Name: ____________________________ **İTÜ ID:** ____________________ **Signature:** ________________.

BLG 439 Bilgisayar Proje I (Computer Security)

Fall 2013, Midterm Exam - Solutions

04.11.2013, Duration: 90 minutes

Instructions : *This is a closed-book exam. No electronic devices are allowed. Please give your answers in English. Write your answers in the spaces provided for each question.*

Q-1	Q-2	Q-3	Q-4	Q-5	Q-B	Total
/3.5	*/7*	*/7*	*/6.5*	*/6*	*/5*	*/30*

Q-1. (3.5 pts) Computer security basics

a) (1.5pts) What are the key objectives of computer security? Write only names of the objectives. *(Hint: The objectives are also known as the security requirement triad.)*

Confidentiality, Integrity, Availability

b) (2 pts) Give brief definitions of security service and security mechanism. Explain them if you feel that it is necessary.

Security service enhances the security of the data processing systems and the information transfers of an organization. Security mechanism is designed to detect, prevent, or recover from a security attack.

Q-2. (7 pts) Cryptography

a) (1 pt) What is cryptography? Explain briefly.

Cryptography is a study of secret writing to ensure secure systems in the presence of adversaries.

b) (2 pts) Compare symmetric key encryption and public-key encryption in terms of keys used.

In symmetric key encryption sender and receiver use the same key (single key or symmetric key or secret key).

In public key encryption sender and receiver use different keys (two keys, public key and private key).

c) (2 pt) Compare Hash functions and MAC (message authentication code) functions in terms of keys.

A Hash function does not use any key whereas a MAC function uses a secret key.

d) (2 pt) Where are random numbers in cryptography used for? Give two of them.

1) nonces in authentication protocols to prevent replay
2) session keys
3) public key generation
4) key stream for stream ciphers

Q-3. (7 pts) Human Factors

a) (2 pts) What are problems associated with employee behavior? Give two of them.

1) Errors
2) Omissions
3) Fraud
4) Actions by disgruntled employees

b) (1 pts) What are goals of awareness programs? Give only two of them.

1) Rise staff awareness in general
2) Ensure that staff are aware of governmental laws and regulations related to security
3) Organizational security policies and procedures
4) Ensure that staff understand the significance of a sole employee
5) Train staff according to their positions
6) Inform staff that they are monitored
7) Remind the consequences of security breaches
8) Teach the significance of reporting
9) Create a trusted system

c) (2 pts) Compare awareness and training according to attribute.

Awareness: provide answers to what is allowed or not allowed but not how
Training: provide answer to how

d) (2 pts) What are the responsibilities of a computer incident response team for large or medium sized organizations? Give two of them.

1) Rapidly detect incidents
2) Minimizing loss and destruction
3) Mitigating the weakness
4) Restoring computer services

Q-4. (6,5 pts) Malware

a) (1,5 pts) What is malicious software?

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

b) (3 pts) List parts of a computer virus.

1. Infection mechanism (also known as infection vector)
2. Trigger (sometime known as logic bomb)
3. Payload (what the virus does)

c) (1 pt) What is a botnet?

A collection of bots can act in a coordinated manner.

d) (1 pt) Write the name of facility that distinguished a bot and a worm.

Remote control facility

Q-5. (6 pts) Authentication and Access Control

a) (2 pts) What are the steps of user authentication? Give only their names.

Identification and Verification

b) (1 pt) Explain the dictionary attacks.

Dictionary attacks: try each word then obvious variants in large dictionary against hash in password file

c) (1,5 pts) List access control principles.

Authentication, authorization, and audit

d) (1,5 pts) List access control elements.

Subject, object, and access right

Q-B. (5 pts) Bonus Question

Assume that Ayşe wants to send a message over an unsecure network to Ahmet. However, she has some concerns about the confidentiality of the message when she uses the network. Therefore, she needs to send the message in a closed form (as a cipher text) by encrypting the message either with symmetric encryption or asymmetric encryption. Ahmet receives and decrypts the message. Describe the process by using

a) (2 pts) symmetric key encryption

M: message
X: cipertext of M
Ks: shared key (symmetric key)

Ayşe X=E(Ks, M) →Ahmet M=D(Ks, X)

b) (3 pts) public key encryption

M: message
X: cipertext of M
PU: Public key of Ahmet
PK: Private key of Ahmet

Ayşe X=E(PU, M) →Ahmet M=D(PK, X)