Computer Security and Cryptography

CS381

来学嘉
计算机科学与工程系 电院3-423室
34205440 1356 4100825 laix@sjtu.edu.cn

2016-06

Contents

- Introduction -- What is security?
- Cryptography
  - Classical ciphers
  - Today's ciphers
  - Public-key cryptography
  - Hash functions and MAC
  - Authentication protocols
- Applications
  - Digital certificates
  - Secure email
  - Internet security, e-banking

Network security
- SSL
- IPSEC
- Firewall
- VPN

Computer security
- Access control
- Malware
- Ddos/Intrusion
- Password
- Smartcard-TCP

Examples
- Bitcoin
- Wireless

contents

- Hardware-based security
  - Smartcard
  - Trusted Computing

Why hardware?

- Computer is often operating in insecure environment (worms, backdoor..)
- Lack of trusted in/ouput
- Software is easy to copy and modify

- Hardware
  - controlled, tamper-proof
  - Difficult to copy and modify

4

HSM

- **hardware security module (HSM) is a physical device for computing key-related crypto operations.**
- Secret is always inside the device
- **Is tamper resistant**
- **Used in critical infrastructure**

like PKI: CA HSM

- Smartcard, Chip-card, IC-card

5

Security hardware

Smart Cards

- **Types**
- **Applications**
  - **Payment**
  - **authentication**
- **Interface**
- **Physical Security**

TCP

Smart Card Types

SIM card

Crypto card

USB token

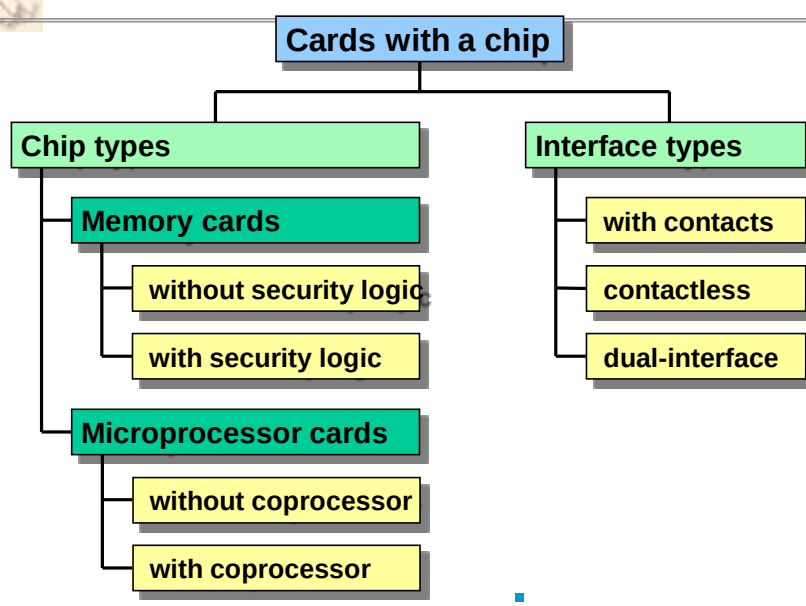
With I/O

Java card

Memory card

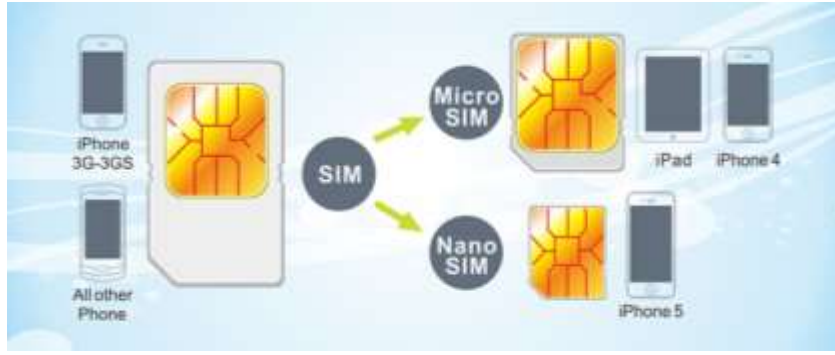
USB token

Smart Card Types



SIM card

SIM (subscriber identity modules) card



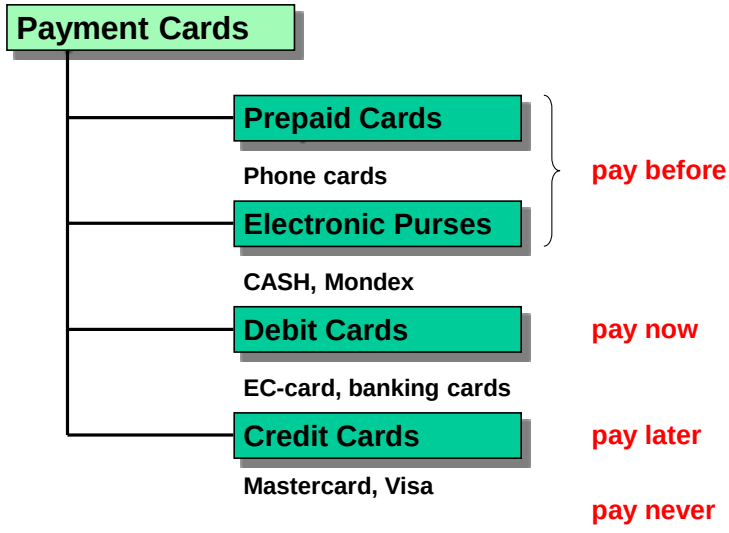
9

Security hardware

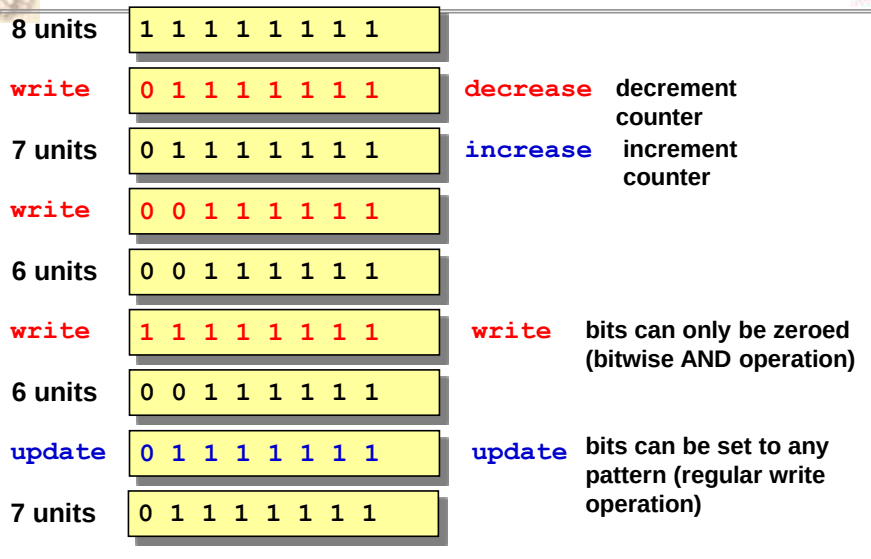
Smart Cards
- **Types**
- **Applications**
  - **Payment**
  - **authentication**
- **Interface**
- **Physical Security**

TCP

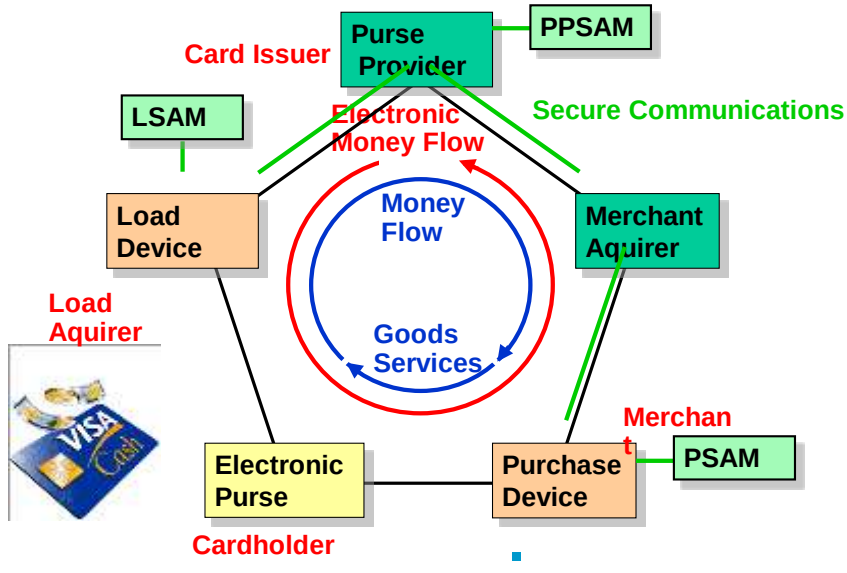
Payment Cards



Prepaid Cards



Electronic Purse – EN 1546



EMV – Europay, MasterCard, Visa

- **the objectives of EMV**
  - **EMV (www.emvco.com) specifies the requirements for interoperability between smart credit/debit cards (IC cards or smart cards) and interoperability between the terminals (ATM, POS).**
  - **RSA key-length: 1024, 1152, 1408, 1984 bits are used.**
  - **Europay, MasterCard, Visa, discovery, 银联**
- **Motivation**
  - **Against harvest PINs and clone of magnetic card**
  - **Europe (2013); US (2014); China (2014)**

银联 芯片卡

ATM

POS机

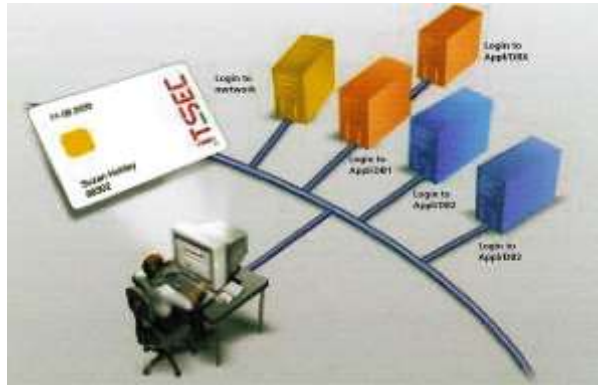
16

Security hardware

Smart Cards
- **Types**
- **Applications**
  - **Payment**
  - **authentication**
- **Interface**
- **Physical Security**

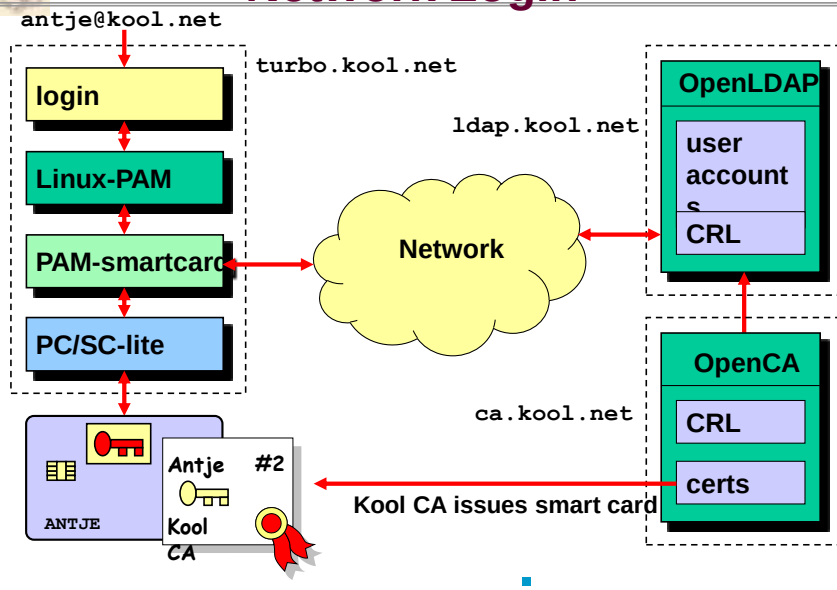
TCP

Single Sign On



- **Manage passwords for different applications**

Smart Card based Linux Network Login



ID card

22

Security hardware

Smart Cards
- **Types**
- **Physical Security**
- **Applications**
  - **Payment**
  - **authentication**
- **Interface**

TCP

Smart Card Terminal Interfaces

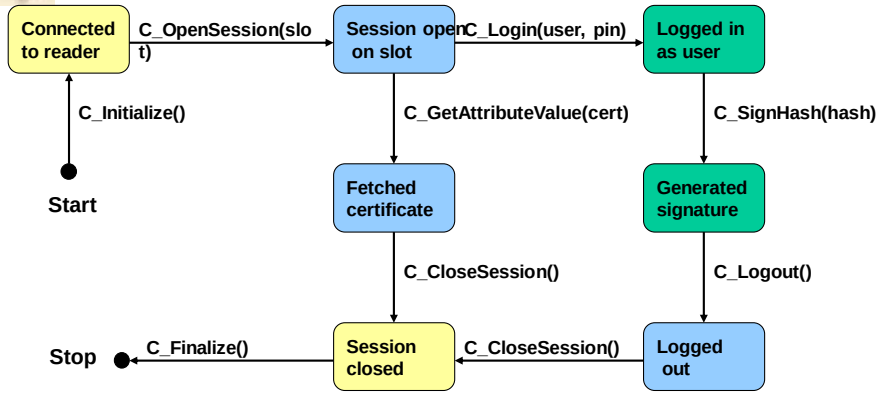
- PC/SC – Personal Computer / Smart Card
  - Version 1.0 specified in December 1997 by Bull, HP, Microsoft, Schlumberger, Siemens, Gemplus, IBM, Sun, Verifone and Toshiba.
  - PC/SC standard comprises 8 parts.
  - Originally targeted at Windows-based PCs
  - Ported to Linux thanks to the M.U.S.C.L.E project (pcsc-lite)
  - APIs for C, C++, Java and BASIC

PC/SC Workgroup

- OCF – Open Card Framework
  - Java-based interface, independent of the underlying operating system.
  - Has become an industry standard in Java environments.

OpenCard

PKCS#11 Cryptographic Token Interface Standard



- Standardized C/C++ Cryptoki API (cryptoki.h, pksc11.h)
- Simple object-based approach (slots, objects, attributes)
- Most smartcard vendors offer dynamic libraries (pkcs11.dll)

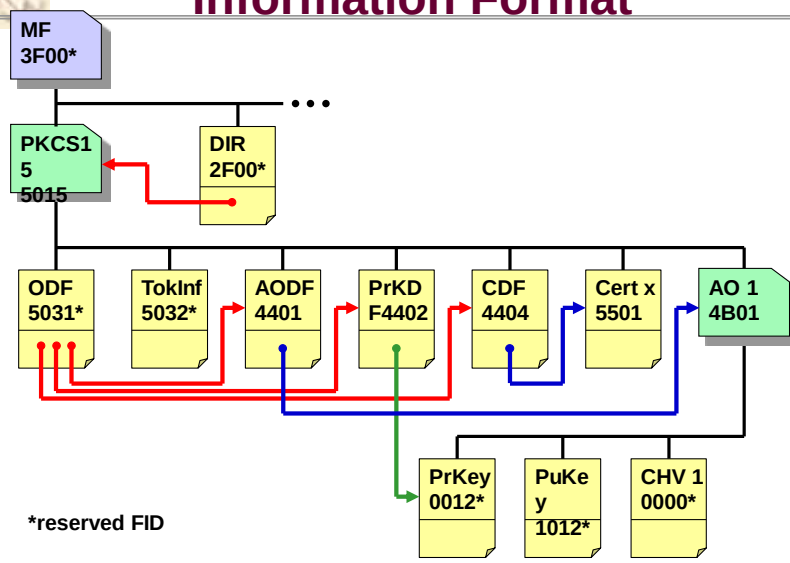
Finnish Electronic Identification Card (FINEID)

- **Issued by the Finnish local police. Cost 29 €, valid for 3 years**
- **Used for personal digital signatures over the Internet**
- **Contains two X.509 user certificates and matching RSA private keys**
- **Uses PKCS#15 Cryptographic Token Information Format Standard**

The Estonian ID Card

- **Contains two X.509 user certificates and matching RSA private keys**
- **Certified email address: name.surname_nnnn@eesti.ee**
- **Uses PKCS#15 Cryptographic Token Information Format Standard**
- **Uses OpenSC PKCS#11 drivers for Windows**

PKCS#15 Cryptographic Token Information Format



Additional PKCS#15 based Applications

- **Electronic ID Cards**
  - **Austria, Belgium, Estonia, Finnland, Italy, Latvia, Malta, Slovenia, Spain, Sweden. Germany in pilot phase.**
- **WIM – Wireless Identification Module**
  - **Uses SIM (GSM) or USIM (UMTS) or a second smart card in a dual slot mobile phone.**
  - **Can be used for client side authentication in the Wireless Transport Layer Security protocol WTLS that is part of WAP.**
  - **AID is A0 00 00 00 00 63 (RID) and "WAP-WIM" (PIX)**
- **The PKCS#15 standard is rapidly gaining wide-spread popularity and has become the de-facto standard for the information structure on cryptographic tokens.**

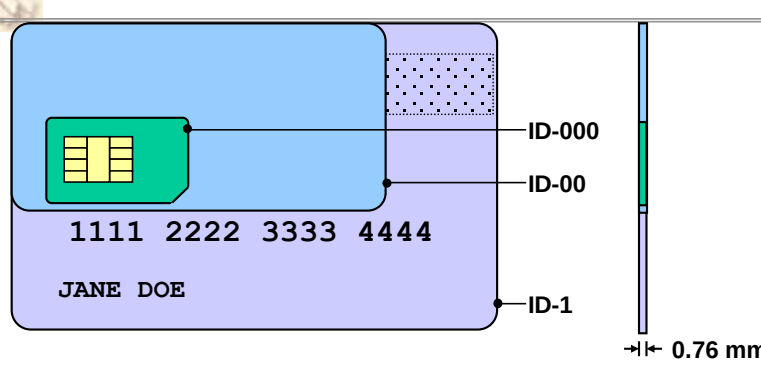
Security hardware

Smart Cards

- **Types**
- **Applications**
  - **Payment**
  - **authentication**
- **Interface**
- **Physical Security**

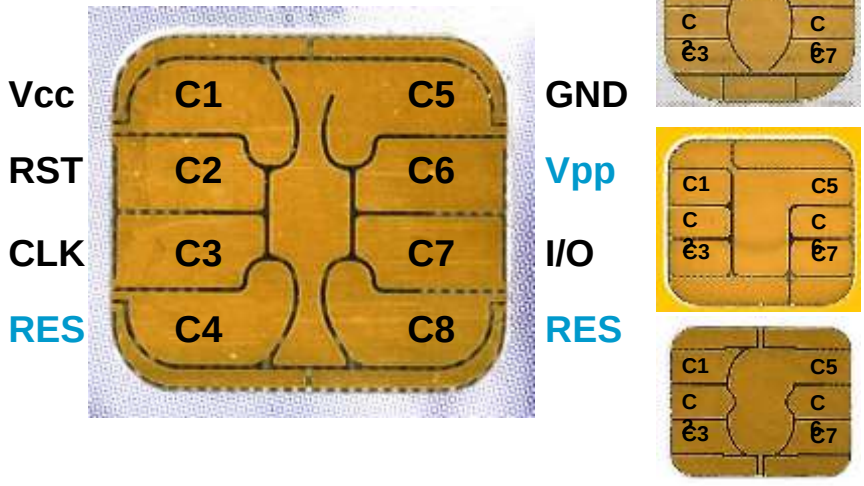
TCP

Physical Form Factors (ISO 7816)



- ID-1 54 x 85.6 mm (ISO 7810 credit card format)
- **ID-00 33 x 66 mm**
- **ID-000 15 x 25 mm (GSM SIM card)**

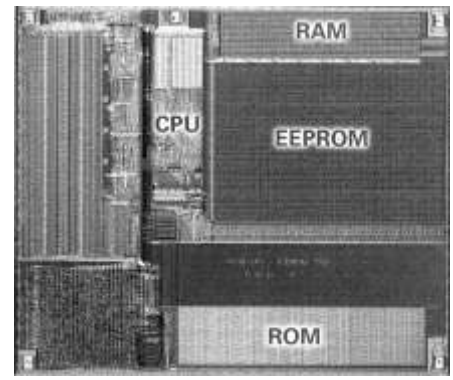
Electrical Contacts (ISO 7816-2)



Classical Microprocessor Layout

Typical Smart Card Chip Components

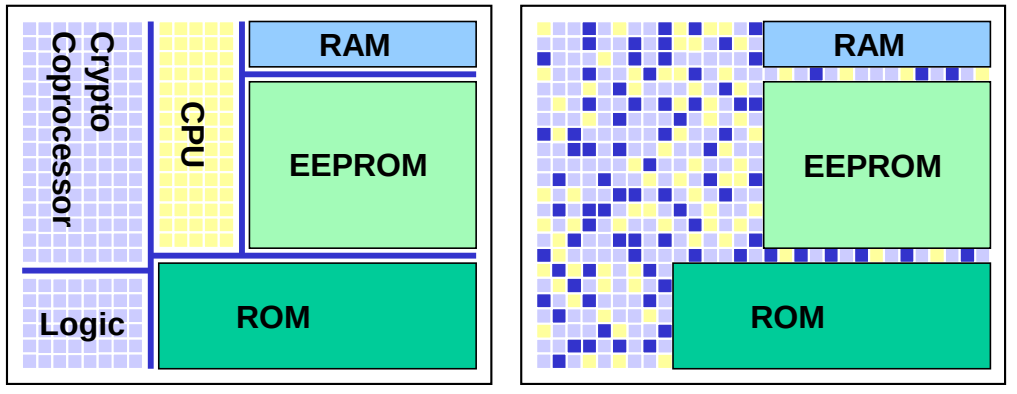
- **CPU:**
  - **8051 8 bit architecture**
  - **6805 8 bit architecture**
  - **H8 (Hitachi), 16 bit architecture**
  - **ARM 7， MIPS 32 bit**
- **RAM:**
  256 – 2048 Bytes (1 RAM cell = 4 EEPROM cells)
- **EEPROM:**
  1 – 64 kBytes (1 EEPROM cell = 4 ROM cells)
- **ROM:**
  8 – 64 kByte



Infineon

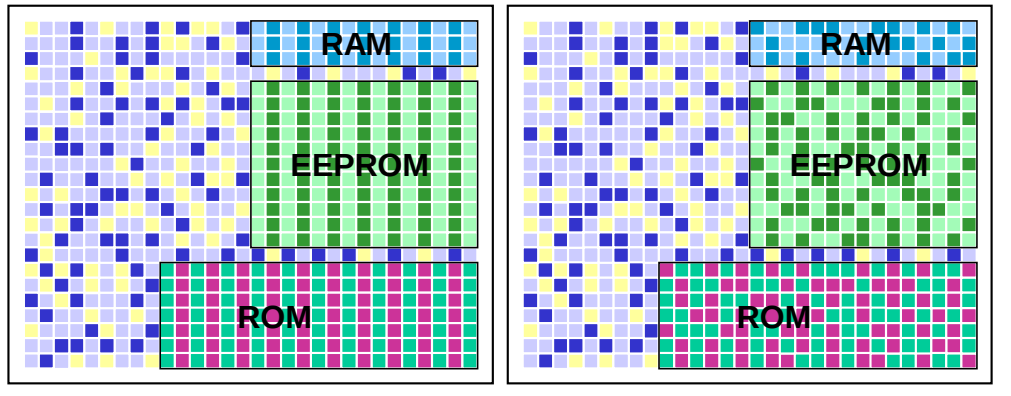
SLE 66CX160S

Block Layout



Standard cell Random cell placement

Memory Layout



Regular Structures Scrambled Addressing

EEPROM

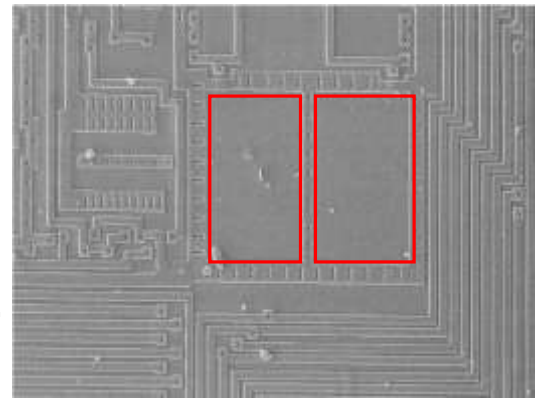
- **E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory (e.g. Flash memory)
- individual bytes in a traditional EEPROM can be independently read, erased, and re-written.
- An EPROM can't be erased electrically, must be removed from the device for erasing and programming

37

Passivation Layer Removal Detection

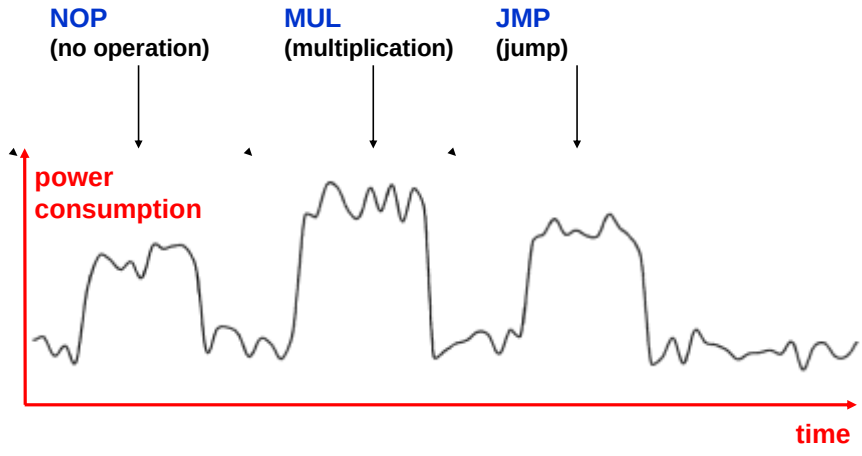
• When cooled to -60 ° C, RAM cells can keep their charge up to several weeks after the power supply has been switched off.

• The content of a RAM cell can be read out using electron-beam microscope.



the passivation and metallization layers covering the RAM structure must first be physically removed, leading to the destruction of the RAM cells.

Side channel attacks



Power and Timing Analysis

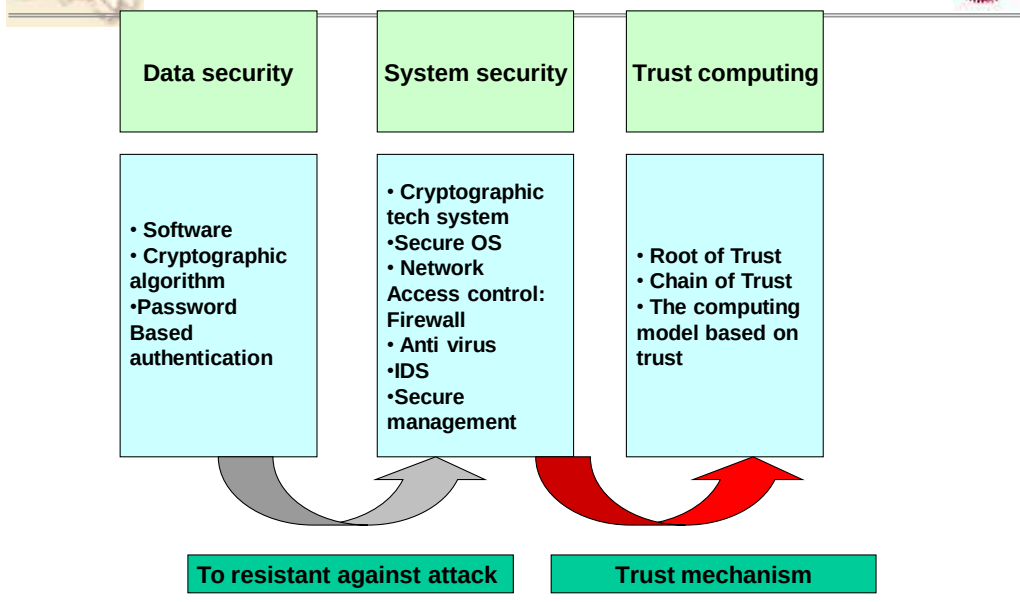
Security hardware

Smart Cards

- **Types**
- **Applications**
  - **Payment**
  - **authentication**
- **Interface**
- **Physical Security**

TCP - Trusted Computing

Information Security Technology Evolution



Understanding trusted computing

- Trusted：behave as expected

Do good + Not do evil

trusted computing
= Availability, Reliability + Security

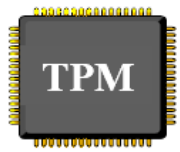
PKI: trust = binding of ID and pub-key

TCP means essentially using TPM

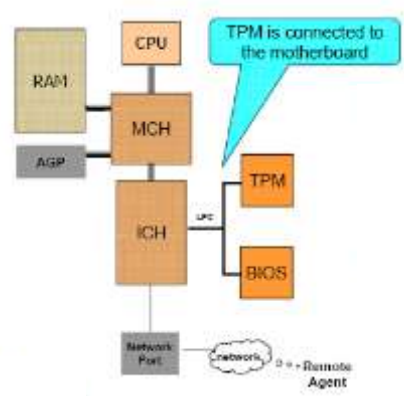
- **TCP – Trusted Computing Platform**
- **TCG - Trusted computing Group, non-profit industry standard organization**
- **TPM -- Trusted Platform Module, A chip embedded on the motherboard**

What is TPM?

- A new embedded security subsystem build into many computers



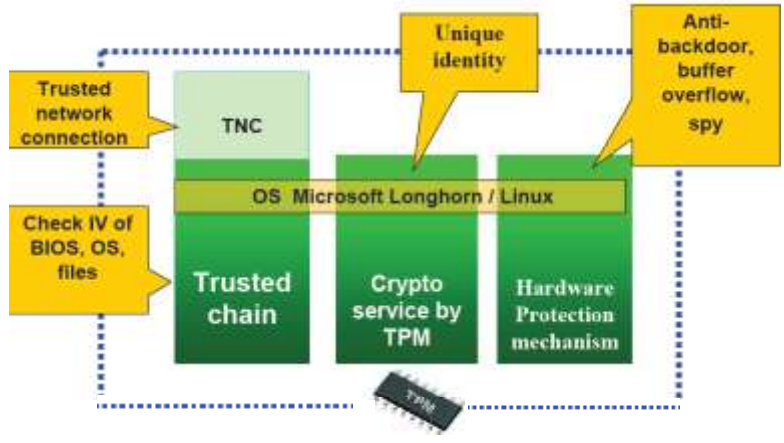
- **Protected capability**
- **Shielded locations**



Why TPM?

- **Software cannot be made completely secure**
  - **Complexity: Unix/Windows..1 bug/1000 lines of source codes…**
  - **Compatibility: How can we replace the billions of lines of code in and for existing OS?**
  - **Compromise: Any attempt to detect malicious changes in software without HW support could be circumvented.**
- **How can TPM help?**
  - **To provide an anchor in the sea of software**
    - **Private keys cannot be stolen or given away.**
    - **The addition of malicious code is always detected.**
    - **Malicious code is prevented from using the private keys.**
    - **Encryption keys are not easily available to a physical thief.**

Mission of Trusted computing



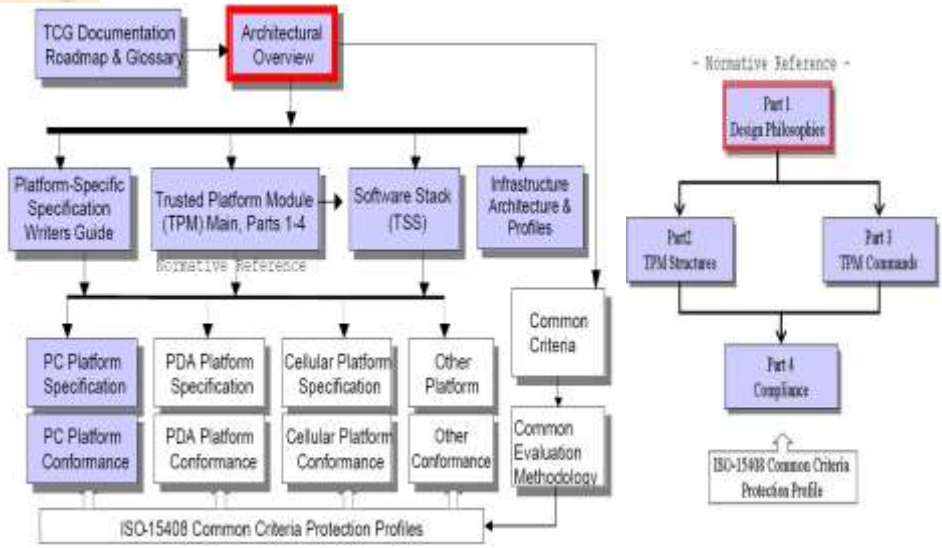
Trusted Computing Platform:

TPM + OS + Software + Network infrastructure

Trusted computing Group

- Dependable computing
- TCPA
  - 2000,CMU, NASA, …
  - Specify the construction of secure HW platform
- TCG
  - 2003
  - Non-profit industry standard organization
  - Adopt the specification of TCPA
  - Incorporate “Root of Trust”
  - Not rely on specific vender

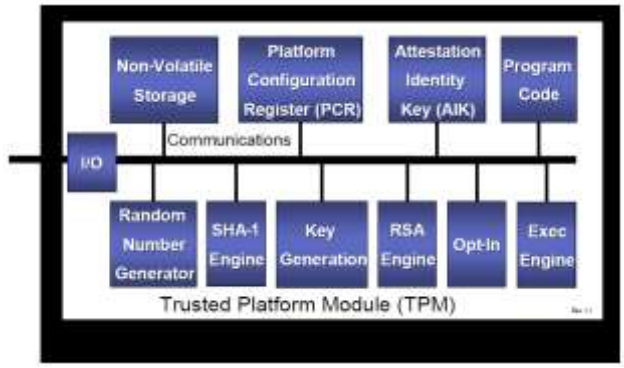
TCG Document Roadmap



Applications

TPM: Trusted Platform Module

- A chip embedded on the motherboard

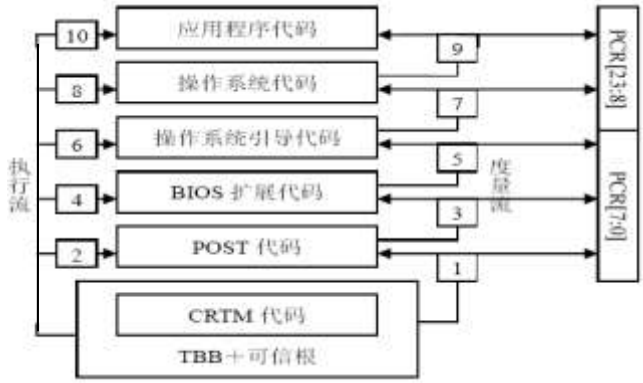


Fundamental Features of TPM

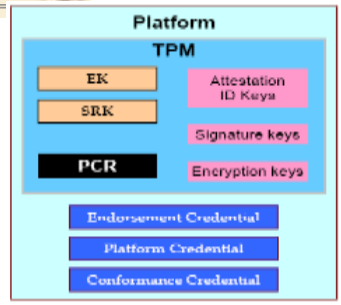
- **Protected Capability**
  - **A set of commands to access shielded locations (places to safely operate on sensitive data)**
  - **Function: to protect and report integrity measurements, store keys, key management, random number generation, sealing data…**
- **Attestation**
  - **Vouch for the accuracy of information**
  - **By the TPM / To the TPM / Of the TPM/ Authentication of the platform**
- **Integrity Measurement and Reporting**
  - **Integrity Measurement**
  - **Integrity logging**
  - **Integrity reporting**

Trust Boundary and Transitive Trust

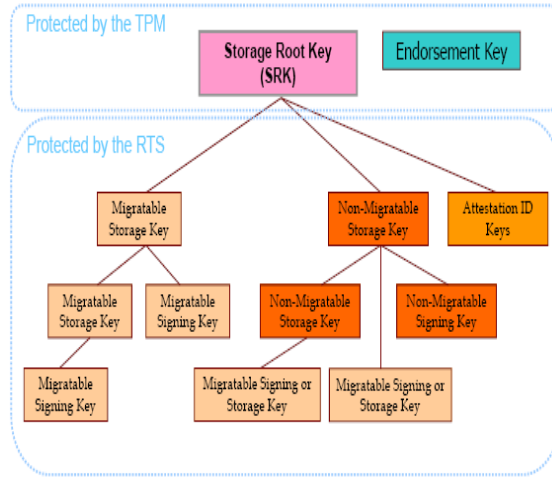
- Root of Trust: RTM RTS RTR
- Chain of Trust



TPM Persistence Key and Key Hierarchy



- Endorsement Key (EK)
  - Not part of the key hierarchy
- Storage Root Key (SRK)
  - All keys are protected by this key
    - Root of Key Hierarchy
  - Changed on new owner



Key Type - migration

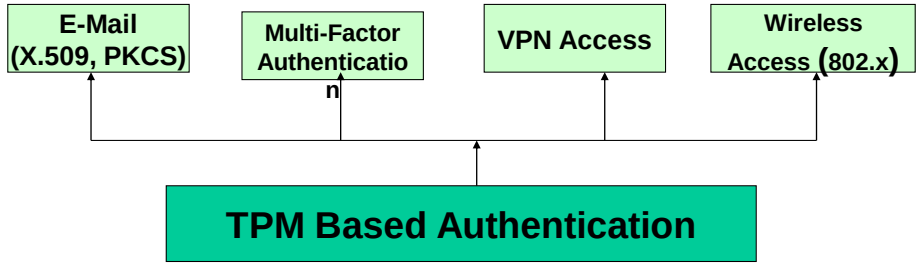
- Migratable VS. Non-Migratable
  - Migratable key
    - Usage: Key transfer, more than one system to use a key, info backup to another platform /clone or update
    - Use the parent key to unwrap the private part of a migratable key, and rewrap it with a different parent key
  - Non-migratable key
    - Usage: To identify a machine, store migratable key,…
    - Only be created by the TPM and only when the parent key is present
    - E.g. EK, SRK
  - Key is only valid on the TPM on which it was created unless migrated by the user to a new TPM

Key Types - functions

- Storage key: used to store other things (NOT symmetric key), 2048bit, RSA type, migratable or not. (not for signing)
- Binding Key: Used to store small amount of data (not for signing)
- Identity Key: AIK, non-migratable, provide two functions
  - Sign PCR as required
  - Sign other keys
- Signature key: at most 2048bit, RSA type(not for binding)
- Authentication Keys: Symmetric key used to protect transport session involving the TPM
- Legacy key: both sign and encryption, created outside the TPM

TPM Based Authentication

- **PCs shipped with a TPM chip capabilities beyond traditional tokens or smart cards.**
- **The key differentiator: TPMs uniquely support both user and machine authentication in one token**
- **Only authorized users and authorized PCs are on the network**



reality

- TCP enabled computers are not well accepted (root, 越狱，DRM）
- TCM – Chinese version of TPM (+encryption)
- Windows 8.1 banned
- Effective in protecting devices
- Trusted Handy

64

Exercise 20

1. Is it possible to clone a smartcard ?
2. What kind of properties of EEPROM are used to provide security for smartcard?
3. Describe the similarities and differences of PKCS15 and PKCS11
4. How is TPM used to provide security for computers?

Hand in your answer whenever you like

65

overview

IT-security
•Definition
•5 services
•1-way function

Key-manage

Classical Shannon

Security Un/condition

Integer factor Discrete log

Block cipher Stream cipher | **Hash MAC** | **PKC signature**

Kerberos

Cert.PKI

DDOS Intrusion Password

Malware Flame

Smartcard TCP

Firewall

wireless

IPSEC VPN

SSL TLS

PGP S/MIME

applications

66