Enterprise Security with Trusted Computing

Dhiwakar Viswanathan
Infineon Technologies India Private Limited, Bangalore
www.infineon.com
Contents

- Why do we need trusted computing?
- What is Trusted Computing?
- What is Trusted Platform Module and what does it offer?
- What does Trusted Computing offer for enterprise?
- Infineon at a glance
- Q & A
Today’s IT environment

- Resulting in
  - Pervasive network
  - External / Internal security threat (Attack, Theft, Fraud, Virus, Worm, Trojan horse)
  - Threat by ‘insecure’ applications (e.g. XML, Spyware)

New business network model i.e. B2B, B2C via Internet

Open enterprise network system
Typical security concerns

- Clients
  - BOT infections

- Servers
  - Phishing website hosts

- Storage
  - Identities breached due to data loss and theft

- Network
  - Conficker infections

- Majority of IT security incidents have 3 underlying technological flaws
  - Weak authentication: single factor, password only
  - No data protection: unencrypted plain data
  - Compromised systems: malware, tampered
Common security practices

User

What You Know
(Password)

What You Have
(Smartcard/Token)

Who You Are
(Biometric)

Server

VPN
IPSEC
SSL
Today’s needs in Enterprise security

<table>
<thead>
<tr>
<th>Security Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td>Definite identification of people and systems</td>
</tr>
<tr>
<td></td>
<td>“Whom am I talking to?”</td>
</tr>
<tr>
<td><strong>Data Integrity</strong></td>
<td>Data is not manipulated</td>
</tr>
<tr>
<td></td>
<td>“Is the data reliable?”</td>
</tr>
<tr>
<td><strong>System Integrity</strong></td>
<td>The system has not been changed</td>
</tr>
<tr>
<td></td>
<td>“Is my PC for sure not manipulated?”</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Prevent tracking and tapping</td>
</tr>
<tr>
<td></td>
<td>“Is somebody listening me?”</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Availability of data: &quot;anytime, anywhere&quot;</td>
</tr>
<tr>
<td></td>
<td>“Do I have access?”</td>
</tr>
</tbody>
</table>

Security is as strong as the weakest link in the chain
What is NOT security
Key element in trusted computing

- **Root Of Trust** in a system
  - To protect an entire platform including the entire span of software or devices

- Software alone cannot provide a secure Root Of Trust
  - Software can easily be analyzed, modified and copied

- Hardware based security at platform level allows balancing the security requirements between Software and Hardware

![Diagram showing security level vs. effort for SW and HW implementations]
The Trusted Computing Group (TCG) is an international open industry standards development group

- Announced in April 2004. Successor to TCPA for trusted computing specification development
- [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)

TCG Mission Statement

- Develop and promote open, vendor-neutral, worldwide industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms.

Compaq, HP, IBM, Intel and Microsoft established Trusted Computing Platform Alliance in 1999
<table>
<thead>
<tr>
<th>Trusted Computing</th>
<th>Trusted Client</th>
<th>Trusted Servers</th>
<th>Trusted Storage</th>
<th>Trusted Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Built In</strong></td>
<td>- Trusted Platform Module (TPM)</td>
<td>- Security Built In</td>
<td>- Self Encrypting Drive (SED)</td>
<td>- Security Built In &amp; Coordinated</td>
</tr>
<tr>
<td><strong>Features</strong></td>
<td>- Authentication</td>
<td><strong>Features</strong></td>
<td>- Encryption</td>
<td><strong>Features</strong></td>
</tr>
<tr>
<td></td>
<td>- Encryption</td>
<td></td>
<td>- Authentication</td>
<td>- Authenticate</td>
</tr>
<tr>
<td></td>
<td>- Attestation</td>
<td></td>
<td></td>
<td>- Health Check with endpoint integrity</td>
</tr>
</tbody>
</table>

**Trusted Client**
- Security Built In
  - Trusted Platform Module (TPM)
  - Mobile Trusted Module (MTM)

**Features**
- Authentication
- Encryption
- Attestation

**Trusted Servers**
- Security Built In
  - Trusted Platform Module (TPM)
  - Secure Virtualization and Cloud

**Features**
- Authentication
- Encryption
- Attestation

**Trusted Storage**
- Security Built In
  - Self Encrypting Drive (SED)

**Features**
- Encryption
- Authentication

**Trusted Network**
- Security Built In & Coordinated
  - Trusted Network Connect (TNC)

**Features**
- Authenticate
- Health Check with endpoint integrity
- Behavior Monitor
- Enforcement
Trusted Computing application fields

- Mobile Phones
- PDAs
- Security Infrastructure
- Applications
- Credentials
- Operating Systems
- Web Services
- Storage
- Servers
- Notebooks
- Desktops
- PDAs
- Trusted Platform Module
  - The “root of trust” of the system.
  - The TPM is a HW security engine that stores secrets and prevents many common software attacks.
The Trusted Computing Group Standard

- TCG defines a comprehensive and generic standard to enable trusted platforms and trusted computing
- Today about 2700 pages in total publicly available on the TCG-Server

### Trusted Computing Platforms

<table>
<thead>
<tr>
<th>Hard Copy</th>
<th>Infrastructure</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Hard Copy" /></td>
<td><img src="image" alt="Infrastructure" /></td>
<td><img src="image" alt="Mobile" /></td>
</tr>
<tr>
<td>This group is defining open, vendor-neutral specifications for hardcopy devices that will use TCG components to establish their root of trust.</td>
<td>This group defines architectural framework, interfaces and metadata necessary to bridge infrastructure gaps.</td>
<td>This group provides trust for mobile devices including mobile phones and PDAs.</td>
</tr>
<tr>
<td>» Visit the Hard Copy section.</td>
<td>» Visit the Infrastructure section.</td>
<td>» Visit the Mobile section.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PC Client</th>
<th>Server</th>
<th>Software Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="PC Client" /></td>
<td><img src="image" alt="Server" /></td>
<td><img src="image" alt="Software Stack" /></td>
</tr>
<tr>
<td>This group provides common functionality, interfaces and a set of security and privacy requirements for PC clients that use TCG components to establish their root of trust.</td>
<td>This group provides definitions, specifications, guidelines and technical requirements as they pertain to the implementation of TCG technology in servers.</td>
<td>This group provides a standard set of APIs for application vendors who wish to make use of the TPM.</td>
</tr>
<tr>
<td>» Visit the PC Client section.</td>
<td>» Visit the Server section.</td>
<td>» Visit the Software Stack section.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storage</th>
<th>Trusted Network Connect</th>
<th>Trusted Platform Module (TPM)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Storage" /></td>
<td><img src="image" alt="Trusted Network Connect" /></td>
<td><img src="image" alt="Trusted Platform Module (TPM)" /></td>
</tr>
<tr>
<td>The Storage Work Group is building upon existing TCG technologies and focusing on standards for security services on dedicated storage systems.</td>
<td>This group focuses on ensuring endpoint compliance with integrity policies at and after network connection.</td>
<td>This group created the Trusted Platform Module (TPM) specification, version 1.1b and 1.2. The TPM is the root of trust that is the basis of the work of the other TCG work groups.</td>
</tr>
<tr>
<td>» Visit the Storage section.</td>
<td>» Visit the Trusted Network Connect section.</td>
<td>» Visit the Trusted Platform Module (TPM) section.</td>
</tr>
</tbody>
</table>
Trusted Platform Module

What is it?
- Hardware based Root of Trust
- A secure controller with security engine bounded to the main board of a computing platform
- Capable to withstand logical and physical attacks
- Integrated in the booting process as well as in the operating system

What does it do?
- Stores unique PKI key pairs and credential securely
- Authenticate and provide information on the integrity of the platform
- Provide uniqueness of the platform
Cryptographic system basics

- **Three cryptographic algorithms in a crypto system**
  - **MESSAGE DIGEST (MD2-4-5, SHA, SHA-1, ...)**
    - Maps variable length plaintext into fixed length cipher text (irrecoverable)
  - **SECRET KEY (Blowfish, DES, IDEA, RC2-4-5, Triple-DES, AES)**
    - Encrypt and decrypt messages by using the same Secret Key
  - **PUBLIC KEY (DSA, RSA, ECC)**
    - Encrypt and decrypt messages by using two different Keys: Public Key, Private Key (coupled together)

- **Digital Signatures** is a data item that vouches the origin and the integrity of a Message
  - Originator signs using with private key; Recipient verifies with public key
Digital certificate

A Digital Certificate binds an entity’s Public Key and one or more Attributes relating its Identity
A Public Key Infrastructure supports and manage Public Key-based Digital Certificates
Components of TPM

Secure uC based on the certified Smart Card technology integrated with secure hardware features

- **Secure Key Storage**
  - Protected NVM

- **Cryptography**
  - RSA Accelerator
  - Hash Accelerator (SHA-1)

- **Key Generation**
  - True Random Number Generator
  - RSA Key Generator

- **Hashing**
  - Hash Accelerator (SHA-1)

“Smartcards are ‘convenient and secure media’ meant for information storage and processing”
TPM in a host platform

TPM - Firmware (TPM-OS and Security Functions)

Boot-BIOS

Memory Absent/Present Driver

Application

Crypto Infrastructure

TCG Crypto Service Provider

TSS Service Provider

TSS Core Services

TPM-Device–Driver Library

TPM-Device -Driver

TPM Chip

Sep 2011
TPM main feature #1: Providing the root for the “chain of trust”

- The Core Root of Trust for Measurement (CRTM) MUST be an immutable portion of the Platform’s initialization code that executes upon a Platform Reset.

- The Platform’s execution MUST begin at the CRTM upon any Platform Reset.
TPM main feature #2:
Secure storage of keys

- **Endorsement Key**
  - Confirms TPM originates from a secure source
- **Platform Certificate**
  - Confirms that a valid TPM is mounted in a correct platform
- **Conformance Certificate**
  - Confirms the security functions of TPM and platform are compliant with TCG
- **Storage Root Key**
  - Forms the root of a key hierarchy in which other lower-order keys, data (blobs) are securely stored

- **Storage Key**
- **Signature Key**
- **AIK Key**
- **Gen. Data**
TPM Main Feature #3: Attestation

- A mechanism to allow the verifier to check the platform integrity (software and hardware) with the help of trust centre
  - Creates a hash of summary of the hardware and software
- Performed by Attestation Identity Key, which is derived from Storage Root Key
TPM enabled PC: System Overview

TPM Professional Package
Management Software

Application Support Layer
- TSS API
- TPM-CSP MS-CAPI
- TPM-CSP PKCS#11

Applications

TSS
(Trusted Computing Software Stack; Core Service, Driver)

Stack

TPM Firmware

Hardware
MS-CAPI and PKCS#11 Interfaces allow other applications to easily take advantage of TPM

- Microsoft CAPI Cryptographic Service Provider (CSP)
  - Keys and certificates protection

- PKCS#11 Cryptographic Service Provider (CSP)
  - Keys, certificates and objects protection
Examples of TPM usage

- Strong login authentication
- Multi-factor authentication
- Platform integrity
- Strong client/server authentication
- Secure cryptographic service provider
  - For email encryption, authentication etc
- Password vaults
- File and folder encryption
Enterprise motivation for TPM deployment

- Data Protection
  - File, Folder, and Full Disk Encryption
  - Secure messaging
- Strong Authentication of Platform and Users
  - WLAN, VPN
  - 2nd factor/multi-factor authentication
  - ECert based, bound to platform
- Network Access Protection
- Integrity Metrics and Policy Enforcement

Take immediate advantage of the high security that TPM-equipped platforms offer
Enterprise-grade Management of TPM-enabled Platforms

Infineon is the only company that provides a complete solution

TPM Client SW
(TPM Professional Package)

TPM Security Chip

Server SW
(Trusted Computing Management Server, TCMS)

- Ensuring platform integrity
- Strong authentication of the Trusted Platform to a network
- Secure Storage of Secrets and Keys
Infineon Professional Package and TCMS

**Professional Package (Client)**
- On every TPM enabled PC
- TPM vendor neutral
- Simplified User Interface
- Managed by Trusted Domain Admin

**TCMS (Server)**
- Centrally manages deployment & operation of PC-based TPMs in Trusted Domain
- Manages all TPM key, policy, and configuration
- Provides key lifecycle management for TPM-aware applications
- Synchronizes with AD
## TPM Professional Package Key Features

### Management and TPM-Access
- Communication and resource Management Service for the TPM
- TPM Chip configuration
- Password Management
- Certificate Management
- Backup/Restore for Keys and Settings
- Configuration for Application integration
- Diagnostic Support

### Application Integration
- Secure Email
  - MS Outlook, Outlook Express / Windows Mail, Thunderbird, ...
- SSL Client/User Authentication
  - MS Internet Explorer, Firefox, ...
- VPN Client/User Authentication
  - Microsoft VPN, Checkpoint VPN, RSA SecureID, ...
- (W)LAN Access Control via IEEE 802.1X
  - MS WLAN Stack, ...
- Microsoft Encrypting File System
- Document signing
  - Adobe Acrobat, MS Office 2007, ...

### Application
- Personal Secure Drive
  - An encrypted logical volume
Trusted Computing Management Server
Key Features

- **Platform and User Enrollment/Removal**
  - Automatic enrollment for platforms and users belonging to enrollment group (with Endorsement Key trust verification)
  - Secure audit capability

- **Password Reset**
  - Management GUI allows Trust Domain Administrator to prepare user password reset based on Trust Domain password reset key
  - Secure audit capability

- **Dictionary Attack Defense Level Reset**
  - Preparation and automatic reset

- **Platform Restore**
  - Backup/restore feature prevents data loss in event of failure of TPM or storage media
  - Restores key and certificate data, platform security features such as TPM-enhanced Windows Encrypted File System configuration, Personal Secure Drive configuration

- **Full User Roaming**
  - Synchronize credential updates when user logs on to any supported platform
  - Notification of updates, changed credentials
Platform Initialization

*Trusted Computing Management Server TCMS*

Platform Initialization

- Automatic TPM initialization and take-ownership in a trusted domain
- Automatic generation or import of platform keys and credential backup
User Initialization

User Initialization

- Automatic user initialization at first logon
- User Key generation or import via MS-CAPI or PKCS#11
- Automatic user credential backup
User Roaming

**Trusted Computing Management Server TCMS**

User Roaming

- Automatic and secure synchronization of TPM-protected User Keys between multiple PCs

- Supports PC-upgrade scenario
Helpdesk Support

Trusted Computing Management Server TCMS

Help Desk Support

• Solves the #1 cause of help desk calls: forgotten passwords

• Helpdesk assisted, secure and auditable password reset
Infineon at a glance

Automotive
- Power Semiconductors
- Power ICs
- Microcontrollers
- Sensors
- Electric Drive train

Industrial & Multimarket
- Power Discrete
- Power Modules
- Power ICs
- ASICs
- RF & Protection Devices
- Microcontroller

Chip Card & Security
- Payment
- Communication
- Entertainment
- Government ID
- Personal & Object ID
- Platform Security

Innovative semiconductor solutions for Energy Efficiency, Mobility and Security applications #1 in all 3 target markets
Chip Card & Security Business Lines

Business Line Payment & Communication
- Mobile Communication
  - SIM Card
  - Cellular M2M
- Payment
  - ePurse
  - Credit Cards
  - Debit Cards

Business Line Government Identification
- Electronic Passport
- National Electronic ID Card
- Electronic Health Care Card / Electronic Social Security Card
- Electronic Driver License

Business Line Personal & Object Identification
- Personal Identification
  - Transport
  - Access Control
  - Loyalty Schemes
  - Public Telephony
- Object Identification
  - Libraries
  - Document & Media Mgmt
  - Laundry
  - Pharma & Healthcare
  - Factory Automation

Business Line Platform Security
- Pay TV
- Trusted Platform Modules
- Embedded Security
Q & A

Please visit www.infineon.com

Dhiwakar.Viswanthan@infineon.com
- Head of Chip Card and Security
- Infineon Technologies India Private Limited, Bangalore

Mr. Merlin Lucas (Merlin.Lucas@infineon.com)
- Business Development Manager
- Chip Card and Security
- Infineon Technologies India Private Limited, Bangalore
Making COMPUTING so secure even your biggest secrets are safe.

Protected by Trusted Platform Module (TPM)
TPM Professional Package
Feature Overview of version 3.7

- TCG V1.2 compliant TSS Stack
  - TPM Device driver
  - TPM Device Driver Library
  - TSS Core Service
  - TSS Service Provider
- Easy initialization with wizards
  - Security platform initialization
  - Security platform user initialization
  - Simplified Initialization
- Management support
  - Automatic backup and restore
  - Key and certificate migration
  - Secure Password reset
  - Certificate viewer and PKCS#12 import
  - Additional management functionality
- Operating Systems
- Rebranding
  - Customer Rebranding tools available
- Centralized system administration:
  - Silent mode initialization
  - Scripting functionality
  - Secure password reset management
  - Automatic and scheduled backup
  - Group policies (computer/user)
- Application support
  - MS CAPI & PKCS#11 TPM CSP
  - TSS-API via COM interface
  - Integration and Administration SDKs
  - Support of secure email
  - File and folder encryption
  - Personal secure drive
- Security
  - Enhanced authentication via Smartcard and USB token
  - WLAN authentication support
  - Dictionary Attack Prevention
- Languages
  - Localized in 12 Languages
Infineon TPM Professional Package
Global Language Localization Strategy

- Chinese (simplified)
- Chinese (traditional)
- English
- French
- German
- Italian
- Japanese
- Korean
- Spanish
- Brazilian Portuguese
- Spanish
- Russian
Security Certification
Levels of Common Criteria

CC

Assurance level

EAL 7
formally verified design and tested

EAL 6
semi formally verified design and tested

EAL 5
semi formally designed and tested

EAL 4
methodically designed, tested, and reviewed

EAL 3
methodically tested and checked

EAL 2
structurally tested

EAL 1
functionally tested

White Box concept:
Evaluation Lab gets all internal information of supplier.

Black Box concept:
Evaluation Lab TOE as black box, no add. internal information of supplier -> “security by obscurity”
Common Criteria Certification Process

Three different parties are involved in a complex process:

- **Applicant**: Definition of TOE and Security Targets
- **Evaluation Body**: Evaluation documentation according to ITSEC / CC
- **Certification Body**: Evaluation by a trusted third party, Certification by a national certification body