Network Security Exam
DT116G

Lennart Franked[*]

2011-10-27

Instructions

Carefully read the questions before you start to answering them, note the timelimit of the exam and plan your answers accordingly. Only answer the question, do not write about subjects remotely related to the question. Only write on one side of the sheet, and all answers must be written on the sheets, not on the exam paper.
Make sure that you write your answers clearly, if I can't read your answer you will not get any points, even if your answer is correct. The questions are *not* sorted by difficulty.

Aids Dictionary

Time 5 hours

Maximum points 58

Questions 12

Bonus points

You must get an E or higher, to get the bonus points added to your final grade. The bonus-points will be added to this exam, and the first re-exam.

Preliminary grades

$E \geq 50\%, D \geq 60\%, C \geq 70\%, B \geq 80\%, A \geq 90\%$

Questions

1: **Symmetric Encryption** 4p

(a) (3p) Describe the different components of a symmetric cipher.

(b) (1p) Draw a picture showing the different components and how they are interconnected.

2: **Security implementations** 6p

(a) (2p) Give two example of when to use SSLv3 / TLS.

(b) (4p) What information is sent during the handshake process?

3: **Asymmetric encryption** 6p

Show with the help of a picture how RSA works

[*] Tel: 060-148683, email: lennart.franked@miun.com

4: **Public key certificates** 4p

Describe how X.509 certificates are used as a way to insure the validity of a public key.

5: **Digital Signatures** 4p

(a) (2p) Using a block diagram, show how a digital signature is created from a message.

(b) (2p) Using a block diagram, show the principle of the verification process of a digital signature attached to a message.

6: **Email-security** 4p

What is the basic difference between X.509 and PGP in terms of key hierarchies and key trust?

7: **Threats** 6p

Explain the following terms, and give an example for every term:

(a) (2p) Integrity

(b) (2p) Confidentiality

(c) (2p) Authentication

8: **Attacks** 4p

Describe the following attacks:

(a) (2p) DDoS/DoS

(b) (2p) Man-in-the-middle

9: **Firewalls** 4p

Explain the difference between a packet filtering firewall and a stateful packet inspection firewall

10: **AAA** 6p

(a) (2p) In the context of kerberos, what is a realm?

(b) (4p) If host A that lies in one kerbers realm, would like to access a service that is located on host B which lies in another kerberos realm, how must host A proceed to gain access to this service?

11: **Intrusion detection** 2p

Explain the principle of an IDS, how does such a system recognize an attack?

12: **IP-Security** 8p

In the context of IP-Sec, explain the application of the following functions

(a) (2p) AH/ESP

(b) (2p) Tunnel-mode

(c) (2p) Transport-mode

(d) (2p) SA/SAD