UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

Exam in	**INF3510 – Information Security**
Day of exam:	**3 June 2015**
Exam hours:	**14:30h – 18:30h**
This examination paper consists of:	**4 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.

Answers can be written in English or in Norwegian.

Each question can give 10 points, so all 10 questions can give a total of 100 points.

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

Question 1: General Security Concepts.

a. Write the definition (approximately) of *information security* according to ISO27001. (2p)
b. Write the definition (approximately) of *confidentiality* according to ISO27001. (2p)
c. Give the interpretation of authorization consistent with the definition of confidentiality.(1p)
d. Give the other (inconsistent) interpretation of authorization often found in text books. (1p)
e. Mention the 3 main categories of security controls, with one example from each. (2p)
f. In which aspect is non-repudiation of data origin stronger than data authentication ? (2p)

Question 2: Human Factors in Security

a. Mention two situations when increased support to a staff member and special monitoring of her/his integrity could be appropriate in order to reduce the risk of insider threats. (2p)
b. Which type of vulnerability is exploited by social engineering attacks? (2p)
c. Awareness can be seen as an intrusion detection function for stopping social engineering attacks. Unfortunately people can make errors of judgment when trying to detect attacks. In this scenario, what would be: i) a false positive, and ii) a false negative detection? (2p)
d. Explain the consequence on i) the false-positive rate, and ii) the false-negative rate in case a company implements a practice aimed at stopping all social engineering attacks. (2p)
e. The terms *private key* and *firewall* represent security metaphors. Explain why they can be bad metaphors that can cause misunderstanding of the security concepts they represent. (2p)

Question 3: Risk Management.

a. Draw a diagram to explain *risk* as a function of *threat agent*, *vulnerability*, and *impact*. (2p)
b. Mention the 2 factors that determine the strength of a threat agent (attacker). (2p).
c. Mention 2 typical approaches to identify relevant threat scenarios. (2p)
d. Assume that a relevant threat scenario has been identified. Briefly describe the 2 main factors that influence the likelihood of the threat scenario to happen. (2p)
e. Assume a quantitative risk model, where for a particular risk the following values are set:
AV (Asset Value) = EUR 800,000,
EF (Exposure Factor) = 0.2,
ARO (Annualised Rate of Occurrence) = 0.5.
Give the SLE (Single Loss Expectancy) and the ALE (Annualised Loss Expectancy). (2p)

Question 4: Computer Security.

a. Briefly describe 2 typical approaches for strengthening computer platform security. (2p)
b. What does the acronym TPM stand for ? (1p)
c. Briefly explain the 3 main TPM-supported services. (3p)
d. Per unique TPM there is an Endorsement Key pair. How/where is the private key stored? (1p)
e. What does the abbreviation UEFI stand for ? (1p)
f. In Windows 8 (and 10), what is the difference between authenticated boot supported by the TPM, and secure boot supported by UEFI ? (2p)

Question 5: Cryptography.

a. What is the difference between hash functions and MAC functions wrt. usage of keys ? (2p)
b. What is the hash size in SHA-1 ? (1p)
c. What are the possible hash sizes in SHA-2 ? (2p)
d. Which key should Alice use for encrypting messages to Bob with an asymmetric cipher (1p)
e. Alice sends message *M* with digital signature Sig(*M*) to Bob. They have each other's public keys $K_{pub}(A)$ and $K_{pub}(B)$, a hash function h, as well as an asymmetric algorithm running in signature mode S (equivalent to Decryption mode D) or in verification mode V (equivalent to Encryption mode E). Write the steps that Alice takes for signing and sending message *M*, and the steps that recipient Bob takes for verifying and validating the signature Sig(*M*). (4p)

Question 6: Key Management and PKI.

a. In a domain of *n* entities, each pair of entities must be able to communicate securely. For each case A, B, & C, state: i) How many different keys are needed, ii) How many initial key distributions are needed, and iii) What key protection (confidentiality or integrity) is needed.
   A. Symmetric-key cryptography. (3p)
   B. Public/private-key cryptography <u>without</u> PKI. (3p)
   C. Public/private-key cryptography with PKI (1 root CA and no intermediate CAs). (3p)
b. State the main advantage of having a PKI when using public/private-key cryptography. (1p)

Question 7: User Authentication.

a. Mention the three categories of credentials for user authentication. (3p)
b. Briefly explain the 2 main effects/purposes of password salting. (2p)
c. Mention the 4 basic requirements for using a human characteristic as a biometric. (2p)
d. User authentication frameworks for eGovernment typically specify 3 different classes of requirements for each assurance level. Mention these 3 requirement classes. (3p)

Question 8: Identity and Access Management.

a. Draw a diagram of the main phases of IAM, as well as the main steps of each phase. (3p)
b. Briefly describe (without diagram) the silo model for Id management. (1p)
c. Give 1 main advantage and the 1 disadvantage of the silo model. (2p)
d. Define the concept of *Identity Federation* (roughly). (2p)
e. Give 1 main advantage and 1 main disadvantage of federated identity management. (2p)

Question 9: Network Security.

a. Draw a diagram of the message exchange in case of a TLS/SSL stripping attack. (2p)
b. On the diagram you made in a) above, indicate where HSTS stops the attack. (1p)
c. What is the meaning of the acronym HSTS ? (1p)
d. Briefly explain how HSTS protects against TLS/SSL stripping. (2p)
e. Draw a diagram of the message exchange in case of TLS/SSL inspection in a firewall. (2p)
f. How can a user know when TLS-encrypted traffic is being inspected in a firewall ? (2p)

Question 10: Application Security.

a. What is OWASP Top 10 ? (2p)
b. Name the nr.1 in OWASP Top 10, and explain why it is so prevalent. (2p)
c. What is specified as the first phase in Microsoft SDL (Secure Development Lifecycle).(1p)
d. Which type of software development model is Microsoft SDL primarily combined with? (1p)
e. Briefly explain the concept of software fuzzing. (2p)
f. Why is software fuzzing important for cybersecurity ? (2p)