Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT116G Network Security

Lennart Franked*

2012-04-25

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 57

Questions 12

Preliminary grades

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

*lennart.franked@miun.se

Questions

(2p) 1. Match the type of attack on a symmetric cryptosystem with its corresponding description:

a. Ciphertext only	1. The attacker knows what encryption algorithm is used, have managed to get a text of his own choosing encrypted with the secret key and gotten hold of the corresponding ciphertext.
b. Known plaintext	2. The attacker knows what encryption algorithm used, have also managed to get her own version of a ciphertext decrypted, and gotten hold of the result.
c. Chosen plaintext	3. The attacker knows what encryption algorithm used and have a copy of the ciphertext that he want to decrypt.
d. Chosen ciphertext	4. The attacker knows what encryption algorithm is used, have a copy of the ciphertext that is to be decrypted, she has also been able to get a ciphertext of her own choosing decrypted with the secret key and gotten the corresponding plaintext, and also managed to get a plaintext of her own chosing encrypted and gotten hold of the corresponding ciphertext.
e. Chosen text	5. The attacker knows what encryption algorithm is used and have a copy of the ciphertext that is to be decrypted. He have also gotten over one or more plaintexts and its corresponding ciphertext that was encrypted using the secret key

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. Describe the different components of an assymmetric cipher and how these components are interconnected.

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

(4p) 5. How is an SSL session related to an SSL connection?

(4p) 6. What is the basic difference between X.509 and PGP in terms of key hierarchies and key trust?

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

(3p) 8. What are metamorphic and polymorphic viruses and why are they so difficult to detect?

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

10. In the context of Kerberos,

(2p) (a) 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?

(3p) 11. An IDS works by analysing the traffic on the network to identify possible intrusions, list and explain at least three different ways an IDS can use to identify if an attack is 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