CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2018-10-12, 14:00 – 18:00

No extra material is allowed during the exam except for an English language dictionary in paper form. **No electronic devices allowed.**

The last page of this exam contains pictures of some protocols and headers that *may* be useful in some questions.

Give clear answers. Your thoughts and ways of reasoning must be clearly understood! Questions must be answered in English.

Teacher: Tomas Olovsson
Dept. of Computer Science and Engineering

Questions during exam: Tomas Olovsson, 031 - 772 1688

Inspection of exam: See web page for announcement

CTH Grades:	30-38 → 3	39-47 → 4	48-60 → 5
GU Grades:	30-47 → G		48-60 → VG

1. Attacks

a) Give an example of a link-layer attack (2p)

b) Give an example of a Network layer attack (2p)

c) Give an example of a Transport layer attack (2p)

Clearly explain how they work, what makes the attacks possible and the possible/desired results of the attacks!

d) The goal of some DoS attacks is to try to exhaust the resources of the target, for example memory, internal tables, network or the CPU. Describe <u>two</u> possible DoS attacks targeting different resources, how they work and what weaknesses they make use of!
(You cannot reuse attacks in a-c above.) (4p)

2. Authentication

a) An application that wants to authenticate a user (a client) over a network is designed to request the client to encrypt the *username* + *password* with the system's public key and then send it to the server: $\mathbf{E_{pk}(username, password)}$. We can assume the server's private key is at all times kept secret and that the encryption algorithm cannot easily be broken. Is this a good solution or not? Explain! (2p)

b) Describe in detail the process of how a certificate is used, i.e. how the owner's identity can be verified by another party! What does the receiver of the certificate do? How is it distributed to the receiver? (4p)

c) Kerberos is a system we have studied in some detail. Mention briefly four functions or features it has! (4p)

3. Secure protocols

a) Many security protocols support sending messages without encryption and can still be protected against packet modification. Describe how this is done! (2p)

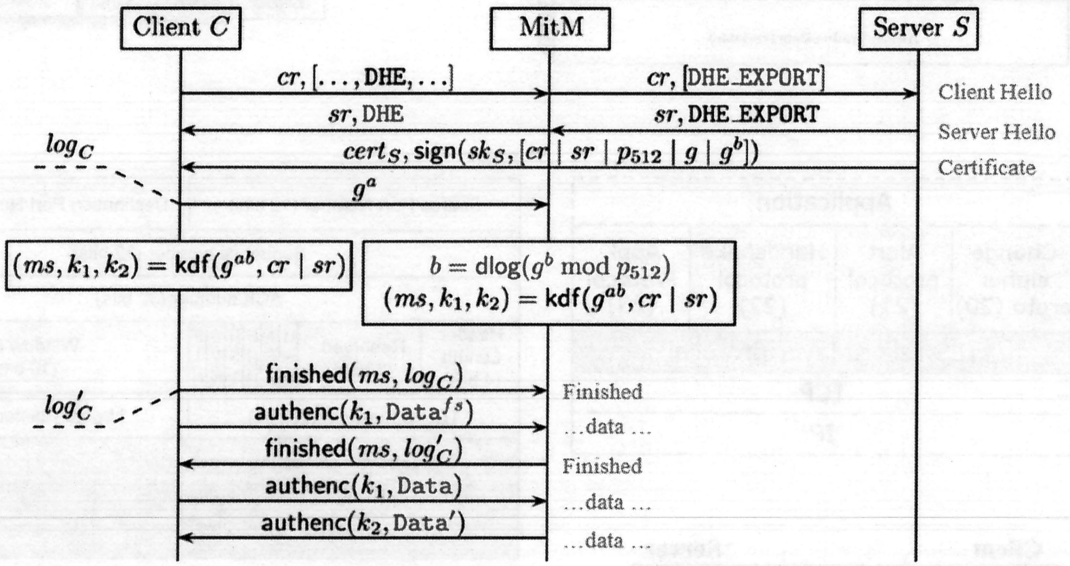
b) In secure protocols, nonces are almost always used. Why? What problem do nonces solve? Explain clearly what may go wrong without the nonces! (2p)

c) What is (Perfect) Forward Secrecy? How can it be achieved? (2p)

5. SSL/TLS and SSH

a) On the last page, there is a picture showing the SSL/TLS protocols (the one with yellow colors). Describe briefly the functionality of the record layer, change cipher, alert and handshake protocols! (4p)

b) The figure below shows a MITM attack against TLS that we have discussed in the course. Explain with some detail the steps shown below, how it is performed and what makes the attack possible to perform! (4p)



c) What is Secure Shell, SSH? What functionality to the user does it offer that is missing in SSL? (2p)

6. WLAN

a) WEP is not a secure protocol anymore. The reuse of initialization vectors (IVs) is one problem. Explain in some detail how this can be used by an attacker! (3p)

b) The WEP protocol is now considered broken. One attack we discussed during the course was the "Caffe Latte Attack", where the attacker could find the key to a network in less than 5 minutes even when the user was not connected to the network. Explain briefly how this attack is performed! (2p)

c) The 802.11i framework (WPA2) offers substantially better security than WEP. Mention three improvements in this protocol! (3p)

d) A feature present in many access points is "SSID broadcast disable". What does this mean? How secure is it? (2p)