QUIZ SECNET 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.

When preparing yourself read the slide sets Lect 2 and Lect 3 and

- Comparison between RADIUS and Diameter, A Hosi, HUT, Finland, 2003.
- Cryptography in an all encrypted world , Ericsson Review, Dec 2015
- Paper on LTE: Security in the Evolved Packet System, R. Blom, et al. Ericsson Review, Oct 2010, http://www.eit.lth.se/fileadmin/eit/courses/eitn50/Literature/security_eps.pdf
- Understanding the Mirai Botnet, M Antonakakis, et all, Usenix, Aug. 2017.

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 2 and 3. 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 69/Lect2)

Key handling:

What is OoB? Key type: session, short –lived, master keys?

Simmons' Bound. Key entropy loss as result of protection (probability of impersonation).

Crypto and Quantum computing:

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

Authentication:

What does AAA stands 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 Radius alternatives work? Where is the key stored used during the authentication? Compare here the two alternatives. Pros and cons to use alternative 2?

What is Diameter?

Give some examples of features that make Diameter better than Radius.

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 4-5/Lect3. Role of A3 and A8.

What is GBA and what is it used for? Understand the diagram of the GBA solution, slide 60-61, Lect 2.

Why is the BSF key Ks not given to the NAF? It now gets KS_NAF.

Secure Connections:

Explain why we use session keys? In a secure transport protocol what are the roles of the subprotocols on Slide 64/Lect2?

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?

TLS 1.3 and QUIC; what are their round trip improvements in TLS 1.3 over TLS1.2

DTLS vs TLS.

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 at the 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 Slide15-16/lect3. 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, Slide17/Lect3?

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

How is the SUCI computed from the SUPI? Slide 27-28, Lect 3.

Botnet:

What is botnet and how are they organized?

DDOS:

What is the role of the command centre?

What is C2?

Understand the role of two evasive techniques (no need to remember details).

Countermeasure against (D)DOS attacks.

What is black hole routing?

DNSEC and DDOS: Why is DNSSEC not so good from DDOS perspective?

DNS amplification attack, how does it basically work?

Reflection attack, how does it basically work?

Mirai botnet: what is it and how is it established (increase it's attack power)?

Mirai botnet: what are its main phases?

Mirai botnet: what is attacked and by how many?