QUIZ Trusted Computing & ID 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.

This quiz covers the lectures 4, 6, 7, and 8, excluding the TPM material in Lecture 4. Be sure that you have read and understood the course slides and have read the mandatory literature. From the EPID material you do not have to understand the mathematical details. There is additional material on the course webpage under the section Trusted computing on the "Literature" page. 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 the lectures. 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.

Mandatory reading

- Mobile Trusted Computing, Ansokan et all
- SGX: Innovative Instructions and Software Model for Isolated Execution
- Enhanced Privacy ID (EPID), DrDobbs, E Brickell, 2009

Trusted Computing:

What is TEE and REE. Why is a TEE usually smaller than a REE?

Trusted execution in a TEE is obtained by two crucial capabilities/functions?

What is TCB and what are the two important components of a TCB of a mobile?

What is the role of the TCB?

To build a secure storage solution one needs at least in a mobile to have what ? (think security here)

What is a root of trust of integrity? (as compared to RTM, RTS and RTR)

What is provisioning?

Understand difference between trusted and trustworthy.

Understand when a system is trusted and when it is trustworthy.
See above. “Trusted” can be just an assumption

EITN50-Quiz 4 Trusted Computing & ID preparation instructions

Ben Smeets, 2017-10-03

Recall from compute security course Common Criteria and EAL levels.

Arguments pro's and con's using hardware of only software for trusted computing.

What is trust chain for trusted computing when applied to a server with hardware and services?

What is RTM, RTS, and RTR?

Secure boot using RTS and RTM, explain the roles of RTS and RTM

Which RoTs are in the TPM? Do we need TPM for secure boot?

What is UEFI boot (ignore use of TPM)?

Primary objective of OS in trusted platform is to create isolation. Explain role of MMU and why this solution is effective in keeping user applications apart. Understand the importance of privileged (super user) mode and Non-privileged (user) mode.

Isolation by abstraction: virtualization and (later) containers.

By able to describe differences between the execution environment alternative on Slide19/Lect5.

Virtualization: what is type 1 and type 2 virtualization. What is Full/pure and impure/para virtualization?

Java

Java as example of trusted execution environment. Evolution of the sandbox model. Role of signed software.

Role of components to java security on Slide 30, 40/Lect8.

What is STIP?

SELinux

MAC added to Linux DAC (recall MAC and DAC from you basic computer security course). Understand this via Slide 61/Lect8. Understand what this means for the access control to, for example, a file where we give permissions via the Linux DAC system and also have the MAC policies in place.

What is the purpose of a SELinux policy?

What are the differences between the three reference policies? Slide 67/lect8

What happens when SELinux is operating in permissive or in enforcing mode?

What is MLS? Example of MLS in basic computer security book.

Why has SELinux problems with Text Relocation?

ARM TrustZone

ARM Architecture: modes Privileged (super user) and non-Privileged (user).

EITN50-Quiz 4 Trusted Computing & ID preparation
instructions   Ben Smeets, 2017-10-03

Role of NS bit and which parts of the HW carry the NS bit. What is the role of the monitor? A secure mode process can access normal world objects if it has the same or higher privilege. A normal world process can never get access to any object marked as belonging to the secure world.

What is the benefit from the NX bit?

HSM

What is an HSM. See Link to SANS: An Overview of Hardware Security Modules in literature list.

What is PKCS#11?

How can people trust a HSM product?

Smartcard

How can you interact with the functions in a smartcard: APDUs. Command and response APDUs. When does the card itself send data, which is not as a result of command. The smartcard is essentially a server. Existence of the T=0 protocol and T=1 protocol. What is T=1 especially designed for? You do not have to know the details by heart of these protocols. Such will be given if needed.

What is the role of the NPU unit on a smartcard?

Slide 50/Lect7: Purpose of the sensor and filters are for defense. Give three types of defensive mechanisms? Why is over and under voltage a condition that should cause the smartcard to shutdown?

What is the purpose of the personalization stage in a cards lifecycle?

What is the message passing model in a Java card?

How can we attack a card? Describe at least two types of attacks.

What is DPA?

What caused that DPA succeeded in finding the secret RSA key? How can that be remedied?

Distinction between RFID and NFC?

Mifare and Felica: what are these?

Why is crypto considered to be problematic for contactless cards? Think here about power and allowed time to interact with the reading device.

How does the Hopper-Blum scheme work and why is it secure?

Why is the blinding vector needed on slide 108/ Lect7

What is the importance of the presence of noise problem for the Hopper-Blum scheme?

What is SGX?

EITN50-Quiz 4 Trusted Computing & ID preparation instructions

Ben Smeets, 2017-10-03

What is an enclave and what protection one has for data and code in an enclave?

Is SGX a pure SW solution?

Is SGX also using a TPM?

Where is the key stored for encrypting the enclave code and data.

Can the kernel of an OS read data from an enclave?

How is the enclave created (see the Innovative Instructions and Software Model for Isolated Execution, watch the SGX video on youtube)

Life-cycle of an enclave. Slides 17,18/Lect6

EPID identity role in remote attestation

Identities

Identity as a link

Identifiers

Role of credential.

What are PUFs and what can they used for?

Zero-knowledge proof: what is the basic idea of it and why is it useful in connection with identities.

EPID, what is it?

EPID: Roles of issuer, member and verifier, who gets what (think keys, revocation lists)

EPID: Unlikability of private keys.

EPID: Join operation

EPID: Revocation lists

Android and iOS

Explain difference in the use of signatures on applications.

Explain DM-verity.

How is the root hash value protected in DM-verity?

How are apps isolated in Android? Slide 101-107/Lect8

How are apps isolated in iOS? Slide 129/Lect8

What is BYOD?

Why is isolation important in BYOD?