UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

Exam in	**INF3510 – Information Security**
Day of exam:	**03 June 2014**
Exam hours:	**09:00h – 13:00h**
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.

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. Mention the 3 security services commonly abbreviated as CIA. (2p)
c. Write the definition (approximately) of *confidentiality* according to ISO27001. (2p)
d. Explain *authorization* in a way consistent with the definition of confidentiality. (1p)
e. Explain the other interpretation of authorization which is often found in text books. (1p)
f. In what way 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: CIA = Confidentiality, Integrity and Availability (1p for partially correct).
c. 2p for something like: Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
d. 1p for: Authorization is to specify access control policy definition, or in other words to define access privileges
e. 1p for: Authorization: The system grants user (subject) access to resources (object).
f. 2p for: Non-repudiation can provide proof of data authenticity to third parties. Data authentication can only prove authenticity to recipient.

Question 2: Information Securituy Management

a. Give the name of ISO27001, and briefly describe what it is (1 sentence is enough). (2p)
b. Give the name of ISO27002, and briefly describe what it is (1 sentence is enough). (2p)
c. Briefly explain the term *security control*, and mention the 3 categories of controls. (4p)
d. What is the fundamental basis for determining which security controls to implement ? (2p)

Answer

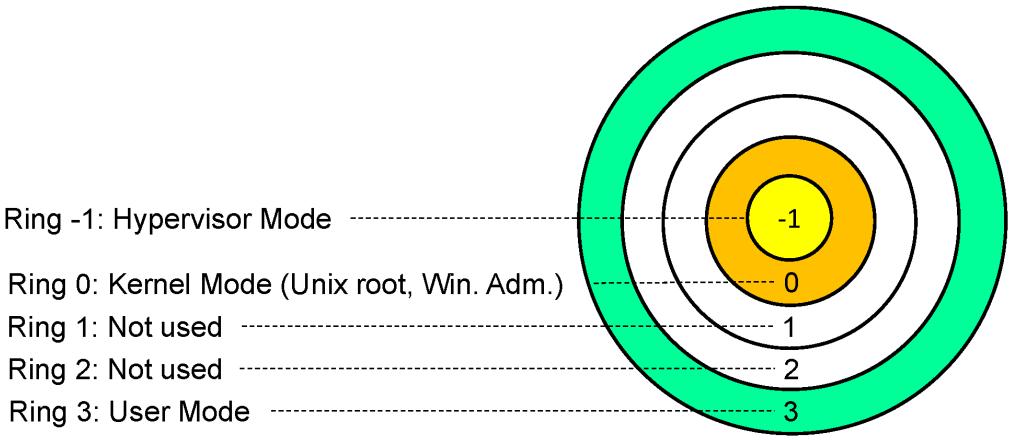
a. 1p for: ISO27001 = Information Security Management System
   1p for something like: It describes a framework setting up and managing an ISMS, i.e. establishing and operating a security program within an organisation.
b. 1p for: ISO27002 = Code of practice for information security management,
   1p for something like: It provides a checklist of security contorols that organisations can consider implementing.
c. 1p for: A security control is a practical mechanism, action, tool or procedure that is used to support security services.
   1p each for for: (i) Physical controls, (ii) Technical controls, (iii) Admin. controls
d. 2p: Risk assessment is used to determine where controls are needed. The most appropriate controls are selected to match risk according to proportionality principle.

Question 3: Computer Security.

a. What is a *reference monitor* ? (2p)
b. Mention 2 requirements for a reference monitor. (2p)
c. Draw a diagram of the 5 protection rings (privilege levels) implemented in modern microprocessors, and indicate the processing modes they are typically assigned to in modern computers. (3p)
d. What is the role of a hypervisor ? (1p)
e. Mention the proteciton ring assigned to the hypervisor in case of:
   i) Type 1 virtualisation (1p)
   ii) Type 2 virtualisation (1p)

Answer

a. 2p for: A reference monitor is a security model for enforcing an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system.
b. 1p each for any 2 of: i) Always invoked, ii) Tamper proof, iii) Verifiable correctness
c. 3p for diagram like:



d. 1p for: A hypervisor manages multiple guest OSs (virtual machines) in a computer.
e. 1p for: Type 1 virtualization: Ring -1 for hypervisor
   1p for: Type 2 virtualization: Ring 3 for hypervisor

Question 4: 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 wants to send message M with a digital signature Sig(M) to Bob. They have each other's public keys $K_{pub}(A)$ and $K_{pub}(B)$, have a hash function h as well as an asymmetric algorithm which runs in signature mode S (equivalent to Decryption mode D) or in verification mode V (equivalent to Encryption mode E). Write the steps that Alice follows when signing and sending message M, and the steps that recipient Bob follows for verifying and validating the signature Sig(M). (4p)

Answer

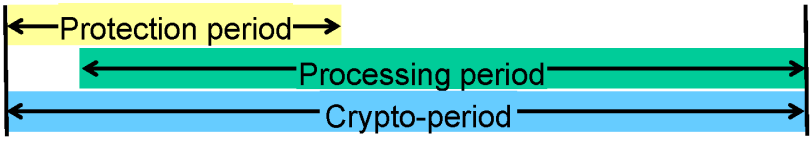
a. 1p for: Hash functions do not use keys, MAC uses keys.
   1p for: MAC functions use keys.
b. 1p for: SHA-1: 160 bit
c. 0.5p each for each of: i) 224, ii) 256, iii) 384, iv) 512 bit.
d. 1p for: Bob's public key.
e. 2p for: Digital signature generation by Alice:
   i. Alice prepares message *M*.
   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 and PKI.

a. Draw a diagram that relates crypto-period, protection period and processing period. (2p)
b. In a public-private key pair for signing, which key protects and which key processes ? (2p)
c. Mention the meaning of the abbreviation PKI. (1p)
d. What is the primary purpose of a PKI ? (2p)
e. Say Yes/No whether the following statements about self-signed certificates are true: (3p)
   i) Self-signed certificates provide assurance of authenticity.
   ii) Self-signing of certificates makes them similar to other certificates for processing.
   iii) Self-signed certificates can always be trusted as root certificates.

Answer

a. 2p for diagram like:



b. 1p each for: i) private key protects, ii) public key processes
c. 1p for: PKI = Public-Key Infrastructure.
d. 2p for: The purpose of a PKI is to ensure authenticity of public keys.
e. 1p for each correct:: i) No, ii) Yes, iii) No. Also subtract 0.5p for each wrong answer

Question 6: User Authentication.

a. Mention three categories of credentials for user authentication. (3p)
b. Briefly explain i) the principle and ii) the purpose of password salting. (2p)
c. Mention the 4 four basic requirements for using a characteristic as a biometric. (2p)
d. eGovernment user authentication frameworks typically define 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 is to include a random number (salt) when hashing
1p for: Salting ensures that equal passwords have different hashes, and makes cracking more 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: Authentication Method Strength requirements
Credential Management Assurance requirements
Identity Registration Assurance requirements

Question 7: Identity and Access Management.

a. Draw a diagram that illustrates the entities involved in the FEIDE system for federated identity management, and explain the messages flow during user authentication. (4p)

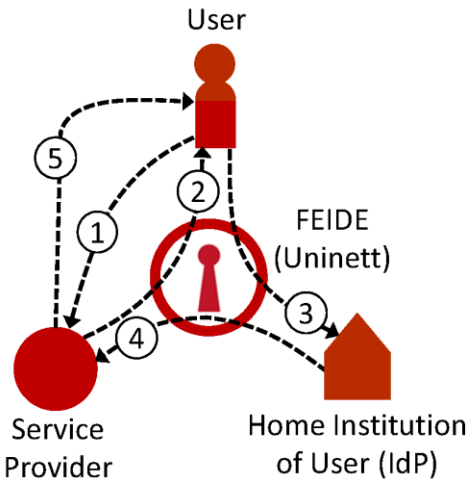
b. Mention the meanings of the abbreviations DAC, MAC, RBAC and ABAC. (2p)

c. Briefly describe how access control is modelled in ABAC. (2p)

d. What is the role of XACML when implementing ABAC systems ? (2p)

Answer

a. 0.5p for each correct entity (User, SP, IdP, FEIDE)
0.5p for each correct message (up to four messages).



1. User requests access to service
2. Service Provider sends authentication request to FEIDE, and displays FEIDE login form to user.
3. User enters name and password in FEIDE login form, which are sent for validation to Home Institution of user.
4. Home Institution confirms authentic user and provides user attributes to FEIDE which forwards these to SP
5. Service Provider analyses user attributes and provides service according to policy

b. 0.5p each for: DAC = Discretionary Access Control
MAC = Mandatory Access Control
RBAC = Role-Based Access Control
ABAC = Attribute-Based Access Control
The meaning of the concepts:

c. 2p for something like: ABAC specifies authorization policies (access rules) as a function of attributes. The access rules can apply to any type of attributes (user attributes, resource attribute, context attributes, access attributes etc.)

d. 2p for: Attributes for subjects, objects, context and action need to be communicated between the various parties in a distributed AC domain. To make this practical a common language for expressing attributes is needed, and this is precisely what XACML does.

Question 8: Communication Security.

a. In TLS/SSL
   i) What is the name of the protocol used for establishing the session key ? (2p)
   ii) Which RSA-key encrypts the transmitted secret used for generating the session key ? (1p)
   iii) Where does the RSA-key in question (ii) above come from ? (1p)
   iv) (How) Can a session key be established without RSA-keys ? (2p)

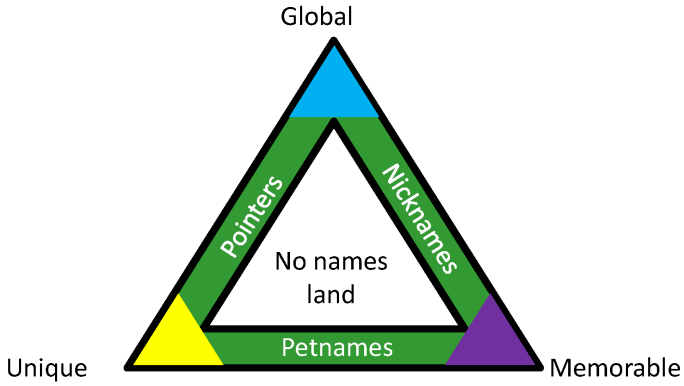
b. Draw Zooko's triangle and explain how it represents 3 types of names. (2p)

c. What is a *petname system* and how can it assist meaningful authentication of websites ? (2p)

Answer

a. For TLS/SSL
   i) 2p for: Handshake Protocol
   ii) 1p for: The server public key.
   iii) 1p for: From the server (certificate)
   iv) 1p for: Yes, 1p for: With Diffie-Hellmann key exchange (called Anonymous D-H)

b. 1p for diagram below
   1p for: No name class can have the 3 properties *global, unique* and *memorable* simultaneously, any name class can only have 2 of them.



c. 1p for: A petname system manages mappings between petnames and pointers.
   1p for: A petname system allows the user to easily recognise a globally unique name (pointer) through the personally defined petname.

Question 9: Perimeter Security.

a. Mention one main advantage and one main disadvantage of
   i) packet filter firewalls (2p)
   ii) application layer proxy firewalls (2p)
b. Briefly describe the method for *TLS/SSL stripping* in firewalls (do **not** draw diagram) (2p)
c. Mention one advantage and one disadvantage of each of the following Intrusion Detection Systems:
   i) Signature-based (misuse-based) IDS (2p)
   ii) Anomaly-based IDS. (2p)

Answer

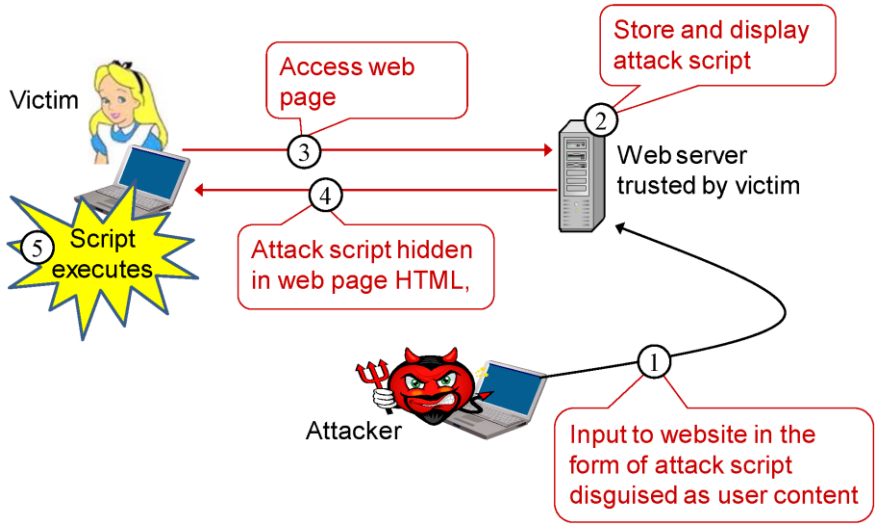
a. Firewalls advantage & disadvantage
   i) 1p for <u>one</u> valid advantage: • Packet filters are fast, • Easy to specify rules, …
      1p for <u>one</u> valid disadvantage: • Only allows primitive filtering rules, …
   ii) 1p for <u>one</u> valid advantage: • Applic. proxy firewalls can do advanced filtering, ...
      1p for <u>one</u> valid disadvantage: • Relatively slow, • Hard to specify filtering rules
b. 2p for: The firewall must be an application gateway with a TLS proxy. It requires the organization to set up an internal PKI and install its root certificate in every internal client computer. When a user accesses an external website through TLS, the TLS proxy connects to the external server with TLS, then generates and sends to the internal client an internal server certificate with the name of the external server, but signed under the internal root. This creates a clear-text gap at the firewall.
c. IDS advantages and disadvantages:
   i) 1p for <u>one</u> valid advantage of signature IDS
      – Fast, immediately detects known intrusions at runtime
      – Relatively fewer false alarms
      1p for <u>one</u> valid disadvantage of signature based IDS:
      – Can't detect new attacks that don't match existing signatures.
      – Must have signatures constantly updated to be effective
   ii) 1p for <u>one</u> valid advantage of Anomaly Based IDS:
      – Can detect new unknown attacks (by identifying unusual behavior)
      – Information from anomaly based IDS can be used as input to signature-based IDS
   | 1p for <u>one</u> valid disadvantage of Anomaly Based IDS such as:
      – Relatively many false positives (false alarms).
      – Usually requires a lot of training and tuning to define models of normal behavior.

Question 10: Application Security.

a. What is Trojan computer program ? (2p)
b. What is a botnet ? (2p)
c. Draw a diagram to explain the principle of Stored XSS (Cross Site Scripting) attacks. (2p)
d. Mention one relevant method for preventing XSS attacks. (2p)
e. State the meaning of the abbreviation OWASP. (1p)
f. Which is the nr.1 application security risk according to OWASP ? (1p)

Answer

a. 2p for: A Trojan is program with hidden side-effects. It is usually superficially attractive, such as a game, s/w upgrade etc., but it performs additional malicious tasks programmed by the attacker.
b. 2p for: A botnet is a collection of computers infected with malicious software agents (robots) that can be controlled remotely by an attacker.
c. 2p for diagram of Stored XSS like:



d. 2p for: XSS can be prevented by always sanitizing input to web servers.
e. 1p for: OWASP: Open Web Application Security Project
f. 1p for: (SQL) Injection vulnerabilities/attacks