Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT116G Network Security

Lennart Franked*

2012-08-29

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 60

Questions 12

Preliminary grades

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

*lennart.franked@miun.se

Questions

(6p) 1. Explain the difference between asymmetric and symmetric ciphers, name some advantages and disadvantages with each type of encryption and give a usage example for each type of cipher.

2. Describe the following modes of operation for block encryption, explain using both text and figures:

(2p) (a) ECB

(2p) (b) CBC

(2p) (c) CFB

(2p) (d) CTR

(4p) 3. Explain in detail how encryption, decryption and authentication in GPG/PGP works.

(2p) 4. Explain the principle of MAC, how does it work, and when is it used?

(4p) 5. The SSL architecture contains four protocols spanned across two layers. Name two protocols and explain their purpose.

(4p) 6. How are X.509 certificates used to ensure the validity of a public key?

7. Explain the following terms, give an example of a threat that can compromise what it stands for, and give an example of a countermeasure for that threat.

(3p) (a) Confidentiality

(3p) (b) Integrity

(3p) (c) Authentication

(1p) 8. Give one example of how a virus could evade detection from an anti-virus software.

(4p) 9. Explain the difference between a packet filtering firewall and a stateful packet inspection firewall

(6p) 10. Name the key components of a Kerberos realm along with an explanation of their purpose.

(4p) 11. An IDS works by analysing the traffic on the network to identify possible intrusions, list and explain at least two different methods an IDS can use to identify an attack in progress.

12. 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