QUIZ TPM1.2 Preparation instructions

General

As with all the quizzes in this course you have to answer 7 out 10 questions in order to pass the test. When preparing yourself read the slide sets Lect 1 and Lect2 dealing with TPM1.2 and the material

- http://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2014/er-trusted-computing.pdf
- TPM main specification for TPM ver 1.2, Part 3, commands

The latter document you need only to glance through and study a number of commands. It will useful for quiz and the TPM project.

There are a lot of (new) terms so it is good that you read through the slides so you know where in the lecture slides things can be found. Below we walk through the different parts of Lectures 1 and 2. In particular, you find items and questions that are useful to study. A good trick is to go through these items and questions with a colleague and ask him/her for explanations and check each other's answers.

TCG goals and impact:

What are the functions the TCG RoT should provide?

How is the TPM integrated in a traditional PC/Server system?

What components in a traditional PC system are at least affected by adding TPM support?

TPM Internal

How many PCR registers does a TPM at least have?

How many PCR registers is Intel TXT using in a TPM?

What is the purpose of the OPT-IN function of a TPM?

Why do we need a GUI in the Bios when adding TPM support?

What is meant by physical presence?

Where (in a system) is the physical presence enforced?

What are the monotonic counters in a TPM and explain one use case of them?

What is meant by a PCR and extending a PCR ?

Why is resetting of PCRs restricted?

Why is it not possible to set a PCR to a user provided value?

The TPM exists in different versions. Which ones?

TPM in a system

What is a platform certificate and what is its role?

What is a TPM certificate and what is its role?

What is an endorsement credential?

Who issues a TPM certificate?

Who issues a Platform certificate?

What part of EK is stored in the endorsement credential?

Explain the trust chain, Lect1/slide 43.

Roots of trust and their use

See also http://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2014/er-trusted-computing.pdf

What is the CRTM, the SRTM and the DRTM?

Explain the secure boot use of a RoT Lect1/slide 48 and 49

What is UEFI secure boot?

Is the TPM needed in UEFI boot?

What is ACM in the context of Intel TXT.

Intel TXT mitigation of reset attacks.

What is meant by a locality and what are localities used for?

Explain how localities and PCRs are linked.

TPM keys and TPM commands

Look through TPM main specification for TPM ver 1.2, Part 3, commands

> Study the commands: TPM_TakeOwership, TPM_Unbind, TPM_Seal, TPM_Quote, TPM_LoadKey2, TPM_Init. Not needed you understand all the fields but study the pseudo code following in the description of the commands. This code explains the behavior in more detail than the text.

What is a legacy key?

What is a binding key?

Who is doing the binding operation, the TPM or some other entity?

What is (TPM) ownership?

Which keys do always stay in a TPM (version 1.2)?

Explain the role of EK and SRK?

If we have a key hierarchy and then take ownership, can we still use the keys in that hierarchy? Explain!

Why is EK privacy sensitive?

Why is SRK not (or at least less) privacy sensitive? Think what happens when we takeownership.

What happened during Takeownership?

What is the function of the passwords and secrets associated with the keys.

Where do we store the non-permanent TPM keys?

What is a migratable key ?

Which TPM keys we have in a TPM version 1.2? Explain.

Can we have an AIK stored under a migratable storage key?

If we have a TPM key blob why then do I have to remember also all keys that were used in the process of creating this key even if these keys are not used for any application?

When loading a key into the TPM why do we have to know the parent secret/password?

Explain the key hierarchy Lect2: slides 3 and 4

What is sealing? Can you seal data to a TPM from outside the TPM (using the public portion of the seal key)?