QUIZ Cloud, Homomorphic, DRM, SW SEC 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 is the last area quiz and it covers varies topics. In particular:

- Cloud computing
- Secure launch and migration of virtual machines
- Homomorphic encryption
- DRM
- SW security

When preparing yourself read the slide sets Lect 9 and 10. 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 these 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

- Secure VM launch: http://soda.swedishict.se/5467/3/protocol.pdf
- First 44 minutes of video Rustan Leino, Microsoft Research - Program Verification: Yesterday, Today, Tomorrow

Cloud

What is SaaS, PaaS, IaaS?

What is OpenStack?

What are Trusted compute pools in Openstack?

What means multiple tenancy?

What is keystone and Nova in OpenStack?

Difference between public and private cloud.

List 3 risks with Cloud computing?

Transparency issues for tenants with cloud computing?

Secure Virtual Machine launch Slide 67/Lect 9- See also paper Secure VM launch

EITN50-Quiz 5 Cloud, Homomorphic, SW SEC preparation instructions

Ben Smeets, 2017-10-13

Understand process in Slide 67/Lect 9 of using bind keys, role of TTP, and TPM.

DRM

What is and the purpose of a protected media path?

Cooperative use of technical protection solutions and legal frameworks to achieve content protection: reason behind this setup.

Use and limitations of watermarking and tracing traitors.

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 14/Lect9

Explain how RSA based homomorphic encryption works

GM homomorphic encryption: understand how it works: encrypt and decrypt

Paillier homomorphic encryption: understand why it is additive homomorphic. Slides 25/Lect9

Legendre symbol, square root and non-square root mod p=prime. What happens if we consider mod n, n product of two primes.

Use of homomorphic encryption in cloud computing.

Practicality of homomorphic encryption.

Software security – code protection

What is the purpose of dongles? Slide 25/Lect10

SW protection by making the program into a service. Slide 32/Lect10

What is obfuscation?

Techniques for obfuscation.

Theoretical result on obfuscation:

Software security – code design

EITN50-Quiz 5 Cloud, Homomorphic, SW SEC preparation instructions

Ben Smeets, 2017-10-13

What is an attack tree?

What does least privilege mean?

Describe 4 ways/secure practices to secure code: Slide 44/Lect10?

What aspects are considered in a threat model?

Software security – code analysis and processes

What is static code analysis?

What is dynamic code analysis?

Soundness and precision in

How does taint analysis work? Slide 75/Lect10

What is fuzz testing?

What is ROP exploit (see exploit project and slide 5,6/Lect10)?