Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT116G Network Security

Lennart Franked*

2012-10-31

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 53

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. You have a large amount of raw data that you need to send to a colleague, it is important that both the confidentiality and integrity of the data is not compromised during the data transmission, you also want to ensure that only your colleaugue will be able to read the information and that your colleauge will be able to verify that the data received is infact from you. Explain how you would solve this using a *combination* of the different security mechanisms that you have read about during this course.

2. Describe the following modes of operation for block encryption using both text and figures. Give an example of usage for each mode.

(2p) (a) ECB

(2p) (b) CFB

(4p) 3. Explain in detail how encryption, decryption and authentication in GPG/PGP works, why is it constructed like this?.

(4p) 4. Explain HMAC using both text and figure.

(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) Availability

(1p) 8. How does a metamorphic virus work?

(2p) 9. Explain the difference between a circuit-level gateway and an application-level gateway.

(3p) 10. What are the main components in a Kerberos system? Explain their purposes.

(4p) 11. An IDS detects potential threats by analysing the traffic on a certain network. List and explain two different techniques an IDS can use to differentiate between legitimate traffic and traffic that might be a potential threat.

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