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)

Answer

a. 0.5p each for: (i) confidentiality, (ii) integrity, (iii) availability, (iv) other security properties, expressed in def. approximately as: "The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved."
b. 2p for something like: Confidentiality is the property that information is not made available or disclosed to *unauthorized* individuals, entities, or processes. Subtract 1p in case of missing therm *(un)authorized*.
c. 1p for: Meaningful authorization is "to specify AC policy (i.e. access privileges)".
d. 1p for: Inconsistent authorization is that "the system grants the user access".
e. 0.5p each for i) Physical Controls, ii) Technical Controls and iii) Admin. Controls, 0.5p for: at least 1 correct example (i.e. strictly only needed for 1 category).
f. 2p for: Non-repudiation can provide proof of data authenticity to third parties. Data authentication can only prove authenticity to intended recipient of data.

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)

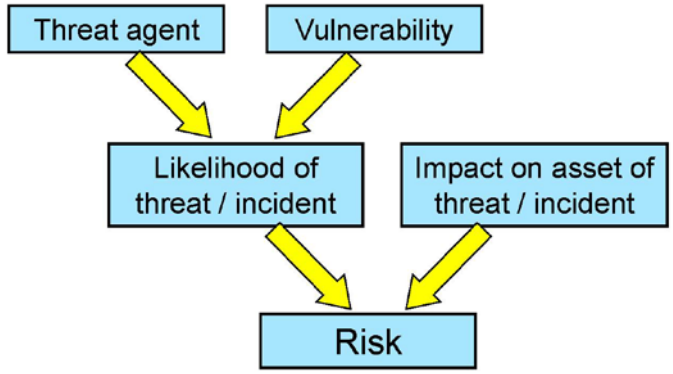
Answer a) 1p each for 2 valid situations such as:
i) For staff who are working in highly trusted/sensitive positions.
ii) For staff in a difficult personal situation such as conflict, personal problems, job loss.
b. 2p for: Social engineering attacks exploit vulnerabilities in humans, such as human ignorance, gullibility and lack of awareness.
c. 1p for: False positive is when staff misjudges a genuine colleague to be an attacker.
1p for: False negative is when staff misjudges an attacker to be a colleague.
d. 1p for: It would give relatively low false negative rate,
1p for: It would give a relatively high false positive rate.
e. 1p for: *Private key* can be misunderstood as giving privacy. In reality it decrypts private (confidential) data, or it provides integrity protection for public data.
1p for: *Firewall* can be misunderstood as an impenetrable barrier (analogous to physical firewall) that stops all (malicious) traffic. In reality it is a security filter where the achieved security (i.e. percentage of blocked attacks) depends on filtering rules.

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)

Answer

a. 2p for diagram like:



(1p for a diagram of a triangle with Assets, Threats, Vulnerabilities in the corners.)

b. 1p for: Capacity, i.e. skills and resources to attack
1p for: Motivation to attack
c. 1p each for any 2 of:
i) Attacker-Centric threat identification,
ii) System-Centric (aka. SW, design or architecture centric) threat identification, a
iii) Asset-Centric threat identification.
d. 1p for: The attacker (threat agent) strength.
1p for: The degree of vulnerability (ease of compromise) of the targeted/involved components (technical or human) in the threat scenario.
e. 1p for: SLE = EUR 160,000
1p for: ALE = EUR 80,000

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)

Answer

a. 1p each for any 2 of: i) Strengthening the OS, ii) Improved CPU security features, iii) Platform virtualization, iv) Trusted Computing (integrated security hardware(TPM) v) External security hardware combined with platform
b. 1p for: Trusted Platform Module.
c. 1p for: Authenticated boot: Report the integrity status of the software when booting.
   1p for: Sealed storage: Decryption with secret keys only ico. correct integrity.
   1p for: Remote Attestation: Report to external party the integrity status of software.
d. 1p for: Stored in secure non-volatile memory inside the TPM. Can not exit TPM. Can only be used inside TPM.
   Subtract 0.5p for incorrect statements such as: "key is encrypted and/or signed".
e. 1p for: Unified Extensible Firmware Interface
f. 1p for: Authenticated/measured boot means that the boot sequence is never halted, but the measures of software modules can be reported to external/remote parties. This is supported by the TPM.
   1p for: Secure boot means that the digital signatures on boot loader, kernel and drivers must be correct for the boot sequence to complete. Supported by UEFI.

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)

Answer

a. 1p for: Hash functions do not use keys, MAC uses keys.
   1p for: MAC functions use keys.
b. 1p for: SHA-1: 160 bit
c. 0.5p for each correct: i) 224, ii) 256, iii) 384, iv) 512 bit.
d. 1p for: Bob's public key.
e. <u>2p for: Digital signature generation by Alice:</u>
   i. Alice prepares message M.
   ii. Alice produces hash h(M).
   iii. Alice uses her private key $K_{priv}(A)$ to produce signature Sig(M) = S(h(M), $K_{priv}(A)$).
   iv. Alice transmits message M and signature Sig(M) to Bob,

   <u>2p for Digital signature validation by Bob:</u>
   i. Bob receives message M' (denoted as M', not M, because its origin is uncertain), as well as the signature Sig(M).
   ii. Bob produces hash value h(M').
   iii. Bob uses Alice's pub key $K_{pub}(A)$ to recover h(M) = V(Sig(M), $K_{pub}(A)$).

iv. Bob checks that h(*M*) = h(*M'*).

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 without 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)

Answer

a. Number of keys, number of distributions, and type of protection

A. 1p for: $n(n-1)/2$ different keys needed.
   1p for: $n(n-1)/2$ distributions (or $n(n-1)$, since 2 parties must receive each key)
   1p for: Secret key protection: Confidentiality

B. 1p for: n different public/private key pairs needed (n keys or $2n$ keys acceptable)
   1p for: $n(n-1)/2$ distributions, because every entity sends its public key to the others.
   1p for: Public key protection: Integrity

C. 1p for: $n + 1$ different public/private key pairs needed. ("n key pairs" is acceptable)
   1p for: n distributions of the root public key are needed.
   1p for: Root public key protection: Integrity.

b. 1p for: With PKI the number of key distributions is reduced from quadratic to linear.

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)

Answer

a. 1p each for: Something you know (knowledge),
   Something you have (ownership),
   Something you are (inherence),

b. 1p for: Password salting ensures that equal passwords have different hashes.
   1p for: Makes cracking difficult by preventing the use of pre-computed hash tables.

c. 0.5p each for: i) Universality, ii) Distinctiveness, iii) Permanence, iv) Collectability

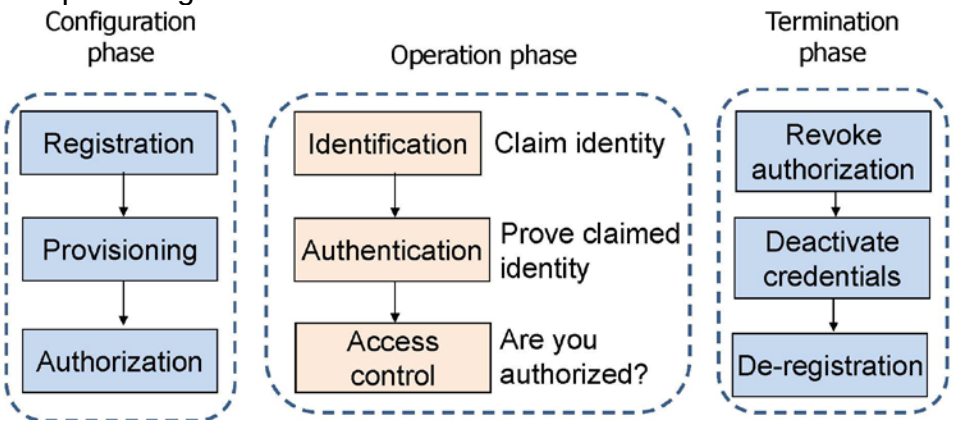
d. 1p each for: i) Authentication Method Strength requirements
   ii) Credential Management Assurance requirements
   iii) Identity Registration Assurance requirements

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)

Answer

a. 3p for diagram like:



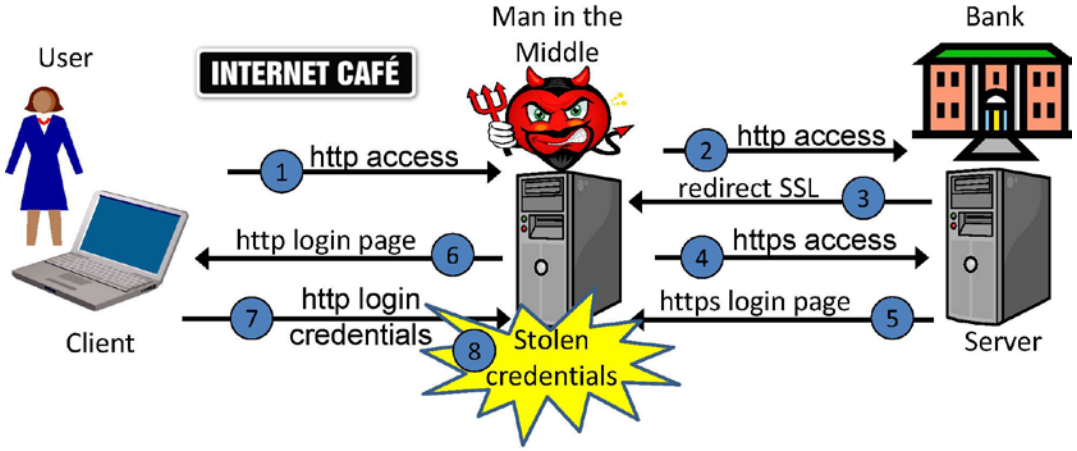
b. 1p for something like: In the silo model, the SP also acts as the IdP and maintains a namespace and a directory of user identities with credentials.
c. 1p for: Advantage: Relatively simple to implement from SP's point of view.
   1p for: Causes identity overload from user's point of view.
d. 2p for something like: Identity federation is a set of agreements, standards and technologies that enable a group of SPs to recognise user identities, credentials & entitlements from other IdPs and SPs.
e. 1p for any relevant advantage:
   (i) Improved usability
   (ii) Allows SPs to bundle services and collect user info
f. 1p for any relevant disadvantage:
   (i) High technical and legal complexity
   (ii) High trust requirements
      e.g. IdP is technically able to access SP on user's behalf
   (iii) Privacy issues,
      IdP collects info about user habits wrt. which SPs are used
   (iv) Limited scalability,
      Can only federate SPs with similar interests
      An Identity federation becomes a new silo

Question 9: Network Security.

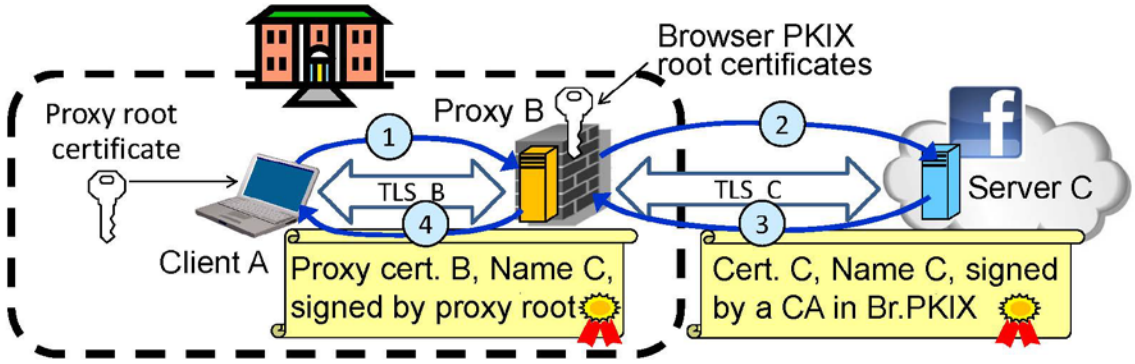
a. Draw a diagram of the message exchange in case of a TLS/SSL stripping attack. (2p)
b. On the diagram you made in a) above, indicate where HSTS stops the attack. (1p)
c. What is the meaning of the acronym HSTS ? (1p)
d. Briefly explain how HSTS protects against TLS/SSL stripping. (2p)
e. Draw a diagram 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)

Answer

a. 2p for diagram like:



b. 1p for: HSTS stops the attack after message (6).
c. 1p for: HSTS = http Strict Transport Security.
d. Browsers that support HSTS can hold HSTS policy for specific websites which dictates browsers to **only** use https to those websites. When the user requests a website with http, the browser automatically translates it to https. If an attacker tries to trick the browser to connect with http, the browser refuses to connect.
e. 2p for diagram like:



f. 2p for: The user must view the certification path of the received server certificate, and know the difference between a Browser PKIX root certificate and the internal proxy root certificate used for validation. If the certification path leads to an authentic root certificate of the Browser PKI, then there is no TLS inspection. If the certification path leads to the internal proxy root CA, the there is TLS inspection.

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)

Answer

a. 2p for: The OWASP Top 10 is a document describing the 10 most prevalent security risks/vulnerabilities in current web application, as well as how they can be avoided.
b. 1p for: (SQL) Injection vulnerabilities/attacks
   1P for: SQL injection is still nr.1 because software developers ignore how to prevent it, or because they are lazy.
c. 1p for: Security training is the forst phase on Microsoft SDL.
d. 1p for: Microsoft SDL is aimed at the waterfall Model.
e. 2p: Fuzzing is to generate many forms of malformed input and then to analyse resulting software crashes. The trace and location of a crash in the software helps to locate the bug causing the crash.
f. 2p: Some software bugs can be exploited by attackers to take control of a system, in which case the bug is a security vulnerability. Such bugs/vulnerabilities should be removed. Fuzzing helps discover and identify bugs that represent a cybersecurity vulnerability.