Assignment 1

CSCE 4357/5933: Database Systems Security

(Spring 2023)

**Due Date: 02/15 @ 11:59pm | Points:** **100**  **| Late Policy: 10%**

**NOTE: Please write everything on your own and do not copy/paste, avoid plagiarism.**

**1). [Total: 40pts]**

**a) [10pts] What are the three properties to ensure data security and privacy? (Single Choice)**

1. Security, Sustainability, Integrity
2. Security, Privacy, Integrity
3. **Confidentiality, Integrity, Availability**
4. Privacy, Integrity, Confidentiality
5. None of the above

**b) [10pts] What is Privacy? (Single Choice)**

1. The right to be let alone
2. limited access to the self
3. secrecy—concealment of certain matters from others
4. control over others' use of information about oneself
5. personhood—the protection of one’s personality, individuality, and dignity
6. intimacy—control over, or limited access to, one’s intimate relationships or aspects of life
7. **All of the above**
8. None of the above

**c) [10pts] What are the key security mechanisms? (Multiple Choice)**

1. **Authentication; Access Control; Secure Communication**
2. **Logging and Auditing**
3. Privacy and Integrity
4. **Intrusion Prevention and Detection**
5. **Recovery**
6. Accessibility

**d) [10pts] What are the levels of accessing rights to any file?**

1. Read – Write – Finish
2. Read – Read – Write
3. **Read – Write – Execute**
4. Read – Execute – Complete
5. None of the above

**2). [Total: 30pts]**

**a) [15pts] In which ways information security is easier than physical security?**

**Please provide at least 3 example scenarios.**

The use of information systems has increased rapidly in recent years, to protect these systems many security mechanisms have been developed and implemented, below are a few scenarios that explain information security is easier than physical security:

1. **Scalability:** As per the requirements of the organization the security policies can be revised and incorporated, this can be done by ISO (information security officers), just by simply installing firewalls, etc. Whereas physical security is not very scalable, it requires people and is hard to manage.
2. **Cost:** Information security has become easy with the increase in the use of information systems, many software, firewalls, and intrusion detection systems are readily available in the market, can be bought at very cheaper rates, and can be installed by an IT professional. Physical security requires a lot of devices like cameras, biometric systems, sensors, etc., that are very expensive.
3. **Disaster recovery:** After a disaster, it is easy for an information system to recover. There are many backup systems and servers that keep storing data and any loss of data due to a disaster is recoverable within hours or days. But for physical security breaches, the loss is high, it is hard to track and recover from the loss.

**b) [15pts] In which ways information security is more difficult than physical security?**

**Please provide at least 3 example scenarios.**

Especially in the technologically advanced generation of today, with rapidly evolving technologies and many open sources to learn about systems, it is hard to secure the system. Information security is more difficult than physical security in the below scenarios:

1. **Securing the networks used by Information Systems:**

The information systems interact with various systems through the networks, these networks are highly complex and agile, and it is hard to secure networks that are constantly changing and especially when attackers are readily trying to exploit the vulnerabilities and take advantage of the information in these systems. On the other hand, physical security is quite straightforward and mainly involves protecting physical assets. Just by adding a few extra security protocols, physical assets can be protected but securing information systems in a network-driven world is hard because the vulnerabilities may go undetected until someone exploits them.

1. **Protecting data on the cloud:** Nowadays most of the data is stored on the cloud or a remote server. So, protecting this data from unauthorized access can be challenging especially with the increase in the number of cyber-attacks. Cyber-attackers cause significant damage to organizations by abusing sensitive user data using different ransomware, malware, viruses, etc. The attackers are sitting far away from the attacked systems, and it is hard to track them and punish them. Whereas in the case of physical security, the vulnerabilities are visible and can be managed, intruders are often captured in the cameras or any other security devices. It is easy to catch them and punish them.
2. **Dealing with insider threats:** It is highly impossible to detect insider threats in an organization, the employees working in positions where they have access to sensitive information can steal data from the information systems. In the case of physical security, it is easy to monitor and control access to physical assets.

**3).** **[Total: 30pts]**

**a) [15pts]** List ALL Principles of Security and/or Access Control.

1. Economy of mechanism  
2. Fail-safe defaults  
3. Complete mediation  
4. Open design  
5. Separation of privilege  
6. Least privilege

7. Least common mechanism  
8. Psychological acceptability

Below are a few more principles of security and Access Control:

1. Confidentiality
2. Integrity
3. Availability
4. Authentication
5. Authorization
6. Accountability
7. Non-Repudiation
8. Least Privilege

**b) [15pts] When can the transition happen from user mode -> system mode?**

The transition from kernel mode/user mode to system mode is mostly initiated by the CPU or by the operating system and can happen in three main situations that are described below:

1. **System calls:** Few operations and resources require special privileges, so whenever a user program tries to access such special resources or operations, a system call is generated. These system calls help the user programs that try to access privileged resources/operations by changing the mode from user mode to system mode, where the kernel performs the operation that is requested in place of the user program.
2. **Interrupts:** The I/O interrupts are usually handled by the kernel, so whenever there is an interrupt from any I/O devices, the CPU switches the mode from user to system mode just for the time being to handle the interrupt.
3. **Exceptions:** When system-level exceptions occur, user mode cannot handle the exceptions, so the CPU switches to system mode for exception handling. Once the error is handled, it switches back to user mode.

Top of Form