UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

QUESTIONS AND ANSWERS

Exam in:	INF3510 – Information Security
Day of exam:	7 June 2011
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 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: Security Management.

a. What is the title of the standard ISO/IEC 27001? (1%)
b. Briefly describe the 4 elements of the PDCA model defined by ISO/IEC 27001. (4%)
c. Information security controls are generally grouped in 3 categories that are often called "the 3 components of information security". Mention the 3 components of information security, and mention 1 example security control for each component. (3%)
d. Briefly define the security services *availability* and *non-repudiation*. (2%)

Answer

a. 1% for: Information Security Management Systems (Requirements)
b. 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.
c. 1% each for
   i. **Physical controls**, e.g. locks, guards, CCTV surveillance
   ii. **Technical controls**, e.g. cryptography, logical access control
   iii. **Procedural controls**, e.g. policies standards, procedures, awareness training
d. 1% each for
   Availability: to ensure resources are accessible when required by authorised user
   Non-repudiation: to create evidence of action to prevent false denial of action later

Question 2: Risk Management and Business Continuity Planning.

a. A possible definition of risk is: *risk* = *likelihood* × *consequence*. Briefly explain what is meant by *likelihood* and *consequence* in this definition. (2%)
b. The P-phase of the PDCA model from ISO/IEC 27001 specifies 5 steps of risk management. Mention those 5 steps. (2%)
c. A qualitative risk analysis method specifies three likelihood levels (low, medium, high) and three impact/consequence levels (minor, moderate, major). Draw the appropriate look-up table for deriving qualitative risk defined with five possible different risk levels: N: negligible risk, L: low risk, M: moderate risk, H: high risk, E: extreme risk. (2%)
d. As part of business continuity planning, a BIA (Business Impact Analysis) is often performed. Briefly explain the meaning and purpose of a BIA. (2%)
e. 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. 1% each for:
   Likelihood is the frequency (or probability) that the negative incident (threat) occurs.
   Consequence is the expected cost (or maybe benefit) from the event occurring.

b. 0.5% each for any 4 of:
   - Define risk assessment method
   - Identify risks
   - Assess risks
   - Identify options to treat risks
   - Select controls

c. 2% for table:

Example Risk Matrix		Consequence		
		Minor	**Moderate**	**Major**
Likelihood	**High**	**M**	**H**	**E**
	Medium	**L**	**M**	**H**
	Low	**N**	**L**	**M**
N: Negligeible, L: Low, M: Moderate, H: High, E: Extreme				

d. 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.

e. 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 3: Computer Security.

a. The Intel microprocessor provides 4 protection rings (0-3). Briefly explain how a process running in ring *m* can access a memory segment in ring *n* in the following cases:
   i) $m \leq n$ (process is equally or more privileged than memory segment) (1%)
   ii) $m > n$ (process is less privileged than memory segment). (1%)

b. Which protection rings are actually used in Linux and Microsoft Windows? (2%)

c. Why are drivers often specified with privilege level 0 contrary to the general security principle of placing drivers at a less privileged level than kernel? (1%)

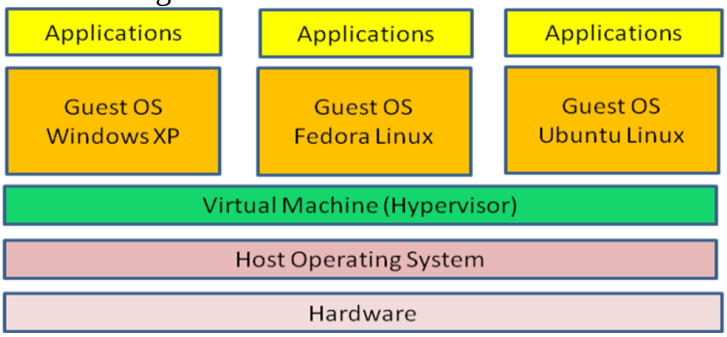
d. Draw a diagram to illustrate a computer platform with virtual machines. (2%)

e. Mention a security benefit of running applications in a virtual machine. (1%)

f. What is the main difference between TCSEC and the Common Criteria regarding how security functionality can be specified relative to the assurance level? (2%)

Answer

a. 1% each for:
   i) $m \leq n$: direct access
   ii) $m > n$: only through OS calls
b. Add +1% each for rings 0 and 3 (correct)
   Subtract −1% each for rings 1 and 2 (wrong)
c. 1% for: Performance reasons.
d. 2% for a diagram like:



e. 1% for a reasonable advantage e.g.:
   - Take a snapshot of current OS state, use this later on to reset system to that state
   - Malware will only infect virtual machine guest OS, not the whole computer.
f. 1% for: TCSEC ties functionality to assurance level
   1% for CC lets functionality be independent from assurance level

Question 4: Cryptography.

a. List the four basic properties of hash functions. (2%)
b. What is the difference between a MAC function and a hash function? (2%)
c. Alice wants to send a secret session key K_S to Bob, with confidentiality. Alice and Bob both have their public-private key pair denoted as $K_{pub}(A)$, $K_{priv}(A)$ and $K_{pub}(B)$, $K_{priv}(B)$ with a corresponding asymmetric encryption algorithm, and have an authentic copy of each others' public keys. Outline the steps that Alice and Bob must follow to encrypt and decrypt the secret session key K_S. Authentication is not considered here. (4%)
d. State in which order the signature and encryption functions should be applied in case digital signature and encryption are combined. Also explain the reason. (2%)

Answer

a. 0.5% each for::
   H1: Fixed length output for arbitrary length input
   H2: One-way - given M it is easy to compute H(M), but given H(M) it is hard to find M.
   H3: Collision resistant - hard to find M and M' so that H(M) = H(M')
   H4: A small change in M produces a major change in H(M).
b. 2% for: A hash function only generates a checksum, and does by itself not support message authentication. A secret key must be used in some with the hash function to support authentication, so a MAC uses a secret key to generate an authentication code.
c. 2% for encryption by Alice:
   i) Alice encrypts the key K_S using the asymmetric algorithm in encryption mode E using Bob's public key $K_{pub}(B)$,, to produce the encrypted key C, where $C = E(K_S, K_{pub}(B))$.
   ii) Alice transmits the encrypted key as C to Bob.

2% for decryption by Bob:
i) Bob receives the encrypted key as C.
ii) Bob decrypts C using the asymmetric algorithm in decryption mode D using his private key $K_{priv}(B)$, to recover K_S, where $K_S = D(C, K_{priv}(B))$.

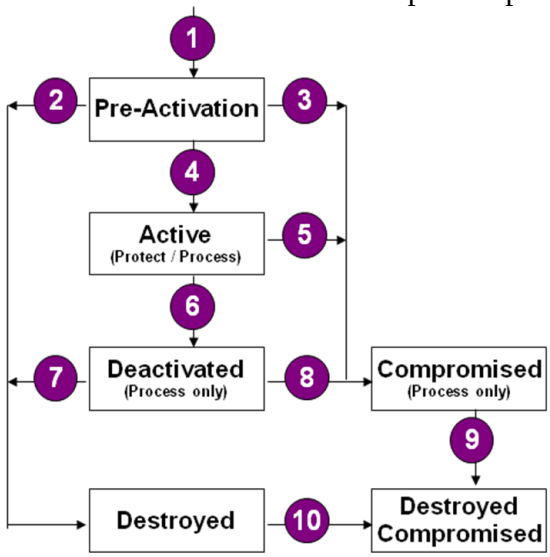
d. 1% for: Signature first, then encryption.
1% for: In case of dispute, some third party must view the message and its signature. If the signature is calculated on an encrypted message, then the third party also needs access to the decryption key to read the original message, which is problematic. Also, it's always best to sign something that you see; otherwise it's difficult to know what you sign.

Question 5: Key Management and PKI.

a. Mention 4 important key management processes/procedures/steps. (2%)
b. Draw the diagram showing the key states and transitions between them as described by NIST SP800-57. Do not explain the diagram, but only indicate for which states a key can be used for protection and/or processing. (4%)
c. In a network of n users, each pair of users must be able to have authentic and confidential communication with each other. State the number of different keys needed in case of:
   i. Symmetric encryption, (1%)
   ii. Asymmetric encryption, (1%)
   iii. Asymmetric encryption with a PKI consisting of m CAs. (1%)
d. Does self-signing of a root certificate provide any evidence of its authenticity? (1%)

Answer

a. 0.5% each for any 4 of: "generation", "distribution", "storage", "updating", "revoking", "recovering", "archiving", "destroying" and "auditing".
b. 2% for diagram below.
2% for correct indication of protect/process



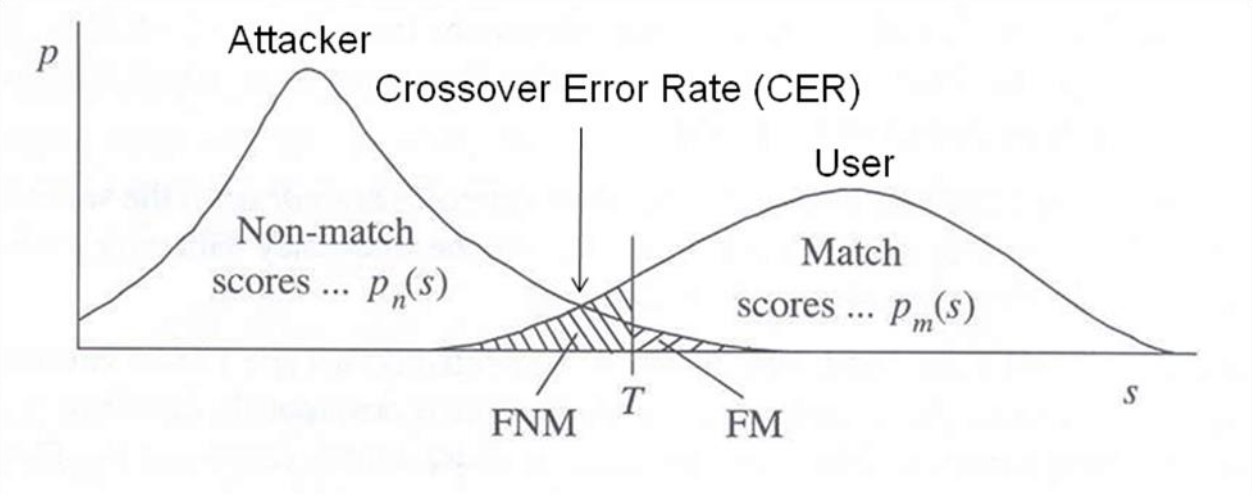
c. 1% for each reasonable answer and assumption:
   i. $n(n\text{-}1)/2$,
   ii. $2n$ (assuming that each user must have 2 keys),
   iii. $2n + 2m$ (assuming that users and CAs must have 2 keys each)
d. 1% for: No!

Question 6: Authentication.

a. Mention two different cryptographic methods of achieving message authentication. (2%)
b. Briefly explain the principle of a *challenge-response protocol*, and mention which specific security service it provides. (2%)
c. Biometric user authentication compares a sample score *s* to a threshold *T* that is tuned to provide a balance between FMR (False Match Rate) and FNMR (False Non-Match Rate). Draw a diagram to illustrate typical attacker score and user score probability distributions, and indicate *T*, FMR, FNMR and the CER (Crossover Error Rate) on the diagram. (4%)
d. The Australian e-Authentication Framework (NeAF) specifies IRAL (Identity Registration Assurance Level) 0. Describe the type of identity registration that IRAL 0 represents, and describe a situation where user authentication combined with IRAL 0 is meaningful. (2%)

Answer

a. 1% each for any 2 of: symmetric encryption, MAC, digital signature,
b. 1% for: A challenge-response protocol is a message exchange between two parties where the verifier challenges the applicant to prove knowledge of secret, by the verifier sending a random number as challenge, and the applicant returning as response the cryptogram of the challenge. This proves knowledge of the secret without exposing the secret in clear.
1% for: It provides user (entity) authentication of the applicant.
c. 4% for something that looks like:



d. 1% for: Anonymous/pseudonymous registration.
1% for: E.g. to provide high sensitivity service to anonymous persons for privacy reasons.

Question 7: Identity and Access Management.

a. Explain 2 common interpretations of "*authorization*", and state which of the interpretations is meaningful and compatible with the definition of confidentiality. (3%)
b. Briefly describe 2 advantages and 2 disadvantages of the silo identity model. (2%)
c. Name the 3 functional steps related to identity and access management that are required during operations before an authorized party gets access to a requested resource. (3%)
d. Briefly describe the concepts of MAC (Mandatory Access Control) and DAC (Discretionary Access Control) as defined by TCSEC (The Orange Book). (2%)

Answer

a. 1% for: Authorization as access request approval, i.e. when the system grants access.
   1% for: Authorization as access policy definition, i.e. to define access privileges.
   1% for: Access policy definition is meaningful and compatible with definition of conf.
b. 0.5% each for 2 reasonable advantages, e.g: Simple to deploy, low cost for SPs
   0.5% each for 2 reasonable disadvantages, e.g: identity overload for users, poor usability
c. 1% each for: identification, authentication, access approval
d. 1% for; Access control based on identity and ACL (Access Control List) or access matrix.
   1% for: Access control based on labels and a hierarchy of security levels

Question 8: Communication Security.

a. Briefly explain the major limitation of HTTP Basic Authentication, and explain how this limitation is overcome in HTTP Digest Authentication. (2%)
b. Explain the purpose of the TLS Handshake Protocol (without sequence diagram). (2%)
c. Mention the security services provided by the TLS Record Protocol. (2%)
d. Encapsulating Security Payload (ESP) is an IPSec protocol that can run in transport mode or in tunnel mode. Explain the main difference between these two modes. (2%)
e. Suppose that you are responsible for application security at an online bank, and that you have been asked to consider three alternative mechanisms for providing confidentiality in the client-server communication: *HTTP Digest Authentication*, *TLS* or *IPSec*. State the most suitable mechanism, and briefly explain why the two others are inadequate? (2%)

Answer

a. 1% for: In basic authentication the password is sent in cleartext over the network and so can be easily obtained by an eavesdropper.
   1% for: In digest authentication a challenge-response protocol with a random challenge is used so each response is unique. It proves knowledge of password without revealing it.
b. 2% for: TLS Handshake Protocol negotiates crypto parameters, establishes session key and authenticates server (optionally authenticates client).
c. 2% for: TLS Record Protocol provides message confidentiality and message integrity
d. 1% for: In transport mode the data is encrypted without the IP header, and the original IP header is used as the packet header after some fields in the original IP header are changed.
   1% for: In tunnel mode the entire original packet is encrypted and a new outer IP header is added. The inner IP header of the original IP packet carries the ultimate source and destination addresses. The outer IP header may contain IP address of security gateway.
e. 1% for: TLS
   1% for: HTTP Digest does not provide confidentiality. IPSec would require distribution of keys by the bank and configuration of clients, which would be logistically difficult.

Question 9: Digital Forensics.

a. Briefly explain the concept of *Chain of Custody*. (1%)
b. Explain the meaning of OOV (order of volatility), and explain how it influence decisions regarding the preservation of forensic evidence. (2%)
c. Explain the difference between “live acquisition” and “post mortem acquisition”. (2%)
d. State one advantage and one disadvantage of live acquisition. (2%)
e. State one advantage and one disadvantages post mortem acquisition. (2%)
f. Give an example when “live acquisition” is necessary. (1%)

Answer

a. 1% for: Chain of custody refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.
b. 2% for: Data stored on media can be modified or erased due to various factors. The volatility expresses the rapidity and ease with which such factors can modify or erase data. The OOV expresses the relative ranking of media according to volatility.
c. 1% for: In case of live acquisition, the evidence is collected from a system where the microprocessor is running.
   1% for: In case of post mortem acquisition, the evidence is collected from storage media of a system that is shut down.
d. 1% for: Post mortem provides better integrity preservation and does not influence data.
   1% for: However, volatile data can be lost in the process of shutting down a system.
e. 1% for: Live acquisition enables the collection of volatile data.
   1% for: However, live acquisition also influences the data.
f. 1% for: In case of encrypted HD it is better to collect the data from the HD while running.

Question 10: Privacy and Regulatory Requirements.

a. Briefly explain 2 of the privacy principles from the 1980 OECD privacy guidelines. (4%)
b. Give the name of the EU directive on data privacy, and its year of publication. (2%)
c. Briefly explain the principle of the Safe Harbour program relating to data privacy. (2%)
d. What is the purpose of the EU Data Retention Directive of 2006? (1%)
e. In case of conflict between data retention legislation and pre-existing privacy legislation, how is this conflict usually resolved? (1%)

Answer

a. 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 fulfilment 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

b. 2% for: The EU Data Protection Directive, 1995 (+/- 2 years).
c. 2% for: Safe Harbour is a voluntary program that companies can opt into by adhering to the 7 principles of the EU Data Protection Directive. EU countries are allowed to export personal info to companies that adopt the Safe Harbour program.
d. 1% for. The EU Data Retention Directive of 2006 mandates member states to enact laws requiring storage of citizens' telecommunications data for 6 to 24 months, in order to support investigations of criminal and terrorist activities.
e. 1% for: Data retention needs are considered more important than privacy needs, so data retention wins and privacy is ignored.