UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

QUESTIONS AND ANSWERS

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%)

Answer

a. 0.5% each for: Confidentiality, Integrity and Availability.
0.5% each for correctly explaining what these terms mean, i.e. preventing unauthorized disclosure of information, preventing unauthorized (accidental or deliberate) modification or destruction of information, and ensuring resources are accessible when required by an authorized user.

b. 1% for: Messages authentication enables a recipient to verify the origin of a message, but does not necessarily enable the recipient to prove the same to a third party. Non-repudiation allows anybody to verify the origin of a message or an action, so that it can not be repudiated by the originator.

c. 1% for each good reason, e.g.: 1) Defines who is authorized to do what, 2) Defines appropriate use

d. 1% for: Authorization as policy definition of who can access what.
1% for: Authorization as positive access control decision
1% for: Attacker who accesses with stolen credentials will be authorized, nonsense.

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%)

Answer

a. 1% for: Symmetric ciphers use the same key for encryption and decryption
1% Asymmetric ciphers use public key for encryption and private key for decryption.

b. 0.5% for: Fixed length output for arbitrary length input
0.5% for: One-way - given M it is easy to compute H(M), but given H(M) hard to find M.
0.5% for: Collision resistant - hard to find M and M' so that H(M) = H(M')
0.5% for: A small change in M produces a major change in H(M).

c. 2% for Alice:
i) Generates message M
ii) Generates H(M), then MAC = E(H(M),K)
iii) Sends {M, MAC} to Bob
2% for Bob:
i) Receives {M, MAC}
ii) Generates MAC′ from M.
iii) Compares MAC′ and MAC
iv) If MAC = MAC′ then knows message is unchanged in transit

d. 2% for: Let a, b be the secret keys of A,B respectively. Then:
- A → B : g^a
- B → B : g^b
- A computes $(gb)^a = g^{ab}$
- B computes $(ga)^b = g^{ab}$

A,B now share the symmetric key g^{ab}

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%)

Answer

a. 1% for each correct meaning and correct key
   i. prot = encryption, proc = decryption, key = symmetric key
   ii. prot = encryption, key= public, proc = decryption, key=private
   iii. prot=generation, key=private, verification=proc, key=public

b. 0.5% for each correct state and operation:
   1) Pre-activation: none
   2) Active: both
   3) Deactivated: process
   4) Compromised: process
   5) Destroyed: none
   6) Destroyed-Compromised: none

c. 1% for: binding identifier & public key

d. 1% for: Through out-of-band secure channel
   1% for: Through browser SW distribution

e. 1% for processing root public key as certificate in the same way as other public-keys

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%)

Answer

a. 1% for: entity authentication: verify the identity of an entity at the end of a session
   1% for: message authentication: verify the origin of a message.

b. 1% each for any two of: symmetric encryption, MAC, digital signature,

c. 1% for: Universality: each person should have the characteristic;
   1% for: Distinctiveness: any two persons should have sufficiently different characteristics;
   1% for: Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
   1% for: Collectability: the characteristic can be measured quantitatively.

d. 1% for: Using n independent mechanism for verifying identity
   1% for: smart card + PIN or any other valid combination

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%)

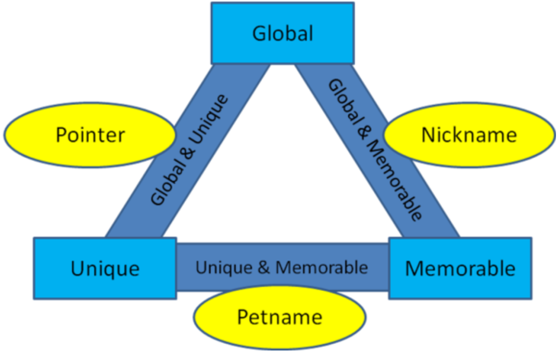
d. Describe one major advantages of the federated model. (1%)

e. Describe one major disadvantages of the federated model. (1%)

Answer

a. 1% for each of
   i. Entity: A person, organisation, agent, system, etc
   ii. Identity: A set of characteristics of an entity in a specific domain
   iii. Identifier : A characteristic or attribute that can be related to a specific entity
   iv. Digital identity: Identity resulting from digital codification of characteristics in a way that is suitable for processing by computer systems

b. 1% for Zooko's Zooko's Triangle



   1% for: can only have two of three desirable properties**:** **global**, **unique** and **memorable**.

c. 2% for: Identity Federation: A set of agreements, standards and technologies that enable a group of SPs (service providers) to recognize user identities and entitlements from other SPs. Identifier (and credential) issuance as for the silo model Mapping between a user's different unique identifiers Authentication by one SP/IdP (identity provider),

d. 1% for any of: Improved usability (theoretically) Compatible with silo user identity domains Allows SPs to bundle services Allows SPs to collect user information

e. 1% for any of: High technical and legal complexity. High trust requirements, e.g. SP1 is technically able to access SP2 on user's behalf. Privacy issues. Unimaginable for all SPs to federate, multiple federated SSOs not much better than the silo model.

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%)

Answer

a. 1% for: Example levels: H=(h1, h2, h3) where h1<h1<h3
   1% for: Example categories: C={c1, c2, c3}.
   A label is then L=(h,c) where $h \in H$ and $c \subseteq C$

b. Assume $L_A = (h_A, c_A)$ and $L_B = (h_B, c_B)$
   1% for: $h_B \leq h_A$
   1% for: $c_B \subseteq c_A$.

c. 1% for: Suppose a subject has observe (read) access to an object. The ss-property is satisfied if the subject security label dominates the object security label.
   1% for: Suppose a subject has simultaneous observe (read) access to object-1 and alter (write or append) access to object-2. The *-property is satisfied if the security label of object-2 dominates the security label of object-1.

d. 1% for Separation of duties means that the same person should not fill multiple roles.
   1% for: This is useful where there can be a conflict of interest, or where it can be required to take extra precautions in the form of involving multiple entities to perform an action.

e. 1% each for: SSD (Static Separation of Duties) and DSD (Dynamic Separation of Duties).

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%)

Answer

a. 1% for: A standby or offline UPS takes over in case of power supply failure from the power company. Causes short interruption and irregularity during switchover.
   1% for The True Online UPS works in the opposite fashion to a standby UPS since the primary power source is the battery, with the power feed from the utility constantly recharging the batteries. This model allows constant feed to the system, while completely eliminating power quality problems.

b. 1% for: Crime Prevention Through Environmental Design

c. 1% for: CPDET discourages intrusion
   1% for: Traditional security provides barriers to intrusion

d. 1% for: Cause a problem and subsequently offer your help to fix it

e. 1% for: Look through garbage to collect intelligence about attacks.

f. 1% each for any 3 of: Policy, Awareness Training for all staff, Resistance Training for key staff, Reminders, SE Detectors, Incident Response.

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%)

Answer

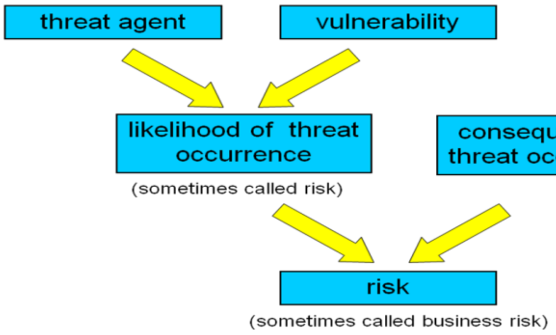
a. 1% for: Code of practice for information security management
b. 1% for: 11
c. 1% each for any three of: 1) Security policy, 2) Internal organization, 3) External parties 4) Asset management, 5) Human resources security. 6) Physical and environmental security, 7) Communications and operations management, 8) Access control, 9) Information systems acquisition, development and maintenance, 10) Information security incident management, 11) Business continuity management
e. 1% for: ISO/IEC 27001 Information Security Management Systems – Requirements;
f. 1% each for:
   i. **Plan** (establish the ISMS). Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organisation's overall policies and objectives
   ii. **Do** (implement and operate the ISMS). Implement and operate the security policy, controls, processes and procedures
   iii. **Check** (monitor and review the ISMS). Assess and where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.
   iv. **Act** (maintain and improve the ISMS). Take corrective and preventive actions based on the results of the management review to achieve continual improvement of the ISMS.

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%)

Answer

a. 2% for any one of the following two types of diagrams


threat agent
vulnerability
likelihood of threat occurrence
(sometimes called risk)
consequence of threat occurrence
risk
(sometimes called business risk)

Example Risk Matrix		**Consequence**			
		Insignificant	**Minor**	**Moderate**	**Major**
Likelihood	**High**	**M**	**H**	**E**	**E**
	Medium	**M**	**M**	**H**	**E**
	Low	**L**	**M**	**M**	**H**
	Unlikely	**L**	**L**	**M**	**M**

L: Low Risk, M: Moderate Risk, H: High Risk, E: Extreme Risk

b. 1% for: 1 mark for: Qualitative analysis uses words to describe the magnitude of potential consequences and likelihoods
1% for Quantitative uses numerical values.
1% for Major drawbacks of qualitative risk analysis are that the results are hard to justify objectively and that an exact value is not available for cost/benefit analysis.
1% for: Major drawbacks of quantitative risk analysis are that the calculations are more complex, it can be difficult to explain how the exact figures are obtained and the process can be very labour intensive (although tools are available).

c. 2% for: A BIA is performed at the beginning of business continuity planning to identify critical functions that in the event of a disruption would cause the greatest financial or otherwise negative impact.

d. 2% for: The estimated time to re-establish the business functions at the existing site is compared with the MTD. The business recovery plan must be invoked if the estimated time exceed the MTD.

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%)

Answer

a. 1% for: OECD, 1% for: 1980.

b. 2% each for any two of:

- **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date
- **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject; or by the authority of law.
- **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- **Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation Principle**: An individual should have the right: a) to obtain confirmation of whether or not the data controller has data relating to him; b) to have data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- **Accountability Principle**: A data controller should be accountable for complying with measures which give effect to the principles stated above

c. 1% each for:

i. Acquisition: Physically or remotely obtaining possession of the computer, all network mappings from the system, and external storage devices

ii. Identification: Identifying what data can be recovered, then electronically retrieving it by running various Computer Forensic tools and software suites

iii. Evaluation: Evaluating the information/data recovered to determine if and how it could be used again the suspect for employment termination or prosecution.

iv. Presentation: Presenting evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by United States and internal laws.