CSE 543 Information Assurance and Security Mid Term

Due Mar 2 at 11:45am **Points** 100 **Questions** 5
Available Mar 2 at 10:30am - Mar 2 at 11:45am 1 hour and 15 minutes
Time Limit 75 Minutes

Instructions

CSE 543 Information Assurance and Security

Classroom: Coor Hall L1-74

Spring 2022

First Examination

Professor Stephen S. Yau

Date: March 2, 2022

Time: 10:30 a.m. - 11:45 a.m.

Duration: 75 minutes

Total: 100 Points

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

Rules for all students:

1. The exam is an open-book exam. Answers must be in your own words (paraphrased), not directly quoted or cut-and-pasted from the outside materials or lecture slides.
2. You are not allowed to collaborate with other students or ask for help from anyone during the exam. You must also keep your answers securely, not accessible by other students. Violation will be considered a serious offense to academic integrity, and an appropriate penalty will apply.
3. Each of you has selected one and only one of the following three groups on the modes of exam:

Group 1: Take the exam in person and in the classroom using the exam paper distributed at the beginning of the exam.

Group 2: Take the exam in person in the classroom using your computer through Canvas.

Group 3: Take the exam at your home using your laptop computer through Canvas.

Instructions for students in Groups 1 and 2:

1. If you have any questions during the exam, you can raise your question to Professor Yau, Rama or Jaya Teja in the classroom.

Instructions for students in Groups 2 and 3:

1. The exam problems will be published through the Canvas (in the Quiz section) in the same format as a regular exam paper. This exam will be made available at 10:30 a.m. on March 2.
2. You must type your answers ***in the space provided for the answer to each question in the Canvas Quiz section***. The Quiz (All your exam answers) must be submitted ***no later than 11:45 a.m. on March 2.***

Additional Instructions for Group 3 students:

1. For each Group 3 student, you must ensure that you have a ***stable internet connection to Canvas throughout the exam period***.

You must be ***on Zoom meeting and keep your camera on throughout the exam period.*** The Zoom link is **https://asu.zoom.us/j/81322153426 (https://asu.zoom.us/j/81322153426)** , which will be activated about 15 minutes before the exam starting time (10:15 a.m. on March 2). You will be continuously monitored and recorded during the exam. If you join the exam after 10:35 a.m., you need to send an email to Rama and Jaya requesting to allow you to join the Zoom meeting. ***If you are found talking with another person, switch off the camera, or move out from the camera, it will be considered a serious offense to academic integrity***, and an appropriate penalty will apply.

2. If you have any questions during the exam, you should send a clear and short message to Rama, Jaya, and Professor Yau through Canvas or

through email or through Zoom, and one of us will answer your questions through Canvas messaging system or email or Zoom.

This quiz was locked Mar 2 at 11:45am.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	75 minutes	49.5 out of 100

Correct answers are hidden.

Score for this quiz: **49.5** out of 100
Submitted Mar 2 at 11:45am
This attempt took 75 minutes.

Question 1

3 / 13 pts

(a) (3%) What is machine learning?

(b) (10%) Why does machine learning become very useful for improving information assurance and security of information systems handling highly sensitive information which will likely attract the attention of many sophisticated attackers?

Your Answer:

a. Machine learning is a branch in artificial intelligence (AI) which makes sure the system automatically learns and improves from its experience without having to program it explicitly. Machine learning focuses on the development of computer programs that can access data and use it to learn for themselves. Machine learning focuses on the use of relevant data and powerful algorithms to imitate humans to learn and improve the accuracy of the recognition process of applications.

b. The use of machine learning in Cybersecurity is as follows:

1. Over Time, it can acquire More Knowledge: Machine learning and deep learning is employed to learn the behavior of a business network over time. It detects and groups patterns in the network. It then detects any

deviations or security incidents from the norm before responding. The patterns that artificial neural networks learn over time may aid in future security. Potential threats with similar characteristics to those recorded are identified and blocked as soon as possible. The fact that AI and ML is constantly learning makes it difficult for hackers to outwit it.

2. It can identify unknown threats: A human may not be able to identify all of the threats that a company might face. The threats can be hundreds of millions of attacks by the hackers. Unknown threats can wreak havoc on a network. Worse, they can have a significant impact before they get detected. As attackers experiment with new tactics ranging from sophisticated social engineering to malware attacks, modern solutions must be used to prevent them. Machine learning has proven to be one of the most effective technologies for mapping and preventing unknown threats from wreaking havoc on a company.

3. Large data can be handled properly: Every day, sensitive data is exchanged between customers and the business. This information must be safeguarded against malicious people and software. Machine Learning is the best solution for detecting threats disguised as normal activity. Because it is automated, it can sift through massive amounts of data and traffic.

4. Overall security has been improved: By shifting all the data to the cloud to reduce the load on external servers and to reduce the hassle of maintenance. Machine learning can help in securing the data by identifying the suspicious logins and then analyzing the IP addresses and their reputation. Machine Learning can detect all types of attacks and helps in prioritizing and preventing them.

5. Authentication Protection: When a user wishes to enter into their account, machine learning secures authentication. For identification, it use a variety of techniques like facial recognition, CAPTCHA, and fingerprint scanners, among others. These traits' data can be used to determine whether a log-in attempt is authentic or not.

b. Plagiarism found (-10)
https://www.ranksecure.in/blog/tag/cybersecurity

Question 2

12 / 22 pts

(a) (2%) What is a formal method?

(b) (5%) Why is the formal method important in information assurance and security of information systems?

(c) (15%) Give two different examples to show where the formal method is useful in improving information assurance and security of information systems.

Your Answer:

a. Formal methods are a type of mathematically rigorous approach used for the specification, development, and verification of software and hardware systems. Formal Methods precisely determine requirements and analyze the system so that security incidents can be prevented or at least identified.

b. The importance of formal method is:

   1. It has clear requirements and design and can clarify them
   2. It can identify unexpected or missed assumptions
   3. It can find defects
   4. It can find out exceptional cases
   5. Evaluation of test coverage is easy
   6. Communication and documentation of implicit assumptions can be done

c. The different examples of formal methods is information assurance and security are:

   1) If the formal specification is executable (operational semantics), it indicates that the observed behavior of the system is comparable to the behavior of the specification

   2) If the formal specification is present in axiomatic semantics, it indicates that the pre and post conditions of the specification may in the future become assertions in the cod

c. Need to explain in detail (-10)

Question 3

15 / 15 pts

(a) (5%) What is situation-aware role-based access control model?

(b) (10%) Give an example in the area of secure information system operations to show that the situation-aware role-based access control model is required?

Your Answer:

a. Situation-aware role-based is a type of access control that is based on the user's intention and purpose. The system admins provide privileges to objects, giving rise to a situation specific access to services. Situation-aware access control model incorporates situation-awareness into RBAC

b.) During the project's live implementation, the best example of situational aware role-based is provided. When a project is handed over to a banking company, the administrator or project manager is given complete access to the server and configurations. If the applications fail unexpectedly during the live phase and the employees of the banking firm are unsure what to do, they will contact the software handling company. If the program is properly managed, individuals may be aware of the problem or able to resolve it within the SLA time frame.

In that case, the admin/project head of the banking company must grant them access to the server or storage to repair the problem and ensure the application's proper operation.

Because there is no other option for resolving the issue and providing the best banking user experience to the client during the application downtime, the preceding example enables safe information system operations in accordance with situation-aware role-based access control. As a result, depending on the circumstances, the application development company will be granted access to the storage or server so that the applications can function properly.

Question 4

5 / 25 pts

(a) (5%) What is information assurance, and what is mission assurance?

(b) (10%) When you conduct a project on a confidential application of an information system involving the use and generation of sensitive information, what method will you use to achieve both mission assurance and information assurance?

(c) (10%) Give an example to illustrate your method in Part (b).

Your Answer:

a.

Information Assurance: encompasses the scientific, technical, and management disciplines required to ensure information security and quality.Security techniques as well as organisation, operation management, user awareness, policy, and legality, all play important roles.

Mission Assurance: is a life-cycle engineering process to identify and mitigate the deficiencies of mission requirements, design, production, test, and field support for mission success. The main objective of mission assurance is creating a state of resilience that supports the continuation of an entity's critical business processes and protects its employees, assets, services, and functions.

b.

Mission Assurance: covers the enterprise, supply base, business partners, and customer base to enable mission success. 1.Requirement analysis 2.Design 3.Development 4.Testing 5.Deployment 6.Operations process.

Information Assurance: contributes to the overall information assurance of information systems and networks.Information assurance focuses on protection of data and systems.

c.

Mission Assurance is a life-cycle engineering process to identify and mitigate the deficiencies of mission requirements, design, production, test, and field support for mission success. The main objective of mission assurance is creating a state of resilience that supports the continuation of an entity's critical business processes and protects its employees, assets, services, and functions. Information assurance (IA) focuses on protection of data and systems, often conflicts with the getting the job done attitude of mission assurance.These conflicts are largely eliminated when the focus of information assurance is bifurcated into: 1. Protecting the infrastructure and data 2.Securely sharing information with authorised recipients.

This is how the important projects involving both Mission assurance and Information Assurance are completed successfully.

b. Incorrect answer c. Incorrect answer

Question 5

14.5 / 25 pts

(a) (10%) What are the properties of blockchain, each of which makes blockchain useful for improving information assurance and security of information systems? Explain why?

(b) (10%) What type of blockchain is suitable to be used for developing trusted coordination in collaborative software development? Why?

(c) (5%) What are the advantages and disadvantages of using blockchain to develop trusted coordination in collaborative software development?

Your Answer:

a. The advantages of using Blockchain to improve information assurance and security in information systems is as follows:

1. CANNOT BE CORRUPTED: Every node on the network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.

2. DECENTRALIZED TECHNOLOGY: The network is decentralized meaning it doesn't have
any governing authority or a single person looking after the framework. Instead, a group of nodes maintain the network making it decentralized.

3. ENHANCED SECURITY: As it eliminates the need for central authority, no one can just simply change any characteristics of the network for their benefit. Also using encryption ensures another layer of security for the system.

4. DISTRIBUTED LEDGERS: The ledger on the network is maintained by all other
users on the system. This distributes the computational power across the computers to ensure a better outcome.

5. CONSENSUS: Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

6. FASTER SETTLEMENT: Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

b. A private blockchain is used to provide trusted coordination in collaborative software development using smart contracts. The complete collaborative software development effort is represented via a blockchain. Each participating software development team is represented on the blockchain by a unique node. Only one of the participating teams is designated as the prime contractor team, which is in charge of negotiating and establishing all of the participants' obligations in the software development project. The participating teams could be from separate organizations or from the same as the lead contractor.

c.

The advantages of using it are:

1. Use a distributed software repository and mechanism for data exchange.

2. Ensure that all software components have an unchangeable history.

3. There is no central authority.

4. All software components should have a traceable history.

5. Establish a secure communication route between the participating teams.

6. Verify that all software components meet the acceptance requirements automatically.

7. Non-repudiation of all software components' histories.

The disadvantages are:

1. Need to increase the trustworthiness of the coordination in collaborative software development.

2. The developer is required to have good knowledge

a. Need to explain the properties of blockchain not the advantages. (-8) c. Incorrect disadvantages (-2.5)

Quiz Score: **49.5** out of 100