CSE 543 First Exam

Due Oct 6 at 7:30pm **Points** 100 **Questions** 6
Available after Oct 6 at 6pm **Time Limit** 75 Minutes

Instructions

CSE 543 Information Assurance and Security

Classroom: CAVC-351

Fall 2022

First Examination

Professor Stephen S. Yau

Date: October 6, 2022

Time: 6:00 p.m. - 7:15 p.m.

Duration: 75 minutes

Total: 100 Points

Read the following rules and relevant instructions for the exam carefully before starting to take the exam:

Instructions for all student modes:

1. The exam is an open book exam. Therefore, answers being sourced from materials outside the lecture slides must be in your own words (paraphrased), not directly quoted or cut-and-pasted from the outside materials or lecture slides. You are not allowed to collaborate with other students or ask for help from anyone during the exam. You must also keep your answers secured, not accessible by other students. Violation will be considered a serious offense to academic integrity, and an appropriate penalty will apply.

Mode 1 - Paper-based exam:

- Must take the exam in person and in classroom using pen and paper

Mode 2 - Computer-based exam in classroom:

- Must take the exam in person and in classroom using your personal computer and your computer must be fully charged.

Mode 3 - Computer-based exam over Zoom.

- Take at home using your personal computer, must turn on your camera on your personal computer and remain in view of the camera at all time without disruption throughout the exam.

Exam Instructions for Mode 1:

1. The exam questions will be provided on the exam paper. This exam will be made available at 6 p.m. on October 6, 2022.
2. You must write your answers on the space provided in the exam paper during the exam. The exam paper must be submitted no later than 7:15 p.m. on October 6, 2022, to the TA.
3. If you have any questions during the exam, you can raise your question to TA or me in the classroom.

Exam Instructions for Mode 2:

1. The exam questions will be posted through the Canvas (in the Quiz section) in the same format as a regular exam paper in an in-person exam. This exam will be made available at 6 p.m. on October 6, 2022.
2. You must type your answers in the space provided to answer each question in the Canvas Quiz section. All answers to the exam questions must be submitted no later than 7:15 p.m. on October 6, 2022 (the submission link will be automatically closed at 7:15 pm).
3. If you have any questions during the exam, you can raise your question to TA or me in the classroom.

Exam Instructions for Mode 3:

1. The exam questions will be posted through the Canvas (in the Quiz section) in the same format as a regular exam paper in an in-person exam. This exam will be made available at 6 p.m. on October 6, 2022.
2. You must type your answers in the space provided to answer each question in the Canvas Quiz section. All answers to the exam questions must be submitted no later than 7:15 p.m. on October 6, 2022 (the submission link will be automatically closed at 7:15 pm).

3. You must ensure that you have a stable internet connection to Canvas throughout the exam period.

If you have any questions during the exam, you should send a clear, concise short message to the TA and me through zoom or through email, then the TA or I will answer your questions through the zoom or email.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	74 minutes	80 out of 100

ⓘ Correct answers are hidden.

Score for this quiz: **80** out of 100
Submitted Oct 6 at 7:14pm
This attempt took 74 minutes.

Question 1

18 / 20 pts

(a) (10 pts) Identify as many principles as possible to protect confidential information of an organization from unauthorized disclosure to any subject (inside or outside the organization).

(b) (10 pts) For each principle identified in (a), give the reason(s) why the principle will prevent protect sensitive information of an organization from unauthorized disclosure to any subject (inside or outside the organization).

Your Answer:

(1.a)

1. **Encryption**
2. **Two-factor authentication**:
3. **Safeguard your keys**
4. **Auditability**
5. **Access Control**
6. **Confidentiality**

7. **Non-disclosure Agreements**
8. **Training and Awareness**
9. **Authentication**
10. **Secrecy**

(1.b)

1. **Encryption**: Any third party who obtains the data will not be able to read it because of the encryption, hence preventing the sensitive information from unauthorized access.
2. **Two-factor authentication**: By requiring two-factor authentication, data security is improved and the chance of data leaks is reduced. You can only access the information using two-factor authentication if you have both a material object (like a card) and an immaterial one (like a security code).
3. **Safeguard your keys**: Access to the keys means access to the information, hence a safety measures should be taken to safeguard and preserve keys to a secure location be it physical keys or software keys. Only Authorized person will have access to keys hence to the organization.
4. **Auditability**: When a technology team conducts an organizational assessment to confirm that the correct and most recent procedures and infrastructure are being used, it results in an information security audit. A series of tests that are part of an audit ensure that information security satisfies all standards and specifications inside an organization. Employees are questioned about their security responsibilities and other pertinent information during this process.
5. **Access Control**: Who is permitted to access and use firm information and resources is determined by access control, a key element of data security. Access control rules ensure users are who they claim to be and have authorized access to company data through authentication and authorization. Additionally, physical access to campuses, buildings, rooms, and datacenters can be restricted using access control.
6. **Confidentiality**: Privacy and confidentiality are similar concepts. Protecting sensitive information from unwanted access is the goal of confidentiality measures. It is common practice to categorize data based on the extent and nature of the harm that may be caused if it got into the wrong hands. Then, based on those classifications, more or less strict controls can be put in place.

7. **Non-disclosure Agreements**: Trade secrets and other sensitive information cannot be revealed without the consent of both parties, according to a confidentiality or non-disclosure agreement (NDA).
8. **Training and Awareness:** Educating employees about security and making them aware about the hacking attacks can majorly contribute to prevent phishing attacks.
9. **Authentication:** Authenticating users to system via username password or any login method can limit the access to authorized personnel only.
10. **Secrecy:** Using techniques like cryptography or computer access control we can limit the access to data to Authenticated users or user group.

(a) -1 missing information (b) -1 missing information

Question 2

14 / 21 pts

(a) (10 pts) What are the three types of security strategies for an organization to protect its confidential information? What are the strengths and weaknesses of each of these three types?

(b) (5 pts) Under what conditions, an organization needs to use all three types of security strategies? Why?

(c) (6 pts) Identify which types of security strategy use the following mechanics or tools?

1. Intrusion detection mechanisms
2. Information assurance policies
3. Smart cards
4. Risk management
5. Steganography
6. Watermark

Your Answer:

(2.a) Three Security Strategies

(I) **Obscurity Strategy:**

1. If the existence of an organization’s IA baseline and critical objects are unknown, the organization might avoid or reduce threats
2. Intent to secure the system by hiding the details of security mechanisms
3. IA involves use of obscurity strategy to a variety of extent

1. Strength - This strategy is intents to secure the system by hiding the details of security mechanisms which is its biggest advantage.
2. Weakness -
   Security by obscurity substitutes concealment for actual security in su ch a way that if the trick is discovered, it will damage your system.

(II) **Perimeter Defense Strategy**

Focus on threats from outsiders
▪ Intent to control flow of information between organization’s internal trusted network and untrusted external networks
▪ Not much IA capabilities is allocated to secure internal system

1. Strength - An organization that is well-prepared should have threat monitoring software to identify unusual behavior and a disaster recovery strategy to restore important data or systems that were attacked and shut down.
2. Weakness - Despite the belief of the majority of modern firms that cybercriminals cannot breach the perimeter defense firewall to access company information, this is not always the case.

(iii) **Defense in Depth Strategy:**

- Define a number of inter-operable and complementary technical and nontechnical IA layers of defense
- Separate organization’s network into enclaves
  - An enclave is an environment under control of a single authority with personnel and physical security measures.
- Perimeter defense for each enclave
- Complicated and multiple connections among enclaves and

between an enclave and outside
- Need multiple layers and different solutions for each connection

1. Strength: The information is protected by several layers.
2. Weaknesses: Implementing this defense strategy requires significant r esources and a high learning curve.

2.b -

First Strategy: When a corporation has very sensitive data and won't reveal where its servers are located, they can employ the first technique. As a result, the attacker will find it challenging to attack the server as they are unaware of its existence.

2nd Strategy: It's likely that we've been interacting with the outside network on a daily basis if we outsource the services to a third party. We can monitor the data and information moving across the organization's internal and external networks by utilizing perimeter defense.

3rd Strategy: The third technique makes use of an enclave, which is highly useful for detecting insider attacks. Every enclave will have a unique authentication process, making it challenging for an attacker to access the company's core data and launch an attack.

2.c

1. **Intrusion detection mechanisms** - Layer 9 (IA policy compliance oversight) which is a part of Defense in depth strategy.
2. **Information assurance policies** - Defense in depth strategy, layer 1
3. **Smart cards**- Layer 4 of Defense in Depth or perimeter defense
4. **Risk management** - Used for mission assurance of information systems
5. **Steganography** - part of Cryptographic encryption
6. **Watermark**- digital watermarking used in cryptography or cryptosystems.

(a) -2 missing information (b) -2 missing information (c) -3 wrong for 4, 5 and 6

Question 3

14 / 16 pts

(a) (10 pts) What are the advantages of using formal methods to address information assurance problems of information systems handling confidential information? Provide reasons for each advantage.

(b) (6 pts) What are the major challenges of using formal methods to address information assurance problems of information systems.

Your Answer:

(3.a)

Advantages of using formal specification:

1. Clarify **requirements and design -** In order to prevent security problems or at the very least identify them, formal approaches carefully define the requirements and analyze the information system.
2. Articulate **implicit assumptions -** The methods can identify the implicit assumptions underlying the system with the formulation.
3. Identify **undocumented or unexpected assumptions**
4. Expose **defects -** Formal methods can be useful to detect defects in the system using mathematical modeling and testing.
5. Identify **exceptions**
6. Evaluate **test coverage**

(3.b) Major Challenges of using Formal Methods are:

1. Requires sound mathematical knowledge of the developer
2. Different aspects of a design may be represented by different formal specification methods
3. Useful for consistency checks, but cannot guarantee the completeness of a specifications
4. It may not offer significant cost or quality advantages over others .

(a) -2 missing information (b)

Question 4

16 / 19 pts

(a) (5 pts) Why has machine learning become very useful only recently for improving information assurance and security of information systems handling confidential information?

(b) (6 pts) What are the major advantages of using machine learning techniques to protect information systems handling confidential information? Give the reasons for having each of the major advantages you mentioned.

(c) (8 pts) Which of the following machine learning techniques will be more useful to protect confidential information of an information system: (i) Unsupervised Learning, and (ii)Reinforcement Learning? If your answer is based on certain conditions, you also need to answer the question if your conditions are not satisfied, which one would you use with reason.

Your Answer:

(4.a) Machine Learning became useful because of the following reasons:

1. In recent years, the field of software security has experienced tremendous growth becauee to machine learning. Using potent ML algorithms, machine learning aids in the detection of anomalies. This makes it simpler to find bugs and attacks from attackers.
2. The algorithm continuously learns from the past data and identifies patterns that are similar. This makes Machine Learning more powerful and preventive.

(4.b) Major Advantages of Machine Learning:

1. Because Machine Learning uses historical data to forecast, anticipate, and combat threats in close to real-time. By examining at the traits and patterns of the threats that have already recorded, detected, and blocked, it may anticipate potential dangers.

2. Network protection shifts from a responsive to a preventative state as a consequence of the network security becoming intelligent. Additionally, the fact that AI and ML algorithms are ever-evolving makes it challenging for attackers to defeat it.

3. ML can also detect a security attack which appears to be normal by learning from the data from past, as well as it has power to identify the suspicious logins, analyzing IP addresses and prevents the unauthorized access request from logging into the system.

4. In recent times, the data generated is huge, and ML can use techniques like, Face recognition, fingerprint authentication etc to secure the system from attacks.

5. The user's behavior can be analyzed to find odd behavior using sophisticated machine learning methods. This will facilitate a quicker detection of the perpetrator.

(4.c):

The greatest strategy to safeguard sensitive data would be **reinforcement learning**. With reinforcement learning, the computer or the agent picks up new information through trial and error after each cycle. The machine will learn about the anomalies and the patterns by using Reinforcement Learning to train on private data. The machine will attempt to correct the errors from the most recent cycles in the following cycle.
The model becomes more reliable and clever as we increase the number of cycles, which helps to safeguard the sensitive data. For this, the prerequisites are that we have prior access to the private information and adequate time for the model to be trained on it. The model will iteratively improve as a result of continuously learning from past cycles.

(a) -1 missing information (b) (c) -2 missing information

Question 5

6 / 10 pts

(a) (5 pts) Identify as many major difficulties as you can to improve physical security for an organization and provide justifications for each of the major difficulties you identify.

(b) (5 pts) What you can do to overcome the major difficulties of physical security you identified in (a)?

Your Answer:

5.a

1. Wrong resource acquisition e.g. Hiring a criminal

2. Fraud, Abuse, Collusion

3. Leak of insider data in organization

4. Employees engaging in businesses of similar nature with other organizations

5. Abuse of confidential data

5.b

1. Conduct a Background Check for each of the employees.

2. To address 2: Job rotation can be done among employees

3. To address 3: We can employ Non disclosure agreements

4. To address 4: We can make employees sign non-compete agreement

5. To address 5: Security clearances for each of the employee while exiting.

(a) -2 missing information (b) -2 missing information

Question 6

12 / 14 pts

(a) (6 pts) How can you ensure that both mission assurance and information assurance can be achieved for carrying out a critical mission?

(b) (8 pts) Give an example to show how you can carry out a critical mission, which requires using an information system, to achieve both mission assurance and information assurance successfully.

Your Answer:

6.a - By Employing and assessing the requirements with the following we can achieve both mission assurance and information assurance

Mission Assurance Requirements
To create a state of resilience that supports the continuation of an entity's critical business processes and protects its employees, assets, services, and functions.
Includes disciplined application of system engineering, risk management, quality and management principles to achieve success in requirement analysis , design , development , testing , deployment and Operations process phases
Information Assurance Requirements
To encompasses the scientific, technical, and management disciplines required to ensure information security and quality.
protect and defend information and information systems (Computer systems and network, information, operating environments) by ensuring their availability, integrity, authentication, confidentiality and nonrepudiation
Also both can follow mission assurance categories (MACs) that form the basis for availability and integrity requirements.
1) MAC I systems handle information vital to the operational readiness or effectiveness of deployed or contingency forces.
2) MAC II systems handle information important to the support of deployed and contingency forces.

3) MAC III systems handle information that is necessary for day-to-day operations, but not directly related to the support of deployed or contingency forces.

6.b - Concerns must be given in order to complete the project successfully and satisfy the needs of both information assurance and mission assurance.
Information assurance and mission assurance are at odds.
Information assurance (IA) prioritizes data and system security, which frequently clashes with mission assurance's "get the job done" mentality.
This conflict is largely eliminated when the focus of information assurance is bifurcated into protecting the infrastructure and data, and securely sharing information with authorized recipients.
includes the methodical use of management, quality, risk, and system engineering principles to accomplish success.

Includes disciplined application of system engineering, risk management, quality and management principles to achieve success
They should concern about availability and integrity.
Both can follow mission assurance categories (MACs) that form the basis for availability and integrity requirements.
1) MAC I systems handle information vital to the operational readiness or effectiveness of deployed or contingency forces.
2) MAC II systems handle information important to the support of deployed and contingency forces.
3) MAC III systems handle information that is necessary for day-to-day operations, but not directly related to the support of deployed or contingency forces.

(a) -2 too much information (b)

Quiz Score: **80** out of 100