Name: ______________________________ **İTÜ ID:** ____________________ **Signature:** __________________.

BLG 439E Computer Project I (Computer Security)
Fall 2015, Midterm Exam - Solutions
09.11.2015, Duration: 90 minutes
Instructor: Dr. Şerif Bahtiyar

Instructions : *This is a closed-book exam. No electronic devices are allowed. Give your answers in English. Write your answers in the space 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-B	Total
/7	/8	/7	/8	/6	/30

Q-1. (7 pts) For each of the following sentence, write either TRUE or FALSE. You will get 1 pt for each correct answer.

a) FALSE_A loss of integrity is unauthorized disclosure of information.

b) TRUE_Stream ciphers process messages one bit or byte at a time.

c) FALSE_The most in-depth program in security is awareness.

d) TRUE_A worm does not need a host program to execute and propagate.

e) TRUE_In password based authentication, salt prevents duplicate passwords in the password file.

f) TRUE_Access control is the prevention of unauthorized use of a computer system's resources.

g) FALSE_Incorrect handling of program input is not a common failings in software security.

Q-2. (8 pts) Use appropriate (correct) words to fill the blanks.

a) (1 pt) A hash function accepts a____variable___size message M as input and produces a____fixed_____size message digest as output H(M).

b) (1 pt) Triage function ensures that all information destined for the incident handling service is channeled through a single _____focal point_____regardless of the _____method_____by which it arrives for appropriate redistribution and handling within the service.

c) (1 pt) 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.

d) (1 pt) A polymorphic virus creates copies during replication that are functionally _______equivalent______ but have distinctly (not fully) _______different_____bit patterns.

e) (1 pt) Attack agent payloads of malware targeted ___integrity____ and ___availability____ of the infected system.

f) (1 pt) In Cross-Site Scripting (XSS) attacks, __input___ from one user is later __output___ to another user.

g) (1 pt) In password based user authentication method, users provide ___name____ and ___password___ to the system.

h) (1 pt) Security vulnerability is a flaw or weakness in a system's _______design______ and _______implementation (or operation and management)_________ that could be exploited to violate the system's security policy.

Name: ______________________________ **İTÜ ID:** ______________________ **Signature:** _________________.

Q-3. (7 pts) Short questions.

a) (1 pt) Write only two 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) What are major benefits of security awareness, training, and education programs? Write only 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

c) (1 pt) What are the requirements for effective malware countermeasures? Write only two of them.

1. Generality: The approach taken should be able to handle a wide variety of attacks.
2. Timeliness: Respond quickly.
3. Minimal denial-of service costs
4. Transparency: Should not require modification to existing system.
5. Global and local coverage: Deal with attack sources both from outside and inside the enterprise network.

d) (1 pt) List only two components (parts) of a virus?

Infection mechanism, Trigger, and Payload

e) (1 pt) What are the steps of user authentication process?

Identification and Verification

f) (1 pt) Write two principles of handling program outputs.

1. Conform expected form**:** Output does conform to the expected form and interpretation.
2. Validate third-party data**:** Any programs that gather and rely on third-party data have to be responsible for ensuring that any subsequent use of such data is safe and does not violate the user's assumptions.
3. Be careful with encoding: Different character sets allow different encodings of meta characters, which may change the interpretation of what is valid output.

g) (1 pt) Explain privilege escalation briefly.

Privilege escalation is to enable an attacker to have privileges greater than those already available to the attacker.

Q-4. (8 pts) Problems

Assume that an e-commerce platform ensures customers who have accounts in financial institutions to buy goods from online stores. The financial institutions support electronic payment options. In this problem, assume that a customer wants to buy books from a book store which is connected the e-commerce platform. The customer has three different payment options (services) for electronic commerce transactions, which options are **debit**, **credit**, and **bonus**. Specifically, the user can select among these options for payment via the e-commerce platform. Additionally, the platform provides three different access rights for payment options. The access rights are **forbidden**, **limited**, and **unlimited**. For instance, a user may have an unlimited access right for payments with credit (unlimited access right to credit service) whereas another user may have a limited access right for such payments. Assume also that the e-commerce platform has an access control mechanism that manages access permissions of users to the payment options.

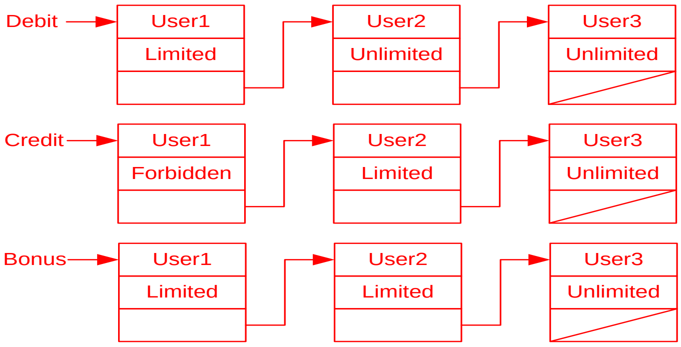
In this scenario, there are three users who have accounts on a specific financial institution, namely **User1**, **User2**, and **User3**. Moreover, each user has different access permissions. **Access permissions for User1 are debit (limited) + credit (forbidden) + bonus (limited), for User2 are debit (unlimited) + credit (limited) + bonus (limited), and for User3 are all unlimited**.

Solve the following problems according to the e-commerce platform described above. Assume that the infrastructure is secure! Do not consider any attack!

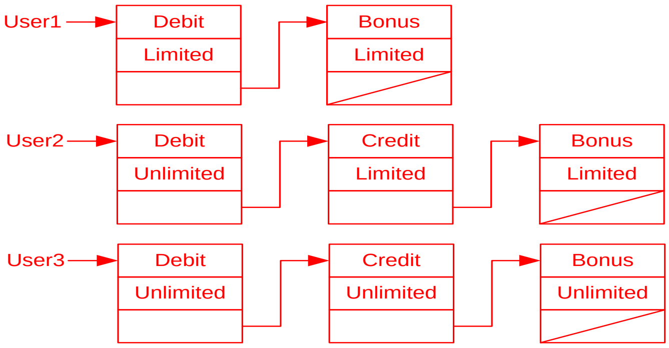
a) (4 pts) Represent (write) the access control system by using **access control matrix**.

	Debit	Credit	Bonus
User1	Limited	Forbidden	Limited
User2	Unlimited	Limited	Limited
User3	Unlimited	Unlimited	Unlimited

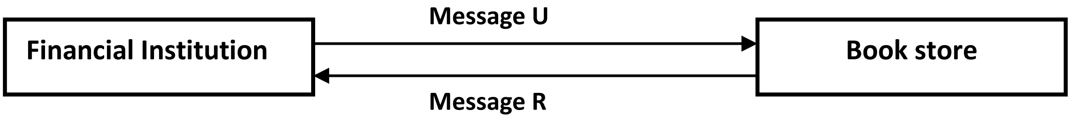
b) (2 pts) Represent (write) the access control system by using **access control list**.



c) (2 pts) Represent (write) the access control system of the client-side digital wallet by using **access control capability tickets**.



Q-B. (6 pts) Bonus Question



Consider the scenario explained in **Q-4**. The cost of payments for e-commerce transactions depends on the amount of interactions between the payment network and participants of e-commerce platforms. To reduce the cost, some security services are provided between financial systems and retailers. In this scenario, there is a financial institution and a book store as a retailer as shown in the figure above. Assume that non-repudiation service of message sender (origin) for both the financial institution and the book store are provided with digital signatures. Origin non-repudiation service proves that the message was sent by the specified party.

Write digital signatures for Message U and Message R and then write verifications of the signatures. **Use public key cryptography for digital signatures.** **Assume that keys are distributed securely (no key distribution problem). Note that the financial institution sends Message U with its signature and the book store sends Message R with its signature!**

PR_{FI}: Private Key of the Financial Institution PU_{FI}: Public Key of the Financial Institution

PR_{BS}: Private Key of the Book Store PU_{BS}: Public Key of the Book Store

E: Encryption D: Decryption

Financial Institution		Book Store .
SignatureFI=E(PR_{FI}, Message U)	→	VerifyFI=D(PU_{FI}, SignatureFI)
VerifyBS=D(PU_{BS}, Signature BS)	←	SignatureBS=E(PR_{BS}, Message BS)