First Exam

Due Oct 7, 2021 at 2:45pm **Points** 100 **Questions** 6
Available Oct 7, 2021 at 1:30pm - Oct 7, 2021 at 2:45pm about 1 hour
Time Limit 75 Minutes

Instructions

CSE 543 Information Assurance and Security

Classroom: Coor Hall L1-74

Fall 2021

First Examination

Professor Stephen S. Yau

Date: October 7, 2021

Time: 1:30 p.m. - 2:45 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:

Rules for all students:

1. The exam is an open-book exam. Answers being sourced from materials outside the lecture slides must be in your own words (paraphrased), not direct quoted or cut-and-pasted from the outside materials.
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 Canvass.

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

Instructions for students in Groups 1 and 2:

1. If you have any questions during the exam, you can raise your question to me, Jaya or Aayush 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 1:30 p.m. on October 7.
2. You must type your answers ***in the space provided for the answer to ea***ch ***question in the Canvas Quiz section***. The Quiz (All your exam answers) must be submitted ***no later than 2:45 p.m. on October 7.***

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/82470787878 (https://asu.zoom.us/j/82470787878)** , which will be activated about 15 minutes before the exam starting time (1:30 p.m. on October 7). You will be continuously monitored and recorded during the exam. If you join the exam after 1:35 p.m., you need to send an email to Jaya Teja and Aayush requesting to allow you to join the zoom meeting. ***If you are found to talk 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 Jaya, Aayush, and me through Canvas, and one of us will answer your questions through Canvas messaging system.

This quiz was locked Oct 7, 2021 at 2:45pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	74 minutes	95 out of 100

Correct answers are hidden.

Score for this quiz: **95** out of 100

Submitted Oct 7, 2021 at 2:45pm

This attempt took 74 minutes.

Question 1

19 / 20 pts

(A) (7%) What are the three major types of strategies for protecting critical objects? Explain each type briefly.

(B) (8%) Identify all major types of strategies that can use (I) firewalls, (ii) intrusion detection, (iii) separation of roles of personnel, and (iv) personnel identification cards. In each case, explain how the kind of security tool or mechanism is used in the strategy.

(C) (5%) How would you protect an information system with a number of critical objects stored in a number of enclaves, each of which is well protected by the defense-in-depth strategy?

Your Answer:

(A)

SECURITY BY OBSCURITY STRATEGY :-

- If the existence of an Organization's IA baseline and critical objects is unknown ,the organization may not be subject to threats .

-Intent to secure the system by hiding the details of a security mechanisms

- IA involves use of obscurity strategy to a variety of extent

PERIMETER DEFENSE STRATEGY :-

- Focus on threats from outsiders

-Intent to control flow of information between organisation's internal trusted network and untrusted external internet .

-Not much IA capabilities is allocated to secure internal systems .

-Examples : firewalls , security access keys , access codes

DEFENSE IN DEPTH STRATEGY :-

-Define a number of operationally inter-operable and complementary technical and non technical IA layers of defense

-seperate organisation's network into enclaves

An enclave is an environment under control of a single authorty with personel 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 .

B)

Firewalls: The firewalls are generally used by the perimeter defense strategy. It is used to avoid the threats that can impact a system from the outside. For example: If a malicious bug or threat is imposed from outside, the firewalls can filter it out and make sure the system is guarded.

Intrusion detection: Intrusion detection are generally found in the Defense in depth strategy. They consist in the layer 9 , IA policy compliance oversight. The main function is to detect, report and correct the noncompliance with IA policies. The goal is to avoid any threats to the system by following a particular set of rules or policies.

Separation of roles of personnel: The Separation of roles of personnel is generally classified in defense in depth strategy. They consist in the layer 4, Operational Security Administration. The use of this role is done to differentiate between personnel with respect to their roles.

C

We can use Perimeter defense for each enclave and

Complicated and multiple connections among enclaves and between an enclave and outside .
Need multiple layers and different solutions for each connection.
We can use below Layers to protect information system with a number of critical objects stored.
Core consists of critical objects and IA baseline that collect, input, process, store, output, and communicate with any element in core.
IA Policies (Layer 1) define the actions and behavior required to accomplish the organization's IA needs.
IA Management (Layer 2) monitors and controls implementation of the IA policies.
IA Architecture (Layer 3) provides a means to allocate and integrate technical and nontechnical controls
Layers 4 to 10: non-technical implementations of IA policies, and provide infrastructure for IA Architecture
Layer 4 Operational security administration
Layer 5 Configuration management
Layer 6 Life-cycle security
Layer 7 Contingency planning
Layer 8 IA education, training, awareness
Layer 9 IA policy Compliance Oversight
Layer 10 IA incident response and reporting

B. separation of roles of personnel comes under Obscurity Strategy -1

Question 2

16 / 16 pts

(A) (6%) What are mission assurance and information assurance requirements when conducting a large-scale and complex project?

(B) (10%) What do you need to be concerned with to achieve the success of the project and satisfying the requirements of both mission assurance and information assurance?

Your Answer:

A)

Following are the requirements of mission assurance and information assurance when conducting a large scale and complex projects.

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.

B) Things need to be concerned with to achieve the success of the project and satisfying the requirements of both mission assurance and information assurance.

Conflict between Information assurance and Mission assurance.

information assurance (IA) focuses on protection of data and systems, often conflicts with the “get the job done” attitude of mission assurance. 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 disciplined application of system engineering, risk management,

quality and management principles to achieve 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.

Question 3

12 / 12 pts

(12%) Describe the following types of access control of confidential objects, and give an example for each type of control:

(A) Mandatory access control

(B) Discretionary access control

(C) Role-base access control

(D) Situation-aware access control

Your Answer:

(A) Mandatory access control

Restrict access to objects based on sensitivity of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity .

(B) Discretionary access control

- Restriciting access to objects based on identity of subjects and /or groups to which they belong

- controls are discretionary in the sense that user or process given discretionary access to information is capable of passing that information to another subject .

(C) Role-base access control

- Associate roles with an each individual

-Each role defines a specific set of operations that the individual acting in that role may perform

-individual needs to be authenticated , chooses a role that has been assigned to individual and accesses information according to operations needed for role .

situation aware access control:

The situation-aware RBAC model is designed for specifying dynamic access policies in an S-ADS system. Due to the situation-awareness capability of our approach, flexible and high-grained access policies can be specified and enforced for various providers and users.

The situation-aware RBAC model is designed for specifying dynamic access policies in an S-ADS system. Due to the situation-awareness capability of our approach, flexible and high-grained access policies can be specified and enforced for various providers and users.

Question 4

9 / 9 pts

(9%) Identify 9 effective ways to improve the personnel security of a large organization.

Your Answer:

Personnel Security is maintaines to reduce the number of risks of human

errors, thefts, frauds or misuse of facilities within an organization.

Protect the data itself, not just the perimeter

Many firms appear to be focusing on securing the walls around their data, with firewall technology accounting for nearly 90% of security budgets. There are hundreds of ways to get through a firewall, including through customers, suppliers, and workers. All of these individuals have the potential to circumvent external cyber-security and misappropriate critical information. As a result, you must guarantee that your security efforts are centered on the data rather than the perimeter.

Pay attention to insider threats

It's easy to imagine threats coming from outside your organization because they're frequently depicted in the news and on television as the most serious and costly. However, the truth is that your insiders are the ones who may injure you the most. Insider assaults are difficult to identify and avoid due to their nature. It can be as simple as an employee clicking on an email attachment that appears to have come from a trusted source, resulting in the spread of a ransomware worm. These types of hazards are the most common and costly around the world.

Encrypt all devices

In today's society, an increasing number of people prefer to work on their mobile or personal gadgets. How can you be certain that these devices are reliable? Make sure that all data is secured and that it stays encrypted during migrations.

Testing your security

Think again if you think that putting antivirus on every computer or gadget can safeguard your firm from cyber-attacks. Hiring a competent agency to undertake a security audit will always find vulnerabilities you weren't expecting, as previous data breaches have demonstrated. I recommend that you take a walk around your office and glance at the desks of your coworkers. I guarantee you'll find a password written down on a sticky note if you look hard enough.

Delete redundant data

Many businesses, particularly those in healthcare, banking, government, and education, deal with sensitive data as a necessary component of their operations. Having information disposal measures in place helps to avoid stale data from being lost and stolen later. Having a mechanism in place for shredding, deleting, or otherwise making redundant data unreadable will go a long way toward ensuring that your staff don't keep it.

Establish strong passwords

Numerous associations are as yet utilizing loosened up secret word arrangements, prompting straightforward, conventional and simple to-hack passwords for basic records, which approach the delicate and significant information. Executing solid passwords is the initial step you can take to fortify your security around here. Utilize sensibly complex passwords and change them like clockwork. Never use passwords like "12345" or "Admin1". Absolutely never record your passwords and pass on them on your workstation for others to discover.

Back-up your data regularly

This should as of now be a urgent piece of your IT security system. With secure reinforcements set up, you can endure everything from unplanned record erasure to a total ransomware lockdown. As a security best practice, reinforcement information ought to be put away in a solid, far off area away from your essential business environment.

Update your programs regularly

Ensure your PC is appropriately fixed and refreshed. This is regularly the most ideal approach to guarantee its sufficiently ensured. Your security applications are just on par with their latest update. Since programmers and ransomware strains are continually adjusting to take advantage of shortcomings in prior programming adaptations, it is prudent to refresh these applications consistently.

Spending more money and time on Cyber-security

Many CIO's have conceded that investing more cash and more energy in information security is an absolute necessity, as its absence keeps on being the main danger to your IT foundation. Many large organizations with delicate business information to ensure are designating boss security officials, regularly to board level situations, with an affirmation that network safety must be a vital piece of all business measures.

Create a company-wide security mindset

Each and every individual who has a secret key and username is answerable for keeping information secure. IT directors should occasionally remind their chiefs and workers that they should not impart logon data to any external party. Data security is everybody's work and isn't simply restricted to simply a modest bunch of representatives in the IT group.

Question 5

13 / 13 pts

(A) (7%) What are the advantages and limitations of applying formal methods to information assurance and security?

(B) (6%) Identify two different types of IA problems that have been studied using formal methods and explain briefly why.

Your Answer:

(A)

ADVANTAGES :-

1.Clarifies requirement and specifications .

2.Articulate implicit assumptions .

3.Identify undocumented or unexpected assumptions .

4.Expose defects .

5.Identify exceptions.

6.Evaluate test coverage .

LIMITATIONS :-

1.It 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 specifications .

4.For majority of the systems , formal methods currently may not offer significant cost or quality advantages over others .

(B)

Applications

Formal strategies are applied in various spaces of equipment and programming, including switches, Ethernet switches, steering conventions, security applications, and working framework microkernels like seL4. There are a few models wherein they have been utilized to confirm the usefulness of the equipment and programming utilized in DCs[clarification needed]. IBM utilized ACL2, a hypothesis prover, in the AMD x86 processor improvement process.[citation needed] Intel uses such strategies to check its equipment and firmware (long-lasting programming modified into a read-just memory). Dansk Datamatik Center utilized conventional techniques during the 1980s to foster a compiler framework for the Ada programming language that proceeded to turn into a seemingly perpetual business item.

There are a few different activities of NASA where formal techniques are applied, for example, Next Generation Air Transportation System[citation needed], Unmanned Aircraft System incorporation in National Airspace System,and Airborne Coordinated Conflict Resolution and Detection (ACCoRD).B-Method with Atelier B, is utilized to foster wellbeing automatisms for the different trams introduced all through the world by Alstom and Siemens, and furthermore for Common Criteria accreditation and the advancement of framework models by ATMEL and STMicroelectronics.

Formal confirmation has been every now and again utilized in equipment by a large portion of the notable equipment merchants, like IBM, Intel, and AMD. There are numerous spaces of equipment, where Intel have utilized FMs to confirm the working of the items, for example, defined check of store intelligent convention, Intel Core i7 processor execution motor approval (utilizing hypothesis demonstrating, BDDs, and emblematic assessment), improvement for Intel IA-64 engineering utilizing HOL light hypothesis prover,and confirmation of elite double port gigabit Ethernet regulator with help for PCI express convention and Intel advance administration innovation utilizing Cadence.Similarly, IBM has utilized proper techniques in the check of force gates,registers,and utilitarian check of the IBM Power7 microchip

Question 6

26 / 30 pts

(A) (6%) Under what conditions is blockchain useful to improve the information assurance and security of an online application? And under what conditions is the blockchain not useful to improve the information assurance and security of an online application? Why?

(B) (24%) Consider a food retail company that has decided to use blockchain for the food management system. This food management system will handle the processes that involve the following types of stakeholders: store managers, staff, suppliers, and customers. These processes include acquisitions, distribution, processing, advertising, and consumption of food. In addition, the system must satisfy the following requirements:

Secure and transparent to connect all stakeholders directly throughout the process and to address the fraud transactions.

(B.1) (4%) What type of blockchain should be used in the system and why?

(B.2) (15%) Describe how you will use the type of blockchain selected in part B to develop the food management system with the specified requirements?

(B.3) (5%). What are the advantages and concerns of using blockchain to develop this food management system?

Your Answer:

A)

It is useful when when the following conditions are satisfied

- We need to store a state

- We have multiple trusted writers

- Writers are always online

If one of the above conditions is not satisfied blockchain should. not be used

Blockchain innovation is utilized for different applications in the field of exceptionally secure information move and monetary repayments completed across web as it will add security and trustworthiness to the data with agreement calculations, decentralized nature, permanence offering protection to data shared across the web.

Example: Online banking and payments, Trading, Healthcare, Real Estate, Taxes

Block chain innovation isn't actually vital for online applications where no basic data or data set should be put away at all between elements.

B)

B.1)

B.2)

Blockchain innovation can help with the formation of an unchanging agreement between the different members in the inventory network, taking into account more straightforwardness. The quantity of mediators in the store network organization can be diminished by utilizing a shrewd agreement. These keen agreements can reduce exchange expenses, upgrade edges, and increment proficiency, permitting the rancher/maker to keep a bigger part of the income.

When joined with state of the art information catch innovation, blockchain offers tremendous guarantee in the food business. We can change the food business by consolidating the forces of blockchain and the Internet of Things (IoT). IoT arrangements interface the genuine and advanced universes by recording information like temperature and mugginess while an item is being moved or put away. Each part in the production network might save and access this information on the blockchain, which is a solid and unchangeable stage.

The production network will be smoothed out, bringing down store costs.

It works on administrative consistence.

It will assist with improving and accelerate the food review methodology.

B.3) Blockchain is not a distributed computing system which means it requires a lot of computation to handle.

Scalability is an issue.

Blockchain cannot go back. It is immutable. If we want to modify the order of a customer it is impossible to do so.

B.1) Missing

Quiz Score: **95** out of 100