Exercise 1: Introduction to Trusted Computing & TPM

1 Introduction

The trusted computing model and technology was proposed by the Trusted Computing Group (TCG)[1] in 2003. Its core component is the Trusted Platform Module (TPM) which is a security microchip mounted on the motherboard of recently developed PCs. The current implementation is in fact a cryptographic co-processor providing hardware-based random number generation and a small set of cryptographic functions (key generation, signing, encryption, hashing, MAC). Additionally, the TPM offers secure[1] storage and platform integrity management and reporting using the Platform Configuration Registers (PCRs), remote attestation, cryptographic binding and sealing.

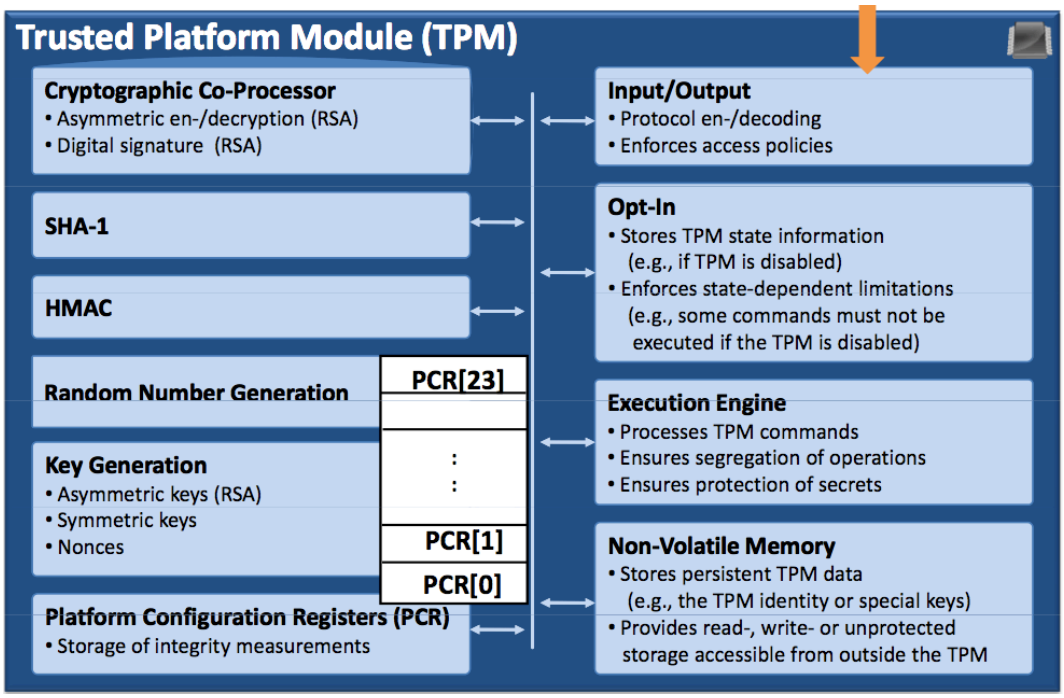

Figure 1: TPM architecture

The architecture of the TPM is shown in figure 1. The TPM acts as a "Root of Trust" for the platform and must be trusted by all parties to behave correctly and not being compromised. For a more detailed view on the TPM see the slides on the lecture "Trusted Computing" [2] or the TCG Specification[3].

[1] meaning: ideally tamper-resistant

1.1 TPM Manager

The TPM Manager[4] is a tool with a graphical interface to manage the TPM, e.g. showing the capabilites of the TPM, reading data from it such as PCR values or changing the settings of the TPM.

1.2 TrouSerS

TrouSerS[5] is an implementation of a trusted software stack (TSS) as defined by the Trusted Computing Group. Application and system developers can use it to access all of the functions of the TPM through a well-defined application programming interface (API). TrouSerS runs a deamon `tcsd` to manage TPM requests from different applications. You will learn more about TrouSerS in exercise 2.

2 Theoretical Assignments (7 Points)

This part of the assignment should be prepared at home. In the exercise lesson you are just going to discuss some issues related to the possible answers of the questions.

1. The Trusted Computing Group defines a system as trusted "[...] if it always behaves in the expected manner for the intended purpose". Another definition states that a trusted system is a "system or component whose failure can break the security policy (Trusted Computing Base)".
   Discuss the difference between these two approaches!

2. Have a look at the system shown in Figure 2. Identify the trusted computing base (TCB) in this system and justify your answer!

3. Today's modern operating systems have a very large and complex trusted computing base. Explain why this is not a good idea! What could be the consequences?

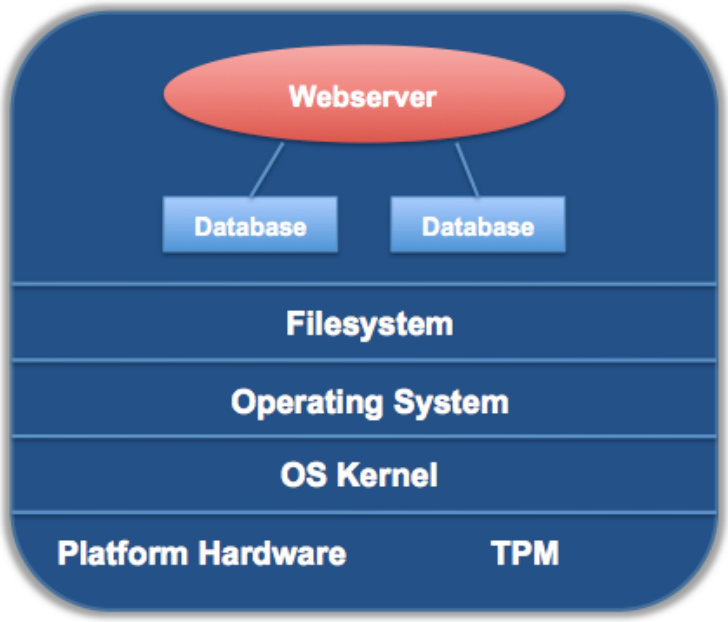

Figure 2: Architecture of an example system

4. Taking the steps towards trustworthy computing, 5 desired primitives were introduced in the lecture. One of them is a metric for code configuration. Explain the need for this metric and justify your answer! Give an example how it could be used to protect a system!

5. The Root of Trust for Measurement (RTM) is the root of the chain of trust. How can trust can be enforced in the RTM?

3 Practical Assignments

This part of the assignment should be done in the Lab for Operating System Security and Trusted Computing. For the exact terms for each exercise check the Course-Website or ask your tutor.

3.1 Assignments for Windows Vista (7 Points)

3.1.1 Enabling and Activating the TPM from BIOS (1 Point)

As the TPM is Opt-in[2] it is disabled by default. To use the Trusted Platform Module, it should be enabled and activated first.

1. Start the PC and press F2 to enter the BIOS.
2. In the "Security" tab you will find both "TPM Security" and the "TPM Activation" setting. Enable and activate the TPM!
3. The BIOS also allows you to clear the TPM. Should access to the BIOS be password-protected? Justify your answer!

3.1.2 Initializing and Taking Ownership (4 Points)

1. After you enabled and activated the TPM you would want to initialize it. Boot into Windows Vista and run Microsoft's TPM Manager by starting `tpm.msc`.
2. Use the TPM Manager to initialize the TPM! What does the initialization of the TPM exactly do?
3. Create the password asked for by the TPM Manager and save it to disk. Why the password should be stored on an external hard or flash drive and not on the platform?

[2] the TPM is disabled by default, using it is not mandatory

4. What is the name of this specific password and what is it used for in the Trusted Computing Model?

5. Try to open the password file using a text editor. Which information can you find inside?

3.1.3 Clearing the TPM (2 Points)

Suppose that you want to sell your computer, because you just bought a new model with double the speed. Of course, you first want to erase all personal data on the hard drive.

1. Should you also clear the TPM? Justify and discuss your answer!

2. Clear the TPM using the TPM Manager!

3. What happens during clearing of the TPM?

3.2 Assignments for Linux (6 Points)

3.2.1 Initializing the TPM (1 Point)

1. To manage the TPM using the TPM Manager software, you should start "TrouSerS"[5] and the TPM Manager[4].

2. What is the role of "TrouSerS" in the trusted computing model? Draw a picture showing the roles of TrouSerS, the TPM and the TPM Manager.

3. The TrouSerS daemon (`tcsd`) should already be running in the background. Verify this! (Hint: use the command `ps ax | grep tcsd`)
4. Initialize the TPM using the TPM Manager!

3.2.2 Taking Ownership (1 Point)

After initializing the TPM you now should also Take Ownership to use all features of the TPM.

1. Take ownership of the TPM using the TPM Manager. When asked, set "SRK" to "WELL_KNOWN_PASSWORD".
2. Use the password "tpmtest" when asked. What is the name of this specific password and what is it used for in the trusted computing model?

3.2.3 Reading the Contents of Platform Configuration Registers (PCR) (2 Points)

Authenticated boot is one of the main features of trusted computing as defined by the TCG. The TPM acts as a root of trust for the bootstrapping process. The boot components establish a chain of trust, where each component being executed is measured by it's predecessor before passing control to it and the measurement value extended into one of the 24 PCRs[3]. Measurement is done computing a 160 bit SHA-1 hash of the binary. The extend function ensures that registers cannot be overwritten by including the old PCR value in the new measurement value being written into the register.

1. Read the contents of the PCR registers:
   - Using the TPM Manager: Info → PCRs
   - From the terminal: `cat /sys/class/misc/tpm0/device/pcrs`
2. In case the chain of trust for measurement is extended into the operating system, so the bootloader will measure the OS kernel before passing control to it, PCR values should differ if two different operating systems are booted using the same platform. Boot two machines running different operating systems and compare the PCR values!

[3] TPM's of version 1.1 only had 16 PCRs, since TPM v1.2, 24 PCRs are mandatory

3.2.4 Using TPM Tools (2 Points)

The TPM Tools allow you to send commands to the TPM from the terminal.

1. Execute the command `tpm_clear` (resets the TPM to factory defaults). Afterwards, activate and enable the TPM again from the BIOS as in task 2.1.1)!
2. Execute the command `tpm_takeownership` (takes ownership of the TPM).
3. What is the difference between the "Owner password" and the "SRK password"?
4. Execute the command `tpm_getpubek` (returns the public endorsement key from the TPM).
5. What is the "Endorsement Key" (EK) and what is it's purpose?

References

[1] Official Website of Trusted Computing Group, https://www.trustedcomputinggroup.org/

[2] Official Website of Lecture "Trusted Computing", http://www.ei.rub.de/studierende/lehrveranstaltungen/231/

[3] Trusted Computing Group Specification, https://www.trustedcomputinggroup.org/specs/

[4] TPM Manager, http://www.sirrix.de/content/pages/51317.htm, http://sourceforge.net/projects/tpmmanager

[5] TrouSerS Project Page, http://trousers.sourceforge.net/