2110413 Computer Security

Lecture 7

Trusted Computing Platform: God or Evil?

Krerk Piromsopa, Ph.D.
Department of Computer Engineering
Chulalongkorn University

Outline

- Objectives
- Components
- Applications
- Criticism
- TPM (Hardware)
- Software

Business Objectives

- Prevent use of unlicensed software
- DRM
  - No CD ripping and DivX creation
  - Plug "analog hole"
  - Information flow control
- PC as Media Center
- Official operation

Overview

- Trusted Computing
- Promoted by Trusted Computing Group
  - founded in 1999 by intel, MS, HP, Compaq, IBM
  - more than 170++ members today
- Make sure that computer will behave in specific ways
- Enforced by hardware and software
- Use a unique ID and encryption (without any knowledge

Core Technology

- **Protected Execution:** Provides applications with the ability to run in isolated protected execution environments such that no other unauthorized software on the platform can observe or compromise the information being operated upon. Each of these isolated environments has dedicated resources that are managed by the processor, chipset and OS kernel.

Core Technology

- **Sealed storage:** Provides for the ability to encrypt and store keys, data or other secrets within hardware on the platform. It does this in such a way that these secrets can only be released (decrypted) to an executing environment that is the same as when the secrets were encrypted. This helps prevent attacks exploiting the vulnerability where the encrypted data has been transferred to other platforms either for normal use (thereby become decrypted) or for malicious attack.

Core Technology

- **Protected Input:** Provides a mechanism that protects communication between the keyboard/mouse and applications running in the protected execution environments from being observed or compromised by any other unauthorized software running on the platform. For USB input, LT does this by cryptographically encrypting the keystrokes and mouse clicks with an encryption key shared between a protected domain's input manager and an input device. Only applications that have the correct encryption key can decrypt and use the transported data.

Core Technology

- **Protected graphics:** Provides a mechanism that enables applications running within the protected execution environment to send display information to the graphics frame buffer without being observed or compromised by any other unauthorized software running on the platform. This is done by creating a more protected pathway between an application or software agent and the output display context (such as a window object).

Core Technology

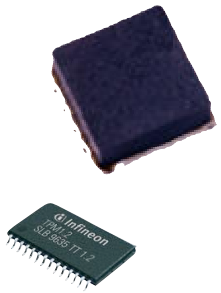
- **Attestation:** Enables a system to provide assurance that the LT protected environment was correctly invoked. It also provides the ability to provide a measurement of the software running in the protected space. The information exchanged during an attestation function is called an Attestation Identity Key credential and is used to help establish mutual trust between parties.

Core Technology

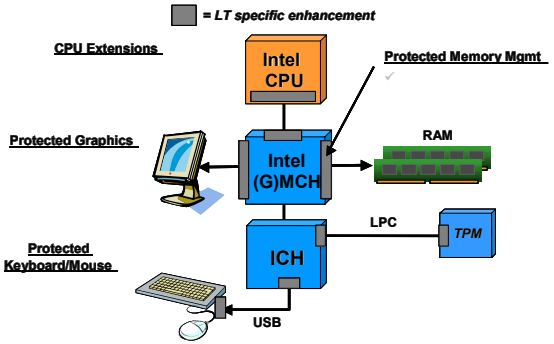
- **Protected Launch:** Provides for the controlled launch and registration of the critical OS and system software components in a protected execution environment.

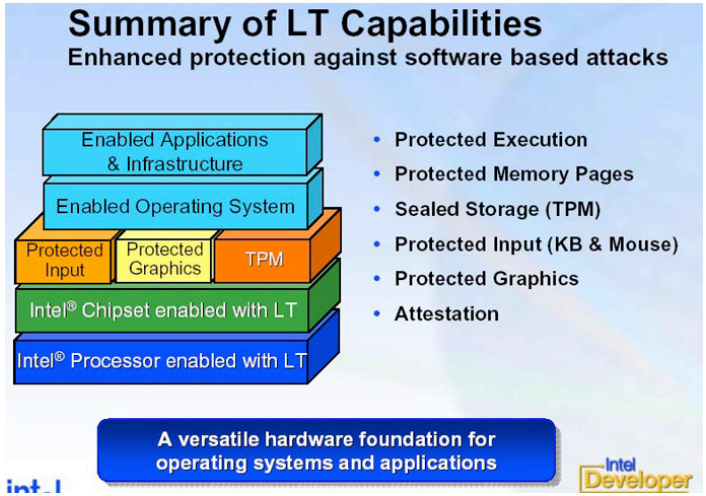
Hardware (TPM)

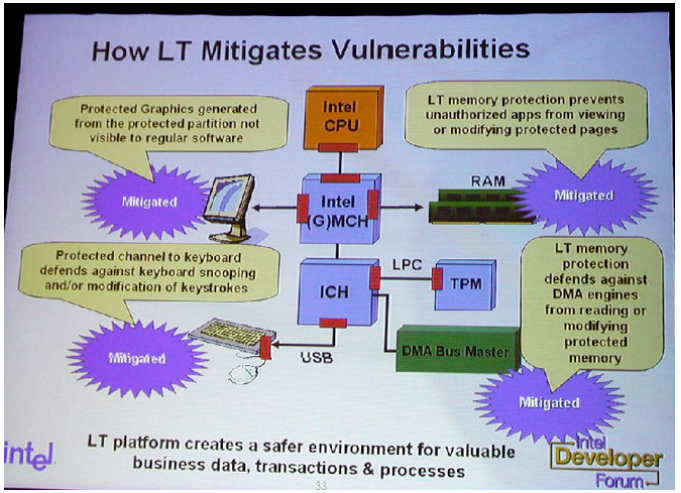
- Trusted Platform Module (TPM)
  - Fritz Chip
- Tamper resistant ?
- Surface mount



Intel LaGrande





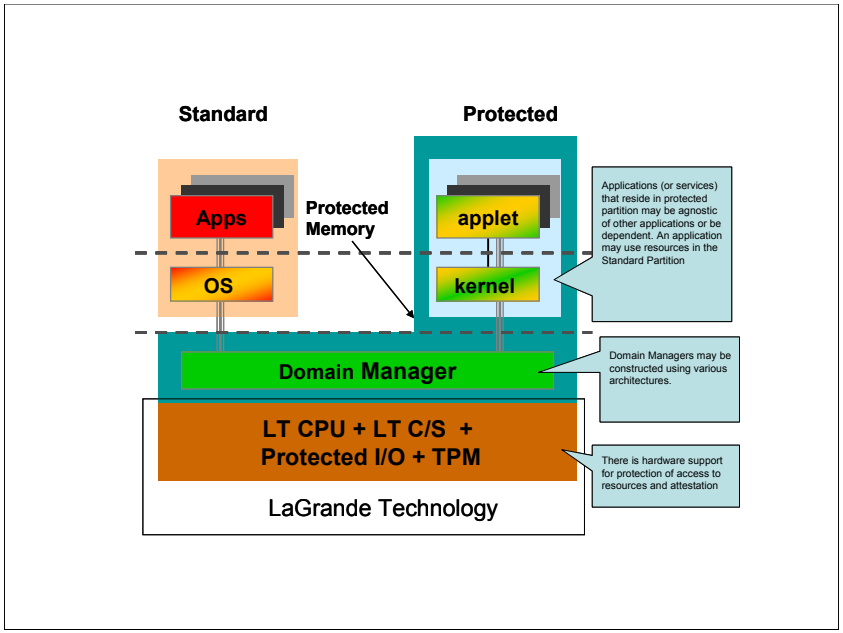


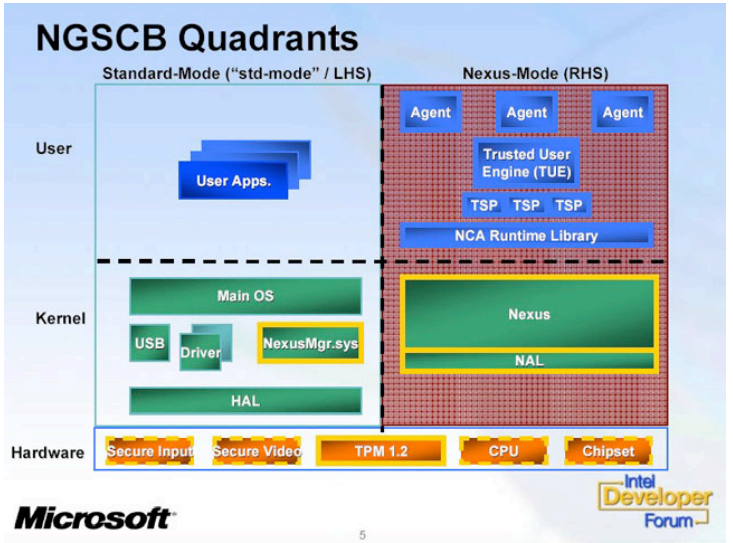
What does it mean?

- Prevent the owner from obtaining root access
- Three domains
  - Privileged access
  - Under privileged access
  - Unprivileged access

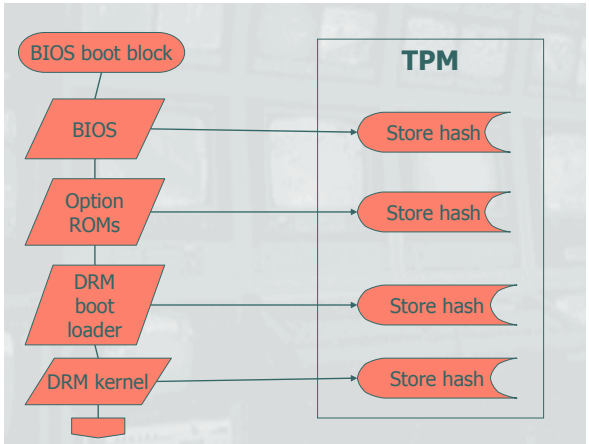
Concepts

- Endorsement key (2048-bit RSA public and private key) is created randomly on the chip at manufacture time and cannot be changed. The private key never leaves the chip.
- Designed to make the extraction of this key by hardware analysis hard.
- Every TPM is required to sign a random number, etc.
- Support several cryptography

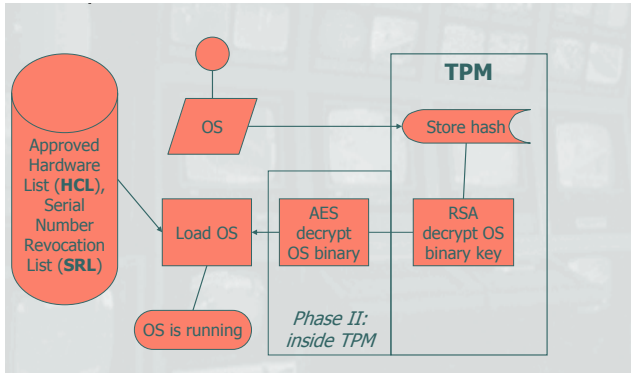




TCP Boot



OS Boot



Initial State/Tasks

- BIOS, I/O devices (+PCI card, DMA devices) are TCPA-approved.
- Secure time counter
- Synchronize system time

Applications

- Protecting hard-drive data
  (see Windows Vista Ultimate and Enterprise)
- Digital rights management
- Identity theft protection

Applications (ctd.)

- Preventing cheating in online games
- Protection from viruses and spyware ?
- Protection of biometric authentication data
- Verification of computer (e.g. grid computing)

Sample

- You could create Word documents that could be read only.
- A music can only be played on certain device/ software.
- What else?
- Open Source?

Criticism

- Digital rights management
- Unable to modify software (e.g. switch software)
- No control over data
- Unable to override
- Loss of anonymity
- Practicality
- Interoperability

FSF's Response

- Treacherous computing is a major treat to our freedom --- Richard M. Stallman.

Intelligence Collection

- Globally unique document IDs ?
- Undeniable proof of authorship
- Document tracking
- ??? (look around yourself) ???

Fritz Hollings S. 2048

- What is the penalty a person selling a non-TCPA approved will face under the bill?
  - Ticket ?
  - 6 months in jail
  - $500,000 fine and 5 years in prison (for first offense); double for the sub sequent.

AntiTCPA??

- See video