CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2018-05-28, 08:30 – 12:30

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) The TTL (time to live) field in IP datagrams can be useful in many different ways for an attacker. Describe two possible attacks! Explain how they work and how they can be mitigated. (4p)

b) The possibility to fragment IP datagrams has shown to be problematic. Describe three different problems or attacks based on fragmentation and explain how they work! (6p)

2. DoS attacks and Authentication

a) One type of attack is SYN flooding. Explain how it works and why it can be problematic for the attacked hosts. Mention three different ways to, at least to some degree, protect a system against SYN-DoS attacks! (4p)

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

c) What is Radius and what high-level features does it have? What parties are involved? Why is it useful? (2p)

3. WLAN

a) In WEP, initialization vectors (IVs) are used together with the secret key when encrypting messages. What is the purpose of the IV? What happens if an IV is reused? Is this likely to happen? Motivate your answer! (3p)

b) WEP was later replaced by WPA2. Mention three changes and what problems they addressed! (3p)

c) The WEP protocol is now considered broken. One is the “Caffe Latte Attack”, where the attacker can find the key to for example a user’s home network in less than 5 minutes even if the user is not connected to the network. Explain briefly how this attack is performed! (2p)

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

4. SSL/TLS

a) On the bottom left on the last page, there is a picture showing the SSL handshake protocol and how a client and a server exchange information. Explain these messages, what they contain and their purpose! (5p)

b) Why are man-in-the-middle attacks not possible in SSL? Consider both the cleartext connection setup phase and data integrity during data communication. (3p)

c) A Pseudo-random function is used in TLS:

$$\mathbf{PRF(k, label, x) = HMAC_k(HMAC_k(label||x) \,||\, label||x) \;||\; HMAC_k(\ldots}$$

What is the purpose of this PRF-function? When is it used? (2p)

5. Firewalls and IDS Systems

a) In the course we have looked at different types of firewalls such as

- Static packet filters
- Dynamic packet filters
- Stateful packet inspection
- Circuit-level gateways/proxies

Explain with a couple of sentences for each type of firewall what it is and what it does! Make sure your answer makes it possible to distinguish the firewalls from each other. (4p)

b) What is the purpose of a screening router? Why not just use a good deep packet inspection firewall that takes care of all traffic? (2p)

c) IDS systems need to know when new TCP sessions are established between hosts. There are two main methods to do this: Handshake synchronization and Synchronize on data. Explain these two methods and give one advantage with each! (4p)

6. Mixed Questions

a) DHCP spoofing is a problem advanced switches can deal with. What is DHCP spoofing? And how can it be dealt with by a switch? (2p)

b) What protocol would you select when implementing a VPN system between two sites? Motivate your answer! (2p)

c) On the last page, there is a picture of an IPsec header. Explain what *next header and SPI* are used for and what purposes they have! (2p)

d) What is the difference between a master key and a session key, for example as in SSL/TLS? Why do we need both? (2p)

e) SSH (Secure Shell) offers a concept called “port forwarding”. What is it? What functionality does it offer? Explain with 2-3 sentences, not more. (2p)

Headers and pictures that may be useful