The Open University of Sri Lanka
Faculty of Natural Sciences
BSE Honours Degree Programme

809

Department	: Computer Science
Level	: 3
Name of the Examination	: Final Examination
Course Title and - Code	: Computer Security Concepts – COU3305/CSI3361
Academic Year	: 2021/22
Date	: 19/11/2022
Time	: 9.30am – 12.30pm
Duration	: Three(3) hrs.

General Instructions

1. Read all instructions carefully before answering the questions.
2. This question paper consists of **six(6)** questions in **four(4)** pages.
3. Answer any **four(4)** questions only. All questions carry equal marks.
4. Answer for each question should commence from a new page.
5. Draw fully labelled diagrams where necessary
6. Involvement in any activity that is considered as an exam offense will lead to punishment
7. Use blue or black ink to answer the questions.
8. Clearly state your index number in your answer script

QUESTION 1

1.1) Define the following terms in security.

i) Privacy
ii) Integrity
iii) Accessibility

1.2) Name three (3) computer security best practices followed by employees of an IT organization.

1.3) List three (3) TEMPEST countermeasures of Emanation security.

1.4) How the *Diversity of defense* technique improve the protection provided by *Defense in Depth* technique?

1.5) Define each component of CIA Triad. List three (3) preserving methods for each component.

QUESTION 2

2.1) Define the following terms in Risk Management.

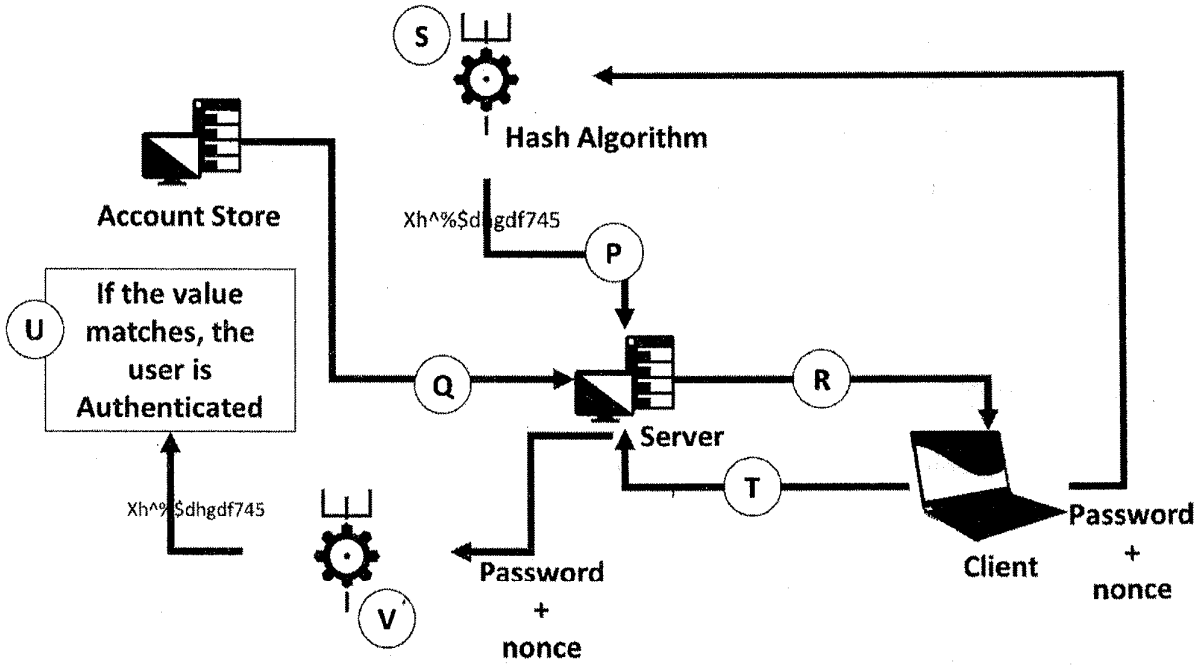
i) Risk management
ii) Threat vector
iii) Qualitative risk assessment
iv) Quantitative risk assessment

2.2) What is known as Threat *Likelihood*?

2.3) Briefly explain the following Risk related terms.

i) Avoidance
ii) Transference
iii) Acceptance
iv) Mitigation
v) Deterrence

2.4) Following diagram shows the operating procedure of digest authentication. What are the steps of *digest authentication* as depicted by the labels **P to V?**



2.5) Discuss the difference between *Authentication* and *Authorization*.

QUESTION 3

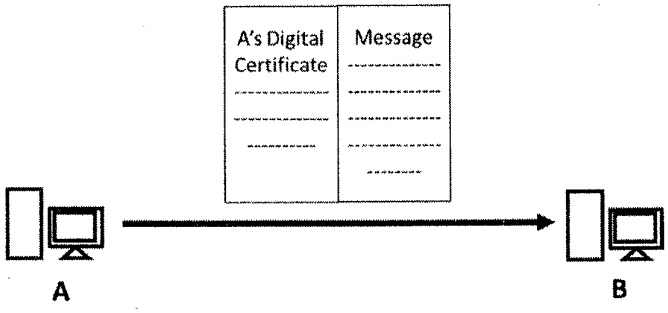
3.1) Define the following terms;

i) Mandatory Access Control (MAC)
ii) Discretionary Access Control (DAC)
iii) Role-Based Access Control (RBAC)

3.2) Name and describe the phases of "*Lockheed Martin's Intrusion Kill Chain*".

3.3) Differentiate between *Confidentiality Model* and *Integrity Model* with examples for each model.

3.4) Briefly explain the steps for verifying the authenticity and integrity of a digital certificate attached to a digitally signed message using a diagram. Consider the example of A sends a message to B.



3.5) Briefly explain *Hierarchical Trust Model* with its main components. Use a diagram if necessary.

QUESTION 4

4.1) List two (2) differences between *Passive Reconnaissance* and *Active Reconnaissance*.

4.2) What is a computer virus? Briefly explain the behavior of the following virus types.

i) Boot Sector Virus
ii) Macro Virus
iii) Armoured Virus

4.3) Briefly describe the impact of *SYN flooding* and *Ping of Death (POD)* attacks.

4.4) Define the following terms stated as attacker's goals with an example.

i) Theft
ii) Vandalism
iii) Espionage

4.5) What is Social Engineering attack? Give four (4) methods to avoid a social engineering attack.

QUESTION 5

5.1) Who is an Insider in the context of information security? Name the types of insider threats.

5.2) Name four (4) types of *Hacktivism*. Briefly explain them.

5.3) Define the following terms in Personally Identifiable Information (PII).

i) Notice
ii) Choice
iii) Consent

5.4) Describe the uses of following components in Secure Communication Protocols.

i) IPsec
ii) Signal Protocol
iii) Secure Remote Procedure Call (S-RPC)

5.5) Briefly explain *Covert Timing Channel* and *Covert Storage Channel*.

QUESTION 6

6.1) What are the level labels under category A to D as defined by the *Trusted Computer System Evaluation Criteria (TCSEC)?* Briefly describe them.

6.2) List the Common Criteria (CC) evaluation assurance levels.

6.3) Compare TCSEC, ITSEC and CC security evaluation standards.

6.4) Briefly explain *Certification* and *Accreditation*.

6.5) Briefly explain how to build a *High Ethical Organization* Environment.

------- End of the Paper -------