Name: _____ **İTÜ ID:** _____ **Signature:** _____.

BLG 439E Computer Project I (Computer Security)

Fall 2014, Midterm Exam - Solutions

27.10.2014, Duration: 90 minutes

Instructor: Dr. Şerif Bahtiyar

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. Write your Name and İTÜ ID on the top of each page and sign all pages.*

Q-1	Q-2	Q-3	Q-4	Q-5	Q-6	Q-B	Total
/2.5	/5	/5	/5.5	/5	/7	/7	/30

Q-1. (2.5 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) (1 pt) Which of the following is not the way to protect your assets? Choose the answer.

a) **Prevention**: Prevent your assets from being damaged or stolen.
b) **Attacking**: Attack to the intruder to save your assets.
c) **Detection**: Detect when, how, and by whom an asset has been damaged.
d) **Reaction**: Recover your assets, such as call police or make an insurance claim.

Attacking – A direct interaction with the intruder may have negative results for the owner of assets. Simply, the intruder may kill the owner. Thus, attacking to the intruder is an incorrect way to protect your assets!

Q-2. (5 pts) Cryptography

a) (2 pts) Classify cryptographic systems in terms of the number of keys used.

-Symmetric, single-key cryptographic system: Both sender and receiver use the same key.

-Public-key, two keys cryptographic system: Sender and receiver use different keys.

b) (3 pts) For each of the following sentence, write either TRUE or FALSE. You will get 1 point for each correct answer.

TRUE A hash function accepts a variable size message M as input and produces a fixed size message digest as output.

TRUE Public-key algorithms are based on mathematical functions rather than on simple operations on bit patterns.

FALSE It is very easy to provide true random numbers.

Name: _____ **İTÜ ID:** _____ **Signature:** _____ .

Q-3. (5 pts) Human Factors

a) (2 pts) What are major benefits of security awareness, training, and education programs? Write two of them.

1) Improving employee behavior
2) Increasing the ability to hold the employees accountable for their actions
3) Mitigating liability of the organization for an employee's behavior
4) Complying with regulations and contractual obligations

b) (3 pts) For each of the following sentence, write either TRUE or FALSE. You will get 1 point for each correct answer.

FALSE Security awareness, training, and education programs can reduce fraud.

FALSE The impact of security awareness programs is long.

FALSE Triage function ensures that all information destined for the incident handling service is channeled through multiple focal points regardless of the method by which it arrives for appropriate redistribution and handling within the service. (Single focal point!)

Q-4. (5,5 pts) Malware

a) (1,5 pts) What are the components (parts) of a virus? Write only their names.

Infection mechanism, Trigger, and Payload

b) (1 pt) Which of the following malware actively seeks out more machines to infect, and then each infected machine serves as an automated launching pad for attacks on other machines? Select one of them.

a)Virus b)Spyware c)Trojan horse d)Worm e)Keyloger f)Spam

c) (3 pts) Write a virus (MyVirus) that has the following properties. Use pseudo-code to write the virus. *(Hint: Your virus should contain all essential components (parts) which you provide as the answer for question a.)*

Your virus infects only executable files in root directory (.exe files). The last line of an infected file contains your İTÜ ID. The virus prints message "You are infected by YOUR NAME" at your birthday to the screen. For example, if my birthday is May 2, MyVirus will print "You are infected by ŞERİF BAHTİYAR" to the screen at May 2.

A similar code is in your textbook. You can also find the code on your lecture notes!

Name: _____ **İTÜ ID:** _____ **Signature:** _____ .

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

a) (2 pts) Write types of the user authentication. (means of user authentication based on an individual's ….). Write only their names.

Knows, Possesses, Is, and Does

b) (2 pts)Use appropriate (correct) words to fill the blanks. In ___reactive___ password checking, the system periodically runs its password cracker to find guessable passwords whereas in ___proactive___ password checking, a user is allowed to select a password if the password complies with system requirements at the time of selection.

c) (1 pt) Compare discretionary access control (DAC) policies and mandatory access control (MAC) policies in terms of delegation of access rights to other entities.

In DAC an entity may enable another entity to access resources whereas in MAC an entity cannot enable another entity to access resources.

Q-6. (7 pts) Software and Operating System Security

a) (2 pts) Buffer overflow occurs in a condition under which more input can be placed into a buffer or data holding area than the capability allocated, which may overwrite other data. What are the aims of an attacker to exploit buffer overflow? *(Hint: consider the consequences of possible attacks on a system.)*

-crash the system

-insert specifically crafted code that allows them to gain control of the system.

b) (3 pts) Write principles of handling program outputs.

-Conform expected form

-Validate third-party data

-Be careful with encoding

c) (2 pts) Write the two problems that prevent machine instructions to be correctly implemented for high-level language code.

-Often ignored by developers

- Assume compiler or interpreter work correctly

Name: _____ **İTÜ ID:** _____ **Signature:** _____ .

Q-B. (7 pts) Bonus Question

Assume that students in a class want to communicate with each other over an unsecure network. However, they have some concerns about the confidentiality of communications. Therefore, they need to encrypt the communications. Note that a communication between two students is bidirectional that means both students can send messages to each other.

a) (1 pt) Two students want to ensure confidentiality of the communication between them with the minimum number of keys by using symmetric-key encryption. How many different key(s) should they use to ensure confidentiality? Explain briefly.

Both parties can use the same key to send messages to each other. Only one symmetric-key is adequate.

b) (2 pts) Solve the previous problem with public-key encryption. Explain briefly.

In public-key encryption, a message is encrypted with the public key of a student and the message is decrypted with the private key of the student. Therefore, if student A wants to send a message to student B, student A encrypts the message with public key of student B then student B decrypts the message with its private key. Since a communication between two students is bidirectional, the similar procedure is used to send a message from student B to student A. Therefore, student A has its private key and public key of B, and student B has its private key and the public key of A. Thus, there are totally 4 keys.

c) (2 pts) Consider a class that has 44 students. Each student wants to communicate with other 43 students securely by using symmetric key encryption and with the minimum number of keys. How many different key(s) does the system contain to ensure confidentiality? Explain briefly.

Two students should share one symmetric key that is only known by these students to communicate securely. Since the class contains 44 students, students can form C(44,2)=946 pairs, where each pair can use different symmetric key to communicate. Thus, the system contains 946 different symmetric keys.

d) (2 pts) Solve the previous problem with public-key encryption. Explain briefly.

A student needs its private key and public keys of 43 students to communicate with other students. Since the public key of a student can be used by all other students to send messages to the student, 44 public keys and 44 private keys are adequate to provide confidentiality for all students in the class. Thus, the system contains 88 different keys.