UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

Exam in:	INF3510 – Information Security
Day of exam:	4 June 2010
Exam hours:	14:30h – 17:30h
This examination paper consists of:	3 pages.
Appendices:	None
Permitted materials:	Dictionary

Make sure that your copy of this examination paper is complete before answering.

Answer all 10 questions in this examination paper.

Each question is worth 10%.

Be concise. When answering each sub-question a), b), c) etc. it is normally sufficient to write a single sentence to describe each concept that the question asks for.

Question 1: General Information Security.

a. List and briefly explain the three traditional information security services. (3%)
b. Authentication and Non-Repudiation are two additional information security services. Briefly explain these two security services, and the difference between them. (2%)
c. Briefly describe two good reasons for having security policy/policies. (2%)
d. Briefly describe the two different interpretations of authorization, and give an example of how confusion can result from these two different interpretations. (3%)

Question 2: Cryptography.

a. What is the difference between a symmetric cipher and an asymmetric cipher? (2%)
b. List the main four basic properties of hash functions. (2%)
c. Alice wants to send a message M in cleartext to Bob who wants to be able to verify that the message did not change in transit, i.e. to ensure integrity. To provide integrity Alice and Bob have agreed to use a MAC (Message Authentication Code) based on using a hash function and a symmetric cipher. Key exchange has already occurred, so they share a key K. Briefly outline the cryptographic steps that Alice and Bob must follow to transmit and ensure the integrity of the message M by creating and verifying a MAC. (4%)
d. Formally describe the operation of the Diffie–Hellman key exchange protocol. (2%)

Question 3: Key Management and PKI.

a. Keys are used for protection or processing. In each of the following cases explain what protection and processing means and specify which key is used in each operation: (3%)
    i. Symmetric encryption/decryption
    ii. Asymmetric encryption/decryption (for confidentiality)
    iii. Digital signature generation/verification
b. The NIST SP800-57 Recommendation for Key Management specifies a set of 6 different states for cryptographic keys. List these states and specify for each state whether the key can be used for protection, for processing, for both, or for nothing. (3%)
c. What is the main purpose of an X.509 public-key certificate? (1%)
d. In a PKI, how should root certificates/public keys ideally be distributed, and how are they normally distributed in the browser PKI ? (2%)
e. What is the purpose of having self-signed root certificates? (1%)

Question 4: Authentication.

a. Explain the difference between entity authentication and message authentication. (2%)
b. Mention two different cryptographic methods of achieving message authentication. (2%)
c. There are four basic requirements for using a human physiological or behavioural characteristic as a biometric characteristic. Briefly describe these four requirements. (4%)
d. Briefly explain the concept of n-factor user-authentication, and briefly describe an example of 2-factor authentication. (2%)

Question 5: Identity and Access Management.

a. Briefly explain the following four concepts related to identity management:
    1) Entity, 2) Identity, 3) Identifier, 4) Digital identity (4%)
b. Draw Zooko's Triangle, and explain what it says about identifier properties. (2%)
c. Briefly describe the federated model for management of user identities. (2%)
d. Describe one major advantages of the federated model. (1%)
e. Describe one major disadvantages of the federated model. (1%)

Question 6: Access Control and Security Models.

a. The Bell-La Padula security model is a label-based model for access control. Describe with a simple example how labels can be based on a combination of ordered levels and partially ordered categories. (2%)
b. Assuming that labels are defined as in (a) above, formally define the concept of dominance relationship between labels. (2%)
c. Formally define the simple security property (ss) and the star property (*) of the Bell-La Padula security model. (2%)
d. What is separation of duties, and why is it useful for access control policies? (2%)
e. Briefly explain the two ways of specifying separation of duties in the RBAC (Role Based Access Control) model. (2%)

Question 7: Physical Security and the Human Factor.

a. What is the difference between a Standby/Offline UPS (Uninterruptible Power Supply) and a True Online UPS? (2%)
b. What does CPTED stand for? (1%)
c. What is the difference between CPTED and traditional physical security (i.e. locks and walls etc.) with regard to how they can prevent physical intrusion? (2%)
d. Developing trust is a key element in social engineering attacks. Briefly explain the method of "reverse social engineering" for developing trust. (1%)
e. Briefly explain the practice of dumpster diving? (1%)
f. Briefly describe three elements in the defending against social engineering attacks. (3%)

Question 8: Security Management.

a. What is the title of the standard ISO/IEC 27002? (1%)
b. How many security objectives are described in ISO/IEC 27002? (1%)
c. List three of the security objectives from (b) above. (3%)
d. Which standard describes the ISMS (Information Security Management System) ? (1%)
e. List and explain in one sentence the elements of the PDCA model used in the ISMS (4%)

Question 9: Risk Management and Business Continuity Planning.

a. Briefly and clearly explain the concept of risk, and use a diagram to illustrate your explanation. (2%)
b. In the context of risk analysis, describe the main difference between qualitative and quantitative analysis, and mention one drawback for each method. (4%)
c. As part of business continuity planning, a BIA (Business Impact Analysis) is often performed. Briefly explain the meaning and purpose of a BIA. (2%)
d. What is the MTD (Maximum Tolerable Downtime) and how is it taken into account when deciding whether business recovery at an alternative site should be invoked? (2%)

Question 10: Privacy and Computer Forensics.

a. Which international organization first published guidelines on data privacy in the form of a set of data privacy principles, and in which year were these guidelines published? (2%)
b. List and briefly explain two of the privacy principles from the guidelines of (a). (4%)
c. List and explain (in one sentence each) the four main steps of computer forensics. (4%)

End of paper