

# 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	<u>Attempt 1</u>	74 minutes	82 out of 100

⚠️ Correct answers are hidden.

Score for this quiz: **82** out of 100

Submitted Mar 2 at 11:44am

This attempt took 74 minutes.

### Question 1

13 / 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 the broad field that concentrates on leveraging relevant data and strong algorithms to mimic human knowledge and improvise the accuracy and precision of the used applications.

b. Machine learning has become inseparable in the field of cybersecurity as it can proactively filter out cyber threats and improvises security infrastructure through various methods like pattern detection, real-time cybercrime mapping and penetration testing. Machine learning has come out as powerful in many issues while few are listed below:

1. Protect data in cloud-based applications:

It can protect the applications by analyzing and sending reports on suspicious account cloud login activity, detecting any new location sign-ins and performing IP based analysis to identify risks and threats.

2. Detect malware in encrypted traffic:

It can detect dangerous malware in encrypted traffic by performing analysis on encrypted traffic data in common network telemetry. Instead of decrypting, machine learning algorithms pointedly find out the malicious patterns to identify threats hidden with encryption

3. Provide endpoint malware protection

These machine learning algorithms can identify any new malware that is trying to run on endpoints of any network. They can identify brand new malicious files and activities based on the previous attacks, attributes and behaviours of known malware.

4. finding threats on a network

Machine learning identifies dangers by continuously monitoring network behaviour for anomalies. To detect major occurrences, machine learning engines process huge volumes of data in near real-time. Insider threats, undiscovered malware, and policy infractions can all be detected using these tactics.

5. Keeping people safe while browsing

Machine learning can help users avoid connecting to harmful websites by predicting "bad neighbourhoods" online. Machine learning examines Internet behaviour to detect attack infrastructures that are ready to respond to existing and emerging threats.

## Question 2

17 / 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. The approaches which reason about computational entities along with logical or mathematical descriptions of those entities are called formal methods. They also enable in eliciting reliable conclusions about their behaviour.

b. Formal methods significantly enable the following:

1. modelling and creating a design.
2. verifying the test coverage.
3. synthesizing
4. Establishing requirements
5. Make explicit any implicit assumptions.
6. Undocumented or unanticipated hypotheses can be identified.
7. Make drawbacks visible.

They can also be very helpful in varying degrees of rigour. Formal methods at assorted levels of abstraction have had significant success in securing computer systems.

c. Consider an example of secure hardware which is frequently built on specialised arithmetic derived from a finite number of fields and usually requires non-standard word lengths. By showing the similarity between specification and implementation, formal tools aid in the design soundness of these operators.

In hardware circuits information-flow analysis, high complexity reduces a designer from overtaking manual verification which is another significant area of verification success. this kind of investigation gives us an ensured isolation

This can be identified in a physical chip package that allows trusted and untrusted logic to coexist.

c. Irrelevant examples (-5)

**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. It is a dynamic process that access decisions based on situations like allowing cameras.

Here, the user gains a particular level of authority till he or she is able to keep that role's permission for as long as the user holds that power. RBAC combines situation-awareness into the situation-aware access control concept.

b. Consider an example where only when the user is in the Smart Classroom in the position of a teacher during class time can the user establish a group discussion. Only the host of a Zoom conference, for example, can construct Breakout rooms because only he possesses context-aware RBAC. He is capable of safeguarding the privacy of each group. If a Host leaves the meeting, the Co-Host takes over as Host and has control over rights such as screen sharing and breakout rooms. The meeting's host can only create, therefore the user in the meeting gets Situation Aware RBAC.

**Question 4****20 / 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: It includes the scientific, technical, and management disciplines that are needed to assure data security and quality. Security techniques, as well as an organization, operational management and environments, user awareness, policy, and legality, all play critical roles. The overall information assurance of information systems and networks is aided by the quality of information.

Mission assurance: For mission success, a life-cycle engineering approach is used to identify and address weaknesses in mission requirements, design, production, testing, and field support which is called mission assurance.

b. We can follow the below-mentioned steps to proceed methodologically to achieve both mission assurance and information assurance.

1. Determine the importance of critical missions, functions, and supporting assets and create priorities for them.
2. Create and implement a mission that is both comprehensive and integrated. Assurance Methodology for Risk Management
3. To optimize risk management solutions, use risk-informed decision making.
4. Risk Reduction Through Collaboration - A Shared Responsibility

c. Consider the example:

Mission analysis and breakdown procedures used by the Department of Defense, as well as related training, are being improved. This can be achieved by:

1. Improving the integration and coordination of the following well-established programs:
  - o Counter-terrorism Defense Critical Infrastructure Program
  - o Physical Security
  - o Information Security
  - o Emergency Management Installation
  - o Operational Continuity
2. Using and strengthening existing or forming new advocacy groups at the installation, Component, and DoD-wide levels to advocate for and incorporate mission assurance into policy, planning, and resource decisions.
3. Reviewing and developing a range of options for streamlining and integrating current assessment processes.

4. Creating a DoD-wide policy to standardize mission assurance goals, objectives, roles, and duties, as well as supporting structures and processes, and generating DoD-wide outcome metrics.

5. Finding or creating a method for sharing assessment results.

6. Identifying current capabilities within the Department of Defense that may be used to conduct a DoD-wide analysis of mission assurance risk trends and strategic challenges.

7. At all three decision-making levels, integrating and growing internally and externally focused relationships on the following issues:  
Transportation, Financial Services, Cyber, Telecommunications.

c. Information assurance is not discussed in your example (-5)

## Question 5

17 / 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. 1. Blockchain offers encryption and validation

Everything on the blockchain is encrypted, and it's easy to establish that no data has been tampered with. You can check file signatures across all ledgers on all nodes in the network and verify that they haven't been



modified because of the network's distributed nature. If someone alters a record, the signature becomes null and void.

## 2. Blockchain is virtually impossible to hack

While traditional networks allow hackers to break in and find all of the data in a single repository, exfiltrate or corrupt it, the blockchain makes this impossible. The network as a whole decentralizes, encrypts, and cross-checks the data. It's nearly hard to change or remove a record from the ledger without causing the signature to be invalidated.

Multiple nodes on the network confirm every genuine transaction. To properly hack blockchain, you'd have to compromise the majority of nodes at the same time, which, while technically doable with adequate supercomputing power and patience, is far above cybercriminals' current capabilities.

## 3. Blockchain is decentralized

Instead of uploading data to a cloud server or storing it in a single location, blockchain divides data into little chunks and distributes them among the network of computers. It's a decentralized digital ledger of transactions with no central control point. Because each computer, or node, has a complete copy of the ledger, data will not be lost if one or two nodes fail. It basically eliminates the middleman – no need to enlist the help of a third party to complete a transaction. When you can rely on a decentralized, immutable ledger, you don't have to trust a vendor or service provider.

## 4. Blockchains can be private or public

While public blockchains have received the most attention and praise for enabling anonymity, private blockchains can be created to limit access to certain people. You still get the benefits of a decentralized peer-to-peer network, but anyone accessing a private blockchain must authenticate their identity in order to get access privileges, and transactions can be controlled.

b. Hyperledger is an example of a blockchain system that can be used to promote trusted collaboration in software development.

During this phase, the software system is broken down into multiple components, each of which is built by a separate team. Each group creates a software specification as well as code for smart contracts. Each team carries out software tasks outlined in a smart contract and logs the results in a blockchain. Any team in the blockchain can verify the findings,

but no team can modify the outcomes. As a result, improving the credibility of coordination in collaborative software development is helpful.

For example, we have three software development teams (T1, T2, and T3) and five key components (C1, C2,...C5). At the outset of the project, each team's tasks are assigned. T1 develops a test strategy for all software components in terms of smart contracts after consulting and negotiating with other teams. T2 uses the blockchain to retrieve a component in order to perform unit testing and publish the results. If the reported findings meet the acceptance parameters for the component's smart contract, they are uploaded to the blockchain after consensus and endorsement. T3 can query the smart contract to see all previous operations on the software component, and the smart contract can accommodate any modifications to the software testing plan or activities.

#### c. Advantages

- Secure - Every transaction is made public. This leaves no room for fraud.
- No third party interference - No government or financial institution has control
- Secure transactions - keeping a record of all the transactions cannot be edited or manipulated.
- Instant transactions – Blockchain technology transactions are completed in a few minutes.

#### Disadvantages:

1. Difficulties with Updating and Elimination of Errors
2. Network Robustness for Dedicated Purposes
3. Difficulty of Development. There can be room for: a. Crime b. Technology for the geeks. c. Human errors.

a. Incorrect answer (-8)

Quiz Score: **82** out of 100