Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT116G Network Security

Lennart Franked*

2012-01-13

Instructions

Carefully read the questions before you start answering them. Note the time limit of the exam and plan your answers accordingly. Only answer the question, do not write about subjects remotely related to the question.

Write your answers on separate sheets, not on the exam paper. Only write on one side of the sheets. Start each question on a new sheet.

Make sure you write your answers clearly, if I cannot read an answer the answer will be awarded no points – even if the answer is correct. The questions are *not* sorted by difficulty.

Time 5 hours.

Aids Dictionary.

Maximum points 56

Questions 12

Bonus points

You must get an E or higher, to get the bonus points added to your final grade. 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** 5p

Explain the following types of attacks on a symmectric encryption scheme:

(1p) (a) Ciphertext only

(1p) (b) Known plaintext

(1p) (c) Chosen plaintext

*lennart.franked@miun.se

(1p) (d) Chosen ciphertext

(1p) (e) Chosen text

2: **Digital signatures** 5p

(4p) (a) Describe HMAC and show with a figure how it works.

(1p) (b) Give an example of when HMAC is used

3: **Asymmetric encryption** 4p

(3p) (a) Describe the different components of an asymmetric cipher

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

4: **Public key cryptosystem** 3p

List and briefly define three uses of a public-key cryptosystem.

5: **Security Implementations** 4p

What is the difference between an SSL connection and an SSL session?

6: **Email-security** 4p

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

7: **Threats** 8p

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

(2p) (a) Confidentiality

(2p) (b) Integrity

(2p) (c) Availability

(2p) (d) Accountability

8: **Attacks** 3p

List and briefly define three classes of intruders

9: **Firewalls** 4p

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

10: **AAA** 6p

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

(4p) (b) If host A that lies in one Kerberos 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 IPSec, explain the application of the following functions

(2p) (a) AH/ESP

(2p) (b) Tunnel-mode

(2p) (c) Transport-mode

(2p) (d) SA/SAD