UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

Paper version of digital exam

Exam in	**INF3510 – Information Security**
Day of exam:	**8 June 2016**
Exam hours:	**9:00h – 13:00h**
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.

1. Write the definition (approximately) of *confidentiality* according to ISO27001. (2p)
2. Security controls can be grouped into three main categories.
   Padlocks and security guards represent which category of security controls? (1p)
   User authentication and data encryption represent which category of security controls? (1p)
   Security policies and awareness training represent which category of security controls? (1p)
3. Give one example of a preventive security control:. (1p)
   Give one example of a detective security control: (1p)
   Give one example of a corrective security control: (1p)
4. In which aspect is non-repudiation of data origin stronger than data authentication ? (1p)
   Which control/mechanism is typically used to implement non-repudiation? (1p)

Answer

1. 2p for: Confidentiality is the property that information is not made available or disclosed to *unauthorized* individuals, entities, or processes.
   Subtract 1p in case of missing term *(un)authorized*.
2. 1p for: Physical security controls (padlocks and security guards).
   1p for: Technical security controls (user authentication and data encryption).
   1p for: Administrative controls (security policies and awareness training)
3. 1p for any valid preventive control: encryption, authentication, awareness, padlock…
   1p for any valid detective control: IDS (intrusion detect.sys.) surveillance cameras…
   1p for any valid corrective control: backup of data & software, removal of malware…
4. 1p for: Non-repudiation can provide proof of data authenticity to third parties. Data authentication can only prove authenticity to intended recipient of data.
   1p for Non-repudiation is implemented with digital signatures.

Question 2: Information Security Management

5. Give the name of ISO27001 (1p)
   Briefly describe what ISO27001 is about (1 sentence is enough). (1p)
6. Give the name of ISO27002 (1p)
   Briefly describe what ISO27002 is about (1 sentence is enough). (1p)
7. 20 CSC (Critical Security Controls) is a framework which describes a set of elements for each of the 20 essential security controls. Select two correct elements. (2p)
8. Which is the highest level in COBIT's PCL (Process Capability Level) model ? (1p)
   Which aspect of security governance in PCL is the most fundamental/important? (1p)
   What is the basis for knowing the effectiveness of a security control? (1p)
   Which PCL level requires: *"Security culture permeates the organization"* ? (1p)

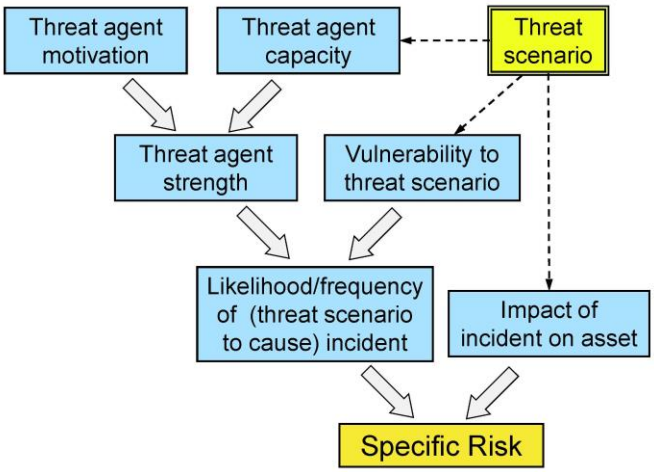
Answer

5. 1p for: ISO27001 = Information Security Management System
   1p for something like: It describes a framework setting up and managing an ISMS, i.e. establishing and operating a security program within an organisation.
6. 1p for: ISO27002 = Code of practice for information security management,
   1p for something like: It provides a checklist of security controls that organisations can consider using and implementing.
7. 1p for: *Why the control is critical* (specified by 20 CSC)
   1p for: *Effectiveness metrics* (specified by 20 CSC)
8. 1p for: *Level 5 (Optimizing)* is the highest in the COBIT Process Capability Levels.
   1p for: *Risk assessment* is the most important aspect of security governance.
   1p for: *Effectiveness metrics* are used to determine the effectiveness of controls.

1p for: *Level 5 (Optimizing)* requires: *"Security culture permeates the organization"*.

Question 3: Risk Management.

9. Select two elements from the diagram that must be specified in a typical practical method for qualitative assessment of risk. (2p)



10. Mention 2 typical approaches to identify relevant threat scenarios. (2p)
11. Briefly explain the principle for determining risk levels with a qualitative method. (2p)
12. Assume a quantitative risk model, where for a particular risk the following values are set:
    AV (Asset Value) = EUR 1,000,000,
    EF (Exposure Factor) = 0.2,
    ARO (Annualised Rate of Occurrence) = 0.1.
    Give the SLE (Single Loss Expectancy) and the ALE (Annualised Loss Expectancy). (2p)
13. Mention two (of the four) strategies for managing risk. (2p)

Answer

9. 1p for: Likelihood of incident
   1p for: Impact of incident on asset
10. 1p each for any 2 of:
    - Attacker-Centric threat identification,
    - System-Centric (aka. SW, design or architecture centric) threat identification
    - Asset-Centric threat identification.
11. 2p for: A matrix is used to determine a qualitative level of risk as a function of qualitative levels of likelihood and impact of incident.
12. 1p for: SLE = EUR 200,000
    1p for: ALE = EUR 20,000
13. 1p each for any two of:
    - Reduce/mitigate risk (security and mitigation controls)
    - Share/transfer risk (outsource activity that causes risk, or insure)
    - Retain risk (understand tolerate potential consequences)
    - Avoid risk (stop activity that causes risk)

Question 4: Cryptography.

14. What are the block size and possible key sizes in AES ? (4p)
15. Select two important factors for the cryptographic strength of a cipher (2p)
    - The design randomness
    - The cipher's key size
    - The cipher's ability to hide statistical patterns in data

- The computation speed

16. 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

14. 1p for: Block size 128 bits
    3p for: Key sizes i) 128, ii) 192, iii) 256 bits.
15. 1p for: The cipher's key size
    1p for: The cipher's ability to hide statistical patterns in data
16. 2p for: Digital signature generation by Alice:
    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,
    2p for Digital signature validation by Bob:
    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 5: Key Management.

17. The cryptoperiod (which may consist of separate protection and processing periods) limits the time a cryptographic key can be used, and mandates the key to be changed. Select the correct statement regarding cryptoperiods.. (1p)
    - The usage frequency of a key does not influence its cryptoperiod.
    - Frequent use of a key requires longer cryptoperiod.
    - Frequent use of a key requires shorter cryptoperiod.
18. Select the correct statement regarding cryptoperiods.. (1p)
    - High overhead for changing a key does not influence the cryptoperiod.
    - High overhead for changing a key requires longer cryptoperiod.
    - High overhead for changing a key requires shorter cryptoperiod.
19. Select the correct statement regarding cryptoperiods.. (1p)
    - High criticality and sensitivity does not influence the key's cryptoperiod.
    - High criticality and sensitivity requires longer cryptoperiod of the key.
    - High criticality and sensitivity requires shorter cryptoperiod of the key.
20. Select the correct statement regarding cryptoperiods.. (1p)
    - Fast computation of the encryption algorithm does not influence the key's cryoptoperiod.
    - Fast computation of the encryption algorithm requires longer cryoptoperiod of the key.
    - Fast computation of the encryption algorithm requires shorter cryoptoperiod of the key.

NIST SP800-57, Part 1, "Recommendation for Key Management" recommends cryptoperiods.

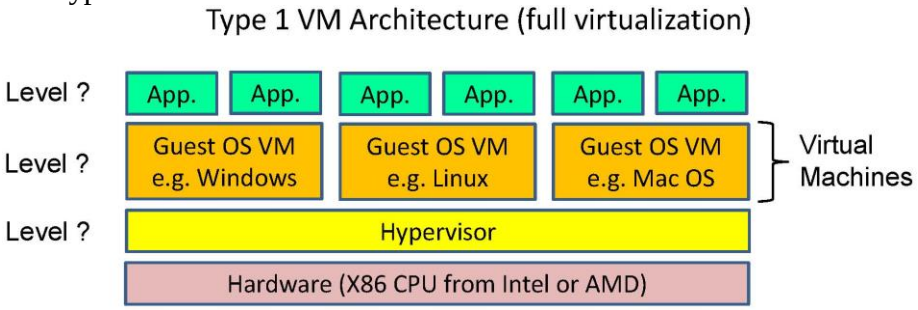
21. What is the latest recommended protection period time for a 1024 bit RSA key? (1p)
22. What is the latest recommended processing period time for a 1024 bit RSA key? (1p)
23. What is the latest recommended protection period time for a 2048 bit RSA key? (1p)
24. What is the latest recommended processing period time for a 2048 bit RSA key? (1p)
25. What is the latest recommended protection period time for a 3072 bit RSA key? (1p)
26. What is the latest recommended processing period time for a 3072 bit RSA key? (1p)

Answer

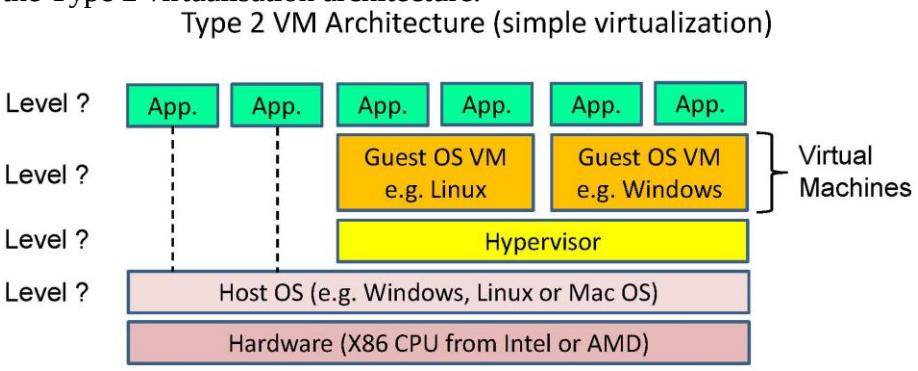
17. 1p for: Frequent use of a key requires shorter cryptoperiod.
18. 1p for: High overhead for changing a key requires longer cryptoperiod
19. 1p for: High criticality and sensitivity of the encrypted messages requires shorter cryptoperiod of the key.
20. 1p for: Fast computation of the encryption algorithm does not influence the key's cryoptoperiod.
21. 1p for: 1024 bit RSA key for protection: Not allowed now.
22. 1p for: 1024 bit RSA key for processing: Not allowed now (but legacy use OK).
23. 1p for: 2048 bit RSA key for protection: Until 2030
24. 1p for: 2048 bit RSA key for processing: Until 2030 (only legacy use after that)
25. 1p for: 3072 bit RSA key for protection: After 2030
26. 1p for: 3072 bit RSA key for processing: After 2030

Question 6: Computer Security.

27. The X86 CPU architecture protects processes from each other based on the privilege level (protection ring) structure. Indicate for each process type the corresponding privilege level in the Type 1 virtualisation architecture. (3p)



28. The X86 CPU architecture protects processes from each other based on the privilege level (protection ring) structure. Indicate for each process type the corresponding privilege level in the Type 2 virtualisation architecture. (4p)



29. Virtual machine architectures have implications for security. Select the correct statements about VMs and security. (3p)
    - Virtual machines prevent social engineering attacks.
    - Virtual machines are immune against computer viruses.
    - The OS or hypervisor can not interfere with VMs.
    - Malware can be executed in a VM without posing a risk for the rest of the computer.
    - Hackers can not hide their malware in a VM.
    - Malware can easily be detected in a VM.
    - A VM crash caused by malware can easily be analysed.
    - VMs running on the same physical machine are isolated/protected from each other.

Answer

27. 1p for: Applications, privilege level 3
    1p for: VMs, privilege level 0
    1p for: Hypervisor, privilege level -1
28. 1p for: Applications, privilege level 3
    1p for: VMs, privilege level 3
    1p for: Hypervisor, privilege level 3
    1p for: Host OS, privilege level 0
29. Correct statements are:
    1p for: Malware can be executed in a VM without posing a risk for the rest of the computer
    1p for: A VM crash caused by malware can easily be analysed.
    1p for: VMs running on the same physical machine are isolated/protected from each other.

Question 7: User Authentication.

30. Mention two types of synchronized authentication tokens. (2p)
    Mention the authentication principle used by tokens not based on synchronization, and which is typically used by physical access cards. (1p)
31. Briefly explain the two main effects/purposes of password salting. (2p)
32. In a biometric authentication system, the following statistical parameters are known:
    MAS= (number of matching attacker samples),
    TAS = (total number of attacker samples),
    NMUS= (number non-matching user samples),
    TUS = (total number user samples)

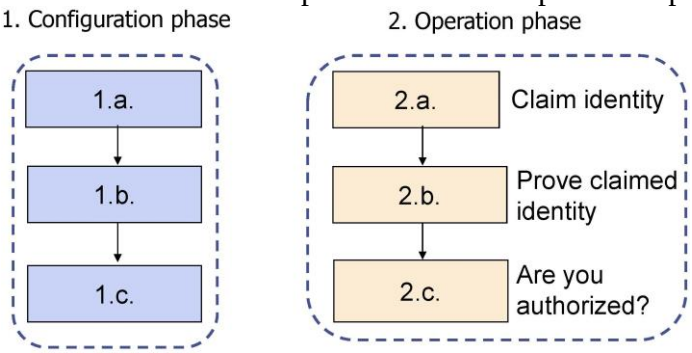
    FMR (False Match Rate) and FNMR (False Non-Match Rate) are expressed as fractions of two of the parameters above. Use the symbol "/" between parameters to write the fractions:
    FMR = ? (1p)
    FNMR = ? . (1p)
33. User authentication frameworks for eGovernment typically specify 3 different classes of requirements per authentication assurance level. Mention these 3 requirement classes. (3p)

Answer

30. 1p each for: Synchronised clock-based authentication tokens,
    Synchronised counter-based authentication tokens,
    Challenge-response authentication,
31. 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.
32. 1p for: FMR = MAS / TAS
    1p for: FNMR = NMUS / TUS
33. 1p each for: i) Authentication Method Strength requirements
    ii) Credential Management Assurance requirements
    iii) Identity Registration Assurance requirements

Question 8: Identity and Access Management.

34. IAM (Identity & Access Management) can be described in terms of separate phases, as illustrated above. Each phase consists of specific steps. Mention the name of each step: (2p)



35. Briefly describe the concept of *Identity Federation*. (2p)
36. Identity federations can have centralised or distributed identity management, as well as centralised or distributed authentication. The possible combinations are indicated with the letters A, B, C and D in the diagram. Facebook Connect, FEIDE and Id-porten/Altinn are three different identity federations. Indicate with a letter A, B, C or D the correct type that each federation corresponds to. One of the federation types in the diagram does not have a corresponding federation. (3p)

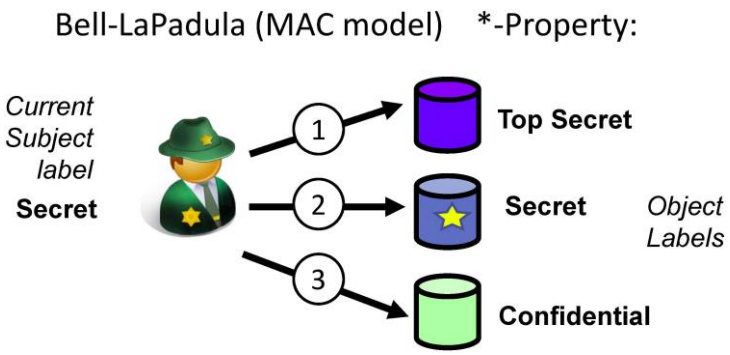
Federation types	Centralised Identity	Distributed Identity
Centralised Authentication	**A**	**B**
Distributed Authentication	**C**	**D**

Facebook Connect

FEIDE

Id-porten / Altinn

37. In the access control model of Bell-LaPadula, access authorizations are specified as a function of subject and object security labels. The diagram above indicates write-access operations for three combinations of subject and object security labels. Specify Allowed or Not allowed for each of the three write operations below to indicate the correct write-access authorization according to the Bell-LaPadula write-access rule (called the *-property). (3p)



Answer

34. 1p for: Configuration phase: a) Registration, b) Provisioning, c) Autorization
    1p for: Operation phase: a) Identification, b) Authentication, c) Access control
35. 2p for something like: A set of agreements, standards and technologies that enable a group of SPs to recognise and trust user identities and credentials from different IdPs (Identity Providers), CrPs (Credential Providers) and SPs (Service Providers).
36. 1p for: Facebook Connect: Type B (Type A is acceptable)
    1p for: FEIDE: Type D
    1p for: Id-porten / Altinn: Type C.
37. 1p for: Write op 1: Allowed
    1p for: Write op 2: Allowed
    1p for: Write op 3: Not allowed

Question 9: Communication Security.

38. DROWN is the name of an attack against TLS server software.
    i) What does the acronym DROWN stand for? (1p)
    ii) Briefly describe the nature of the DROWN vulnerability in TLS software. (2p)
    iii) Briefly describe the standard way of removing the DROWN vulnerability. (1p)
39. TLS/SSL stripping is an attack against TLS/SSL. HSTS is a technology to protect against the TLS/SSL stripping attack.
    i) Briefly describe the nature of the TLS/SSL stripping attack. (2p)
    ii) What does the acronym HSTS stand for? (1p)
    iii) Briefly explain how HSTS works. (1p)
40. How can a user know when TLS-encrypted traffic is being inspected in a firewall ? (2p)

Answer

38. 1p for DROWN: Decrypting RSA with Obsolete and Weakened eNcryption
    2p for: DROWN is a cross-protocol attack that abuses weaknesses in SSLv2 combined with the secure TLS protocol. Servers that run TLS but allow SSLv2 for backwards compatibility are vulnerable to DROWN attacks.
    1p for: To remove DROWN vulnerabilities, update TLS server software, and disable SSLv2 (and SSLv3).
39. i) 2p for: TLS/SSL stripping is a MitM (Man-in-the-Middle) attack, whereby a rogue (WIFI) router acts as a hidden proxy between a client and server, via a https connection to the server and a http connection to the client. The rogue router can then read, and inject data into the communication between the client and server.
    ii) 1p for: HSTS: HTTP Strict Transport Security
    iii)1p for: HSTS forces the browsers to only use https to servers that support HSTS. Users are not able to override the HSTS policy.
40. 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.

41. What is OWASP Top 10 ? (2p)
42. Name the nr.1 in OWASP Top 10, and explain why it is so prevalent. (2p)
43. What is specified as the first phase in Microsoft SDL (Secure Development Lifecycle)? (1p)
44. What do the abbreviations OpenSAMM and BSIMM stand for ? (2p)
45. What is the purpose of using a framework like OpenSAMM and BSIMM ? (2p)
46. Mention 1 difference between OpenSAMM and BSIMM. (1p)

Answer

41. 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.
42. 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.
43. 1p for: Security training is the first phase on Microsoft SDL.
44. 1p for: OpenSAMM: Open Software Assurance Maturity Mode
    1p for: BSIMM Build Security In Maturity Model
45. 2p for: They offer a framework for helping software development organisations to become better at making secure software, and a method for an organisation to assess how good (how mature) they are at doing secure software development.
46. Differences between OpenSAMM and BSIMM
    1p for any valid difference

OpenSAMM	**BSIMM**
Based on experience and principles of secure software development	Based on study of software security practices
Enables you to evaluate yourself against best practice	Enables you to compare yourself against others
Prescriptive	Descriptive
Sponsored by OWASP	Sponsored by Cigital and FortifySoftware
Not commercially oriented	Commercially oriented