UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

Exam in	**INF3510 – Information Security**
Day of exam:	**08 June 2012**
Exam hours:	**14:30h – 18:30h**
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.

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 sentence to describe each concept that the question asks for.

Question 1: General Security Concepts.

a. Write the definition of confidentiality (approximately) according to X.800. (2p)
b. Explain authorization in a way consistent with the definition of confidentiality, and mention in which of the access control phases this form of authorization belongs (2p).
c. Write the definitions (approximately) of the 2 authentication types according to X800.(4p)
d. Explain whether data confidentiality can provide data integrity and authentication. (2p)

Answer

a. 2p for: Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
b. 1p for: Authorization is to specify access control policy definition, or in other words to define access privileges
   1p for: Authorization takes place in the registration phase.
c. 2p for: Data origin authentication is the corroboration or (proof, verification etc.) that the source of data received is as claimed.
   2p for: Peer-entity authentication is the corroboration (or proof, verification etc.) that a peer entity in an association is the one claimed.
d. 1p for: Normally when data is encrypted for confidentiality, a breach of integrity will be discovered because the data can not be decrypted correctly, i.e. the decrypted data will be meaningless. But in some cases (e.g. with stream ciphers or when using ECB mode) it might be possible to change small portions of encrypted data in a way that the decrypted data is still meaningful, so that the breach of integrity will not be discovered. Encryption alone therefore provides a relatively weak form of data integrity.
   1p for: If it is assumed that the data is encrypted with a secret key known only to the sender and recipient, then encryption normally also implies authenticity, but the same exception as above also applies here. Encryption alone therefore provides a relatively weak form of data authenticity.

Question 2: Risk Management and Business Continuity Planning.

a. Explain the concepts of threat, vulnerability and risk. (3p)
b. Assume that threat impact is expressed as: *Nil, Minor, Moderate, Major,* and that threat likelihood is expressed as: *Never, Low, Medium, High*. Draw a diagram for semi-quantitative risk estimation based on these impact and likelihood categories. (2p)
c. Briefly explain the purpose of BCP (Business Continuity Planning) and why it is necessary to consider it separately from risk management. (2p)
d. Briefly explain the BCP concepts: *Redundant Site, Hot Site, and Cold Site* with respect to equipment installed and typical time it takes to be operable (3p)

Answer

a. 1p for: Threat is a security incident with potential negative impact
   1p for: Vulnerability is a property of an asset which makes threat occurrence possible.
   1p for: Risk is the expected negative consequence resulting from the combination of
   Likelihood of threat occurrence, vulnerability to threat, and impact of threat.

b. 2p for something like table below. No need for verbal risk categories, just numbers is OK. Other numbers than 0,1,2,3 is also OK. The important point is the product rule.

Semi-Quantitative Risk Matrix		Consequence			
		Nil (0)	Minor (1)	Moderate (2)	Major (3)
Likelihood	High (3)	0	3	6	9
	Medium (2)	0	2	4	6
	Low (1)	0	1	2	3
	Never (0)	0	0	0	0
0: No Risk, … 9: Extreme Risk					

c. 1p for something like: BCP is the preparation for restoring normal business functions after disruption caused by major or catastrophic incidents.
   1p for: It is meaningless to assess the likelihood of a disaster, so that traditional risk assessment is not applicable. A business needs BCP in order to survive a disaster.

d. Redundant site:
   0.5p for: Mirror of the primary processing environment
   0.5p for: Operable within minutes
   Hot site:
   0.5p for: Fully configured hardware and software, but no data
   0.5p for: Operable within hours
   Cold site:
   0.5p for: Basic electricity and plumbing
   0.5p for: Operable within weeks

Question 3: Computer Security.

a. There are two main architectures for OS virtualization, typically named Type 1 and Type 2 VM (Virtual Machine) architecture. Make one diagram for each architecture, with all the abstraction layers from hardware to the application layer included. (3p)

b. Indicate in diagram(s) how protection ring -1 can be used, wherever appropriate. (1p)

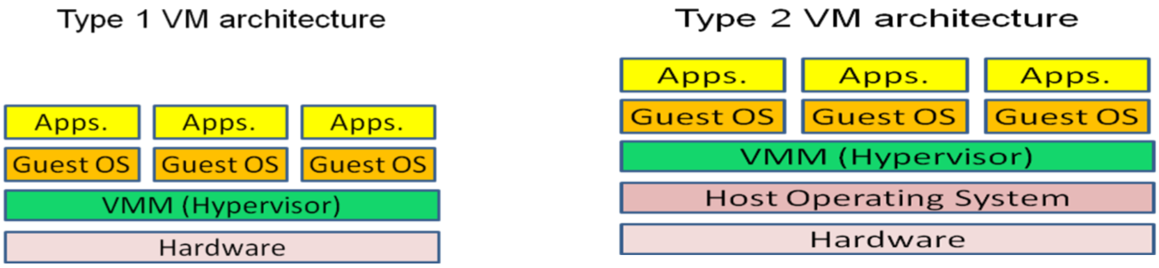
c. Mention one advantage and one disadvantage of both Type 1 and 2 VM architectures. (2p)

d. What is the difference between TCSEC (Trusted Computer System Evaluation Criteria) and CC (The Common Criteria) regarding how functional security requirements and assurance levels are related? (2p)

e. The Common Criteria (CC) for security evaluation uses specific terms. Define the terms:
   i) *"Security Target"* (ST), (1p)
   ii) *"Protection Profile"* (PP). (1p)

Answer

a. 1p for each correct diagram,
1p for correctly assigning Type 1 and Type 2 names to each architecture.



b. 1p for: Protection ring -1 can be assigned to the hypervisor in Type 1 VM architecture.

c. 0.5p for: Advantage of Type 1 VM, e.g. **high performance**
0.5p for: Disadvantage of Type 1 VM, e.g. **limited GUI**
0.5p for: Advantage of Type 2 VM, e.g. **good GUI**, **better HW support**
0.5p for: Disadvantage of Type 2 VM, e.g. **performance penalty**

d. 2p for: Functionality and assurance aspects are independent. Possible to have simple functionality with high assurance, or to have rich functionality with moderate assurance

e. 1p for: ST: An implementation-dependent specification of security needs for a TOE.
1p for: PP: An implementation-independent specification of security needs for a TOE.

Question 4: Cryptography.

a. Draw a diagram showing the taxonomy of cipher algorithms. (2p)

b. What are the possible key sizes of the DES and AES block ciphers? (2p)

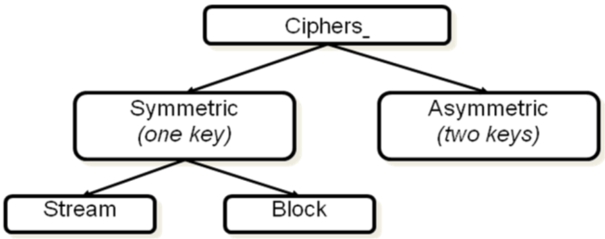
c. There are several different modes of operation for block ciphers. State the meaning of the two abbreviations *ECB Mode* and *CBC Mode*. (2p)

d. Draw a diagram showing the operation of the CTR Mode (Counter Mode) (2p)

e. Briefly explain the principle of hybrid cryptosystems and their advantage. (2p)

Answer

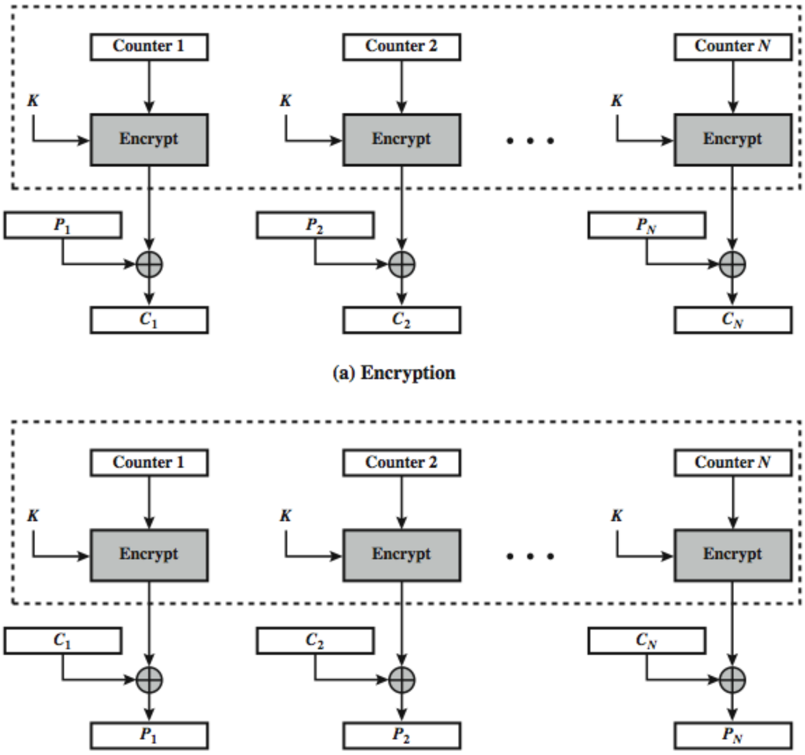
a. 2p for diagram like:



b. 0.5p for: DES, 56 bit key
0.5p each for: 128, 192 and 256 bit key

c. 1p for: ECB Mode: Electronic Code Book Mode
1p for: CBC Mode: Cipher Block Chaining Mode

d. 2p for: Fully correct diagram of CTR Mode, 1p for partially correct diagram.



(a) Encryption

(b) Decryption

e. 1p for: Hybrid cryptosystems use a combination of public-key and secret-key algorithms. 1p for: Advantages: Key management of public-key, and speed of secret-key algorithms.

Question 5: User Authentication.

a. Mention three categories of credentials for user authentication. (3p)

b. Describe the principle of HTTP Digest Authentication (2p)

c. Briefly explain how biometrics can be used for authentication, including how the system decides whether a user is authentic or not. (3p).

d. How many different authentication assurance levels (AALs) are specified in the Norwegian e-Authentication framework? (1p)

e. Which AAL can be supported by the current Norwegian BankID system? (1p)

Answer

a. 1p each for any 3 of: 1) Something you know, 2) something you have, 3) something you are, 4) something you do

b. 2p for: Server sends nonce. User provides password to client. Client computes hash which is returned to server: Password digest = H(nonce, user Id, password)

c. 3p for: Features captured by system are compared against the stored template. Score s is derived from the comparison, where better match leads to higher score. Decision depends on threshold T: Considered authentic (i.e. correct person) when s ≥T. Considered not authentic (i.e. different person) when s < T.

d. 1p for: 4

e. 1p for: AAL 3

Question 6: Identity and Access Management.

a. Briefly explain the following concepts related to identity management.
   (i) Entity. (1p)
   (ii) Identity. (1p)
b. Briefly explain what is meant by the concept “identity management”. (2p)
c. Briefly describe the federated model for management of user identities. (2p)
d. Briefly describe the concepts of MAC (Mandatory Access Control) and DAC (Discretionary Access Control) as defined by TCSEC (The Orange Book). (2p)
e. Briefly describe the purpose of OAuth (Open Authorization). (2p)

Answer

a. The meaning of the concepts:
   1p for: Entity: A person, organisation, agent, system, etc.
   1p for: Identity’: A set of attributes of an entity in a domain, where name is an attribute
b. 2p: Identity management consists of representing and recognising entities as digital identities, for managing name spaces, for assigning unique names to entities, for assigning access credentials/tokens to entities, and provides a basis for Authorization, Authentication, Access Control and Accounting.
c. 2p for: Identity Federation: A set of agreements, standards and technologies that enable a group of SPs (service providers) to recognise user Ids and entitlements from other SPs.
d. 1p for; DAC: based on identity and ACL (Access Control List) or access matrix.
   1p for: MAC: based on labels and a hierarchy of security levels.
e. 2p for; OAuth provides a way to grant access to your user data stored on a specific website *A* to a third party website *B*, without needing to provide this website *B* with your authentication credentials for accessing website *A*.

Question 7: Communication Security.

a. Roughly explain how TLS enables client and server to establish a secret session key in the case where the server sends a server certificate to the client. (2p)
b. Assume a TLS connection with data encryption using secret key established with server certificate. Mention which security services are provided by this TLS connection. (2p)
c. Mention the three major VPN architectures supported by IPSec, and briefly describe a typical application scenario for each architecture. (6p)

Answer

a. 2p for: Client receives server certificate, extracts and validates server public key. Client then generates a secret that is encrypted with public key, and returned to the server. The server decrypts secret with server private key. So client and server share a secret.
b. 2p for: Confidentiality, Integrity, server entity authentication.
c. The major VPN architectures are:
   1p for: Gateway-to-Gateway Architecture.
   1p for: Most often used when connecting two secured networks, such as linking a branch office to headquarters over the Internet.
   1p for: Host-to-Gateway Architecture.
   1p for: Most often used when connecting hosts on unsecured networks to resources on secured networks, such as linking travelling employees around the world to headquarters over the Internet.
   1p for: Host-to-Host Architecture.
   1p for: Typically used for special purpose needs, such as system administrators performing remote management of a single server.

Question 8: Perimeter Security.

a. Mention the main characteristics of a packet filter firewall and an application gateway firewall, as well as one main advantage and disadvantage of each type of firewall.(4p)

b. How can a firewall inspect encrypted TLS traffic payload ? (2p)

c. Mention one strength and one weakness of misuse-based IDS and of anomaly-based IDS (Intrusion Detection Systems). (4p)

Answer

a. 1p for: A packet filter examines header of each packet that attempts to pass through the filter. Stateful packet filters take account of the current state of a connection. Decisions are based on packet's header attributes.
1p for: Packet filters are fast, but only allows relatively primitive filtering rule.
1p for: Application level gateway is a network application proxy that inspects application level traffic. Decisions are based on payload, packet header, and connection state.
1p for: Application level gateway firewalls can support deep inspection of application traffic, but are relatively slow.

b. 2p for: The firewall must be an application gateway with a TLS proxy. It requires the organisation to set up an internal PKI and issue internal proxy server certificates for every external TLS server that internal users access.

c. IDS advantages and disadvantages:
1p for any relevant advantage of Misuse Based IDS such as:
– Fast, only way to detect known intrusions at runtime
– Have more True Positive results than False Positive results. Fewer false alarms
1p for any relevant disadvantage of Misuse Based IDS such as:
– Can't detect new attacks that don't match existing signatures.
– Requires manual administration. Must have signatures constantly updated
– Can be fooled (e.g: use of fragmented packets if the IDS does not de-fragment traffic)
– In DoS attacks, the IDS can be overwhelmed so that it cant function correctly.
1p for any relevant advantage of Anomaly Based IDS such as:
– Can detect new attacks by identifying unusual behaviour
– Information from anomaly based IDS used to develop signatures for misuse based IDS
1p for any relevant disadvantage of Anomaly Based IDS such as:
– Usually generate many false positives (false alarms)
– Usually require a lot of training and tuning to define models of normal behaviour

Question 9: Digital Forensics.

d. Briefly explain the concept of *Chain of Custody*. (1p)

e. Explain the meaning of OOV (order of volatility), and explain how it influence decisions regarding the preservation of forensic evidence. (2p)

f. Explain the difference between *live acquisition* and *post mortem acquisition*. (2p)

g. Mention one advantage and one disadvantage of live acquisition. (2p)

h. Mention one advantage and one disadvantages post mortem acquisition. (2p)

i. Mention one example when "live acquisition" is necessary. (1p)

Answer

d. 1p 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.

e. 2p 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.

f. 1p for: In case of live acquisition, the evidence is collected from a system where the microprocessor is running.
1p for: In case of post mortem acquisition, the evidence is collected from storage media of a system that is shut down.

g. 1p for: Post mortem provides better integrity preservation and does not influence data.
1p for: However, volatile data can be lost in the process of shutting down a system.

h. 1p for: Live acquisition enables the collection of volatile data.
1p for: However, live acquisition also influences the data.

i. 1p for: In case of encrypted HD it is better to collect the data from the HD while running.

Question 10: Operations Security.

a. Briefly explain the principle of SQL injection attack, and mention one relevant method for preventing SQL injection attack. (3p)

b. Briefly explain the principle of XSS (Cross Site Scripting) attacks, and mention one relevant method for preventing XSS attacks. (3p)

c. Briefly explain two essential elements in the activity data backup (2p)

d. Briefly explain two methods of secure data destruction. (2p)

Answer

a. 2p for: SQL injection is an attack against databases whereby the attacker provides SQL commands instead of normal data as input to an application that sends it to a database. The attacker can thus trick the application to execute SQL commands of his choice.
1p for: SQL injection attacks can be prevented by not allowing user input to be directly embedded in SQL statements. Instead, parameterized statements must be used, or user input must be carefully escaped or filtered.

b. 2p: Cross-Site Scripting: (Acronym XSS) is an attack technique whereby the attacker provides script code instead of normal data as input to a web site that reflects this input to other client browsers accessing the web site. This enables the attacker to place scripts of his choice in client browsers accessing the website. XSS attacks do not typically directly target the web server or application, but are rather aimed at the clients. The web server is merely used as a conduit for the XSS data to be presented to the end clients.
1p for: XSS can be prevented by always sanitizing input to web servers.

c. 1p each for any two elements of
- Taking backup copy data at regular intervals
- Protection of backup media on-site
- Off-site storage of backup media
- Testing of data restoration from backup copy

d. 1p each for any two methods of:
- Zeroisation/wiping/shredding: Overwrite media with dummy data
- Degaussing: Strong magnetic field that reorients atoms on media
- Physical destruction: melting, wrecking of media