QUIZ 3 Preparation instructions

General

As with all the quizzes in this course you have to answer 8 out 10 questions in order to pass the test.

When preparing yourselve read the slide sets Lect 5 and Lect 6 . 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 5 and 6. 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.

Trusted Computing:

Difference between trusting computing aspects relating to the programs and relating to the execution environment for the programs.

Open platforms vs Closed platforms. Advantages of each approach. Trusted computing as way to get benefits from both approaches.

Understand difference between trusted and trustworthy.

Understand when a system is trusted and when it is trustworthy.

Recall from compute security course Common Criteria and EAL levels.

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

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

Roots of trust, read also NIST paper on Hardware Rooted security pages 9-13, in Literature list.

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.

What is the role of the TCB? Does the TCB contain roots of trust?

Isolation by abstraction: virtualization and (later) containers.

By able to describe differences between the execution environment alternative on Slide26/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 38/Lect5.

What is STIP?

SELinux

MAC added to Linux DAC (recall MAC and DAC from you basic computer security course). Understand this via Slide 76/Lect5. 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 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 ?

Linux Containers what is this? read article on Security Analysis of Dockers: http://arxiv.org/pdf/1501.02967.pdf in the Literature list, Sections 3 and 4.

ARM TrustZone

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

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 does can you interact with the functions in a smartcard: APDUs. Command and response APDUs. When does the card itself send data, that 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 63/Lect6: 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 to types of attack.

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 is it?

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

Below is 2015 moved to other quiz

How does the Hopper-Blum scheme work and why is it secure? What is learning in the presence of noise?