QUIZ 5 Preparation instructions

General

For this quiz 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 9 through 12 and the following articles

- Mobile TC: http://www.eit.lth.se/fileadmin/eit/courses/eitn50/Literature/mobilecompsecurity.pdf
- Secure VM launch: http://soda.swedishict.se/5467/3/protocol.pdf
- SGX: http://www.eit.lth.se/fileadmin/eit/courses/eitn50/Literature/hasp-2013-innovative-instructions-and-software-model-for-isolated-execution.pdf

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 Lect 9 through 12. 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.

TEE:

What is a TEE? The concept of TEE for protection of sensitive applications and the secure invocation of these services as shown in slide 2/Lect9.

Two techniques to realize a TEE. Read also the Mobile TC paper.

SGX

Is SGX also using a TPM?

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

How is an enclave initialized ? Read SGX paper.

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 45-48/Lect9

How are apps isolated in iOS? Slide 73/Lect9

Cloud

What is SaaS, PaaS, IaaS?

What means multiple tenancy?

List 3 risks with Cloud computing?

Transparency issues for tenants with cloud computing?

Secure Virtual Machine launch Slide 20/Lect 10- See also paper Secure VM launch

Understand process in Slide 20/Lect10 of using bind keys and role of TTP.

Software security – code protection

What is obfuscation?

What is the purpose of dongle? Slide 10/Lect12

SW protection by making the program into a service. Slide 17/Lect12

Software security – code design

What is an attack tree?

What does least privilege mean?

Describe 4 ways/secure practices to secure code: Slide 29/Lect12?

What aspects are considered in a threat model?

Software security – code analysis and processes

What is static code analysis?

What is dynamic code analysis?

What does taint analysis work? Slide 59/Lect12

Homomorphic encryption

Understand difference between fully and somewhat fully homomorphic encryption

Additive and Multiplicative homomorphic encryption. Can you give examples?

Role of randomization in homomorphic encryption. Slide 20/Lect11

Explain how RSA based homomorphic encryption

GM homomorphic encryption understand how it works: encrypt and decrypt

Paillier homomorphic encryption: understand why it is additive homomorphic. Slide 22/Lect11

Legendre symbol, square root and non-square root mod p, p=prime