QUIZ 2 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 yourself read the slide sets Lect2, Lect 3 and Lect 4 and

- Paper on LTE: Security in the Evolved Packet System, R. Blom, et al. Ericsson Review, Oct 2010, http://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2010/security_eps.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 Lectures 3 and 4. 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.

Crypto:

Recall how RSA and Diffie-Helman (DH) work. RSA can be faster than elliptic curve variant. Note the bit size in the tables for getting RSA and ECC of equal strength. Why is RSA with public key much faster than with RSA cloud and private key? The computational complexity of RSA: a^e mode N can be described as

$O(n^2)$ (#one bits in exponent e)

where n is the number of bits of the number N. Recall that DH uses the same type of arithmetic as RSA.

In which cases is ECC better than RSA?

In a DH protocol how small can you make the exponents? Why does this differ from the situation where we use RSA for a key agreement (such as in slide 54/Lect3)

Key handling:

What is OoB? Which types of keys?

Simmons' Bound. Key entropy loss as result of protection.

Crypto and Quantum computing:

How is key size affected for symmetric crypto algorithms? What happens with public-key crypto algorithms?

Authentication:

What does AAA stand for?

What is a challenge-response scheme and what is it used for.

What can be used for authentication? What is two or three and multi factor authentication?

What is CHAP and how does it work?

Radius: how do the two alternatives work? Where is the key stored used during the authentication? Compare here the two alternatives. What could the motives to use alternative 2?

What is Diameter?

What is EAP and what is its purpose?

What is EAP-AKA?

Explain how EAP-AKA can be used to give seamless WiFi network access (no need for entering WiFi network password).

Explain token types.

Kerberos scenarios. Understand how they work (no need to memorize how they work)

Recall how authentication works in GSM, slide 6/Lect4. Role of A3.

What is GBA and what is it used for? Understand the diagram of the GBA solution

Secure Connections:

Explain why we use session keys? In a secure transport protocol what are the roles of the subprotocols on Slide 52/Lect3?

Consider difference of RSA and DH based key agreement. Difference in performance. How hard has NSA to work to get at the agreed key in either scheme?

IPsec: what protection do the AH and ESP protocols give you? What is tunnel and what is transport mode. See also for example your computer security book.

Can we do manual key insertion in IPsec? What is IKE? Which key agreement is that core of IKEv2? Why do we use certificates in the Main mode?

What are the problems with IPsec and NAT. Which IPsec (sub)protocol is blocked by NAT? Explain why?

Use of UDP to get IPsec ESP through NAT device, how? Two problems with NAT-T

What is opportunistic encryption?

What is object encryption and when it is a good choice to use it?

GSM authentication (understand how it works, where are they keys) and the 8 encryption algorithms

What is a false base station attack and why is it possible.

Understand principle of 3G authentication and why it helps against false base station attacks. Why we XOR the AK to the sequence number SQN? What is the role of this sequence number?

Explain trust relations in the LTE architecture show in Slide12/lect4. Explain what is backward and forward security and which threats these solutions provide a counter measure for? X2 and S1 handover:

what is the difference with respect to forward/backward security? What is key derivation and what is a key derivation function.

Why do we have so many keys in the LTE key hierarchy, Slide15/Lect4?

IoT: For small IoT devices what is more critical energy spent on processing or on transmission? What is the consequence of this?

Botnet:

What is botnet and how are they organized? What is the role of the command centre? Understand the role of two evasive techniques (no need to remember details). Countermeasure against (D)DOS attacks. What is black hole routing?