based Self-Encryption versus Software Encryption

- **Transparency**: SEDs come from factory with encryption key already generated

- **Ease of management**: No encrypting key to manage

- **Life-cycle costs**: The cost of an SED is pro-rated into the initial drive cost; software has continuing life cycle costs

- **Disposal or re-purposing cost**: With an SED, erase on-board encryption key

- **Re-encryption**: With SED, there is no need to ever re-encrypt the data

- **Performance**: No degradation in SED performance

- **Standardization**: Whole drive industry is building to the TCG/SED Specs

- **No interference** with upstream processes

**ISSUE**: Hardware acquisition (part of normal replacement cycle)
## Performance Comparisons:
### HDD and SSD, software versus SED

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Startup</strong></td>
<td>7.90</td>
<td>6.97</td>
<td>7.99</td>
<td>82.50</td>
<td>47.90</td>
<td>95.33</td>
</tr>
<tr>
<td><strong>App Loading</strong></td>
<td>7.03</td>
<td>5.77</td>
<td>5.71</td>
<td>48.33</td>
<td>30.77</td>
<td>60.37</td>
</tr>
<tr>
<td><strong>Modest size file test</strong></td>
<td>6.13</td>
<td>5.00</td>
<td>5.28</td>
<td>41.13</td>
<td>26.77</td>
<td>50.40</td>
</tr>
<tr>
<td><strong>Large Scale Data Read</strong></td>
<td>84.67</td>
<td>52.88</td>
<td>82.75</td>
<td>178.00</td>
<td>70.23</td>
<td>169.33</td>
</tr>
<tr>
<td><strong>Large Scale Data Write</strong></td>
<td>79.60</td>
<td>49.50</td>
<td>50.31</td>
<td>170.80</td>
<td>63.60</td>
<td>164.50</td>
</tr>
</tbody>
</table>

http://www.trustedstrategies.com/
The Future: Self-Encryption Everywhere

- **Encryption everywhere!**
  - Data center/branch office to the USB drive

- **Standards-based**
  - Multiple vendors; interoperability

- **Unified key management**
  - Authentication key management handles all forms of storage

- **Simplified key management**
  - Encryption keys never leave the drive. No need to track or manage.

- **Transparent**
  - Transparent to OS, applications, application developers, databases, database administrators

- **Automatic performance scaling**
  - Granular data classification not needed
SUMMARY: Layered Encryption

- Higher-level encryption
- Data context awareness
- Specific legislation requirements
- Encryption-to-storage protection

- Less data context awareness
- Encryption closer to storage
- Self-encrypting drives:
  - Encrypt everything!
  - Transparently
Thank You!
SNIA Security Technical Work Group (TWG)
- Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - [http://www.snia.org/tech_activities/workgroups](http://www.snia.org/tech_activities/workgroups)

Storage Security Industry Forum (SSIF)
- Focus: Marketing collateral, educational materials, customer needs, whitepapers including the BCPs & Encryption of Data At-Rest (a Step-by-Step Checklist)
  - [http://www.snia.org/forums/ssif](http://www.snia.org/forums/ssif)
The SNIA Education Committee thanks the following individuals for their contributions to this Tutorial.

**Authorship History**

Dr. Michael Willett

**Updates:**

Trusted Computing Group

**Additional Contributors**

Gianna DaGiau
Eric Hibbard
Anne Price
Brian Berger

*Please send any questions or comments regarding this SNIA Tutorial to tracktutorials@snia.org*