Trusted Platform Modules and Hardware-based Security

Andreas Nilsson
Master’s Student at Nada, KTH
Pointsec Mobile Technologies
TPM Introduction

• Microcontroller affixed to the motherboard.

• Cryptographic functions like key storage and RSA encryption.

• Basic idea is to make computing platforms more secure. Has received bad publicity for “depriving” the user of platform control.
Use cases

• Secure storage – Hardware based storage of sensitive information like keys.

• Secure communication – Network of trusted entities.

• Digital Rights Management (DRM) - Copy control of media files only under certain conditions.

• Software vendors can block application instances known to be copies.
Trusted Computing (TC)

- Set of hardware and software components ensuring a platform’s behaviour.

- TPM core hardware component.

- No "real" current customer demand for TPMs → cheap

- The TPM is platform agnostic
Trusted Computing Group (TCG)


- Founding members include HP, IBM, Intel and Microsoft, today 100+

- Driving force possibly DRM.

- The goal is to specify TC standards.
Public Key Cryptography

- Symmetric encryption and key distribution
- Asymmetric encryption - private and public keys.
- RSA:
  - public key (n,e), private key d
  - message m, ciphertext c

\[ c = m^e \mod n \]
\[ e = c^d \mod n \]
Public Key Cryptography

• RSA not used for bulk encryption.

• Wrap symmetric key with RSA key.

• RSA-wrapping of other RSA-keys gives key storage structures.

• Digital Signatures
Hash functions

• Representation of a message with a hash-value of predefined length called a digest.

• Design requirements, collision free one-way functions.

• SHA-1 most widely used, developed by NSA.

• Hash functions are often used to "convert" passwords to predefined length.
HMAC

• Stands for keyed Hash Message Authentication Code.

• Compute a digest of a message using a secret key.

\[ \text{HMAC}_K(m) = h(K \otimes \text{opad} || h(K \otimes \text{ipad} || m)) \]

with key K, message m and hash function h. Opad and ipad are just padding parameters.
TPM Components

Cryptographic Functionality

- RSA Encryption
- SHA-1 Engine
- HMAC Engine
- RSA Key Generation
- Random Number Generator
Cryptographic Functionality

- **RSA encryption** – Hardware implementation of encrypt/decrypt. Central function.

- **SHA1 Engine** – Used primarily by the TPM internally. The TPM is not a cryptographic accelerator (no through-put requirements).

- **HMAC Engine** – SHA1 underlying hash function. Same usage principle as SHA1, only resource limited entities should use the TPM implementation directly.
Cryptographic Functionality

- **Random Number Generator (RNG)** – Hardware based random numbers for nonces, and symmetric and assymetric key generation.

- **RSA key generation** – Generation of RSA keys using the RNG.
TPM Components

Other Components

- Volatile memory
- Non-volatile memory
- Monotonic Counter
- Power Detection
- Execution Engine
- Opt-in
The Life of a TPM

1. Manufacturing – Creation of unique Endorsement Key Pair (EK).

2. Platform user takes ownership.
   Identification through shared secret.
   Storage Root Key (SRK) is created.

3. The TPM is used by the platform user, creating for instance so called AIKs.

4. The platform user forgets the owner password, has to retake ownership and loses all stored data.
Programming Interfaces

Windows Support:

- MS-CAPI through TPM CSP.
- PKCS#11, platform independent
- TCG Software Stack (TSS). The only interface compulsory to ship according to the TCG specifications.
Programming Interfaces

- TSS parts in decreasing abstraction level:
  - TSS Service Provider (TSP), dll in Windows. Access point for normal applications.
  - TSS Core Service (TCS), Windows NT Service
  - TCG Device Driver Library (TDDL)

Pre-boot Support:
- BIOS INT 1Ah interrupt interface
Memory Structure

Non-Volatile (persistent) Memory:
- Endorsement Key (EK)
- Storage Root Key (SRK)
- Attestation Identity Keys (AIK)
- Owner shared secret
- Opaque owner data

Volatile Memory:
- RSA key slots
- PCR registers
- Key handles
- Session handles
Protected Storage

- Very limited on-chip storage.
- RSA-wrapping with SRK as root key.
- Storage hierarchy tree:
Access Control

- Shared secrets controls access to entities and certain operations
  - 20 bytes long
  - called AuthData in TCG specifications
  - Typically hash from password

- Owner authorization required to
  - Temporary disable or deactivate the TPM.
  - Read/Write in the NV Memory Area.
  - Change the shared secret for the SRK.
Access Control

- Authorization sessions
  - Rolling nonce (**Number used ONCE**) procedure
  - $\text{HMAC}(\text{params})$ digest = $\text{HMAC}_{\text{AuthData}}(\text{params} \ || \ \text{nonce})$

- Transport encryption – Wrapping of commands containing sensitive information.

\[
\begin{align*}
\text{User} & \quad \text{TPM} \\
\text{inparams} & \quad \text{HMAC(inparams)} \\
\text{Check HMAC digest} & \quad \text{Check HMAC digest} \\
\text{TPM} & \quad \text{outparams} \\
\text{HMAC(outparams)} & 
\end{align*}
\]
Security Problems?

Software attacks:
- SHA1 collision vulnerability
- Dictionary attacks, some form of mitigation required.

Hardware attacks:
- Vulnerable to sophisticated physical attacks due to cost reasons.
Use case – Disc encryption

- User key storage structure

![Diagram showing the relationship between User Keys (UK_i) and Disc encryption Key (DK) under SRK.]

- User Key i
- Disc encryption Key
Use case – Disc encryption

• SRK authorization problem, possible cause DRM background

• Windows Vista Solution: Suppose SRK shared secret is a predefined dummy-value i.e.
  $AuthData_{SRK} \equiv 0x0$

• User keys protected with their own $AuthData$
Smartcard Comparison

- Creditcard-shaped plastic card used to store authentication data.
- TPM affixed to motherboard, Smartcards removable tokens $\rightarrow$ different user mapping.
Smartcard Comparison

- Mobility of the smartcard is an extra security measure. Though easy to lose a portable card.
- Smartcards store all RSA keys on the card. The protected storage structure of the TPM does not.
- TPM has machine binding of i.e. keys using the PCR registers.
Tamper Protection

• Smartcards and TPMs are both vulnerable to so-called non-invasive attacks (i.e. power analysis and timing attacks).

• Smartcards and probably also TPMs are vulnerable to invasive attacks like micro probing.

• Smartcard danger: Physical attacks using "fake" smartcard reader giving no tamper evidence.
Power Analysis of DES
Integrity Protection

• Trusted networks based on TPM:

• Platform integrity through TPM self-authentication together with Root of Trust.

• Unique identity (EK) needed to avoid BORE-attacks.
Integrity Protection

• Attestation Identity Keys (AIK)
  – RSA key pair
  – Aliases for the Endorsement Key (EK)
  – Mapping kept at "trusted third party", normally a Certificate Authority (CA)
  – Trusting the trusted third party?
Integrity Protection

Direct Anonymous Attestation (DAA)

– TPM 1.2 feature after AIK integrity issue.
– Verify a signature without revealing the signer.
– Identify groups of TPMs together. Track individual TPM if a DAA key is repeatedly.
– Based on zero-proof techniques
Tech Outlook

• Current version is 1.2. TPM 1.1 was criticised for lack of security measures and integrity protection.

• Around 5 different vendors manufacture TPM 1.2 microcontrollers.

• Future inclusion of the TPM into the CPU to avoid unnecessary communication over insecure busses.
Usage Outlook

• No current use in major PC applications. Apple uses the TPM to prevent OS X from running on PCs. Cracked in a week.

• Windows Vista, scheduled for the fall 2006 demands a TPM 1.2 installed.

• TPM Linux Driver and TSS implementation exists.
Usage Outlook

• DRM money will probably drive the usage forward forcing customers to accept the technology.

• TPM more likely to be used in enterprise environments than by private customers.

• The next platform is mobile devices. Ericsson has an optional DRM package right now which is not based on the TPM.
Popular Myths

• The TPM will not allow open source software to run.

• TPM Data protection is perfect.

• TC is required to combat computer threats.

• The TPM enhances user authentication.
Questions & Discussion