## COURSE PROJECT

# Enforcement Mechanisms

## Instructions

The goal of this project is for you to apply the concepts we cover in this course to an example system. You should continue working on the same system that you used in the previous three courses.

In **Part One**, you will identify which of the enforcement mechanisms designed previously are examples of monitoring.

In **Part Two**, you will identify which of the enforcement mechanisms designed previously are examples of re-writing.

In **Part Three**, you will identify which of the enforcement mechanisms designed previously are examples of isolation.

Except as indicated, use this document to record all your project work and responses to any questions. At a minimum, you will need to turn in a digital copy of this document to your facilitator as part of your project completion. You may also have additional supporting documents that you will need to submit. Your facilitator will provide feedback to help you work through your findings.

**Note:** Though your work will only be seen by those grading the course and will not be used or shared outside the course, you should take care to obscure any information you feel might be of a sensitive or confidential nature.

*Complete each project part as you progress through the course. Wait to submit the project until all parts are complete. Begin your course project by completing Part One below. Submit your completed project on the final project assignment page online. Information about the grading rubric is available on any of the course project assignment pages online. Do not hesitate to contact your facilitator if you have any questions about the project.*

## Part One

# Monitoring

For this part of the project, you will identify which of the enforcement mechanisms designed previously are examples of a monitor. For each, evaluate to what extent that enforcement mechanism implements complete mediation. Are there any security policies for your system that cannot be enforced with a monitor? Feel free to revise some of your designs from the previous course if appropriate.

Some of the enforcement mechanisms designed previously that are example of monitors include the following:

1. **Access Control List:** If a principal or a process tries to access a resource, a check is done on an access control list to ensure that the principal or process is on the list and has the required privileges to access the resource. Thus, an access control list enforces complete mediation.
2. **Guard:** A system that acts as check between two information systems operating under different security policies and is trusted to mediate information data transfers between the two.

3. **Capability authorization:** Capability authorization ensures that the principals or processes with right capabilities are authorized to carry out certain tasks. An access control list of capabilities can also be created.

In what follows, I will explain and access control list and a guard could help enforce security policies in an electronic voting system.

The system I have been working on the previous courses is an electronic voting system, in particular, internet voting system.

The security policies implemented for the voting system include the following:

- To vote, individuals need to first register at a registration centers designated by the electoral commission. An individual will need to visit a registration centre to be enrolled

unto the voting system. Personal information an an ID confirming identity of the bearer will be need for the registration. A secure link will be sent by the electoral commission to the individual via email or text message after the registration. The link will contain a temporary username and password which will expire after a certain period of time. Note that the username which is a voter ID number will be given upon registration at the enrollment centre. The user is then required to visit the link and update the password. To cast a ballot, an eligible voter will need to access the voting system by logging in with his or her voting credentials (password and username ) through the voting website. An individual who attempts login will be sent a token/code via text message or email. The voter will need to enter the token in text-box that will be provided before he or she is granted access to vote.

An access control list will be implemented in the form of a database to store the credentials. An access control list of the tokens with their expiration times will also be generated.

- To gain access to the election server room, individual must be an electoral commissioner or the voting system administrator. To gain access to the sever room, a principal will need to present a Plastic ID card together with a PIN.

  The principal will need to insert the plastic ID into a ***guard*** and enter a PIN. The guard is a programmable door lock that will store the fingerprints and PINs of the principals. Security officers will be tasked to ensure only authorized principals with valid ID cards can access the server room.

The security policies above have three monitors.

1. **An access control list**: a database that stores voting credentials of eligible voters.
2. **A guard:** This is a programmable door lock that will store the fingerprints and PINs of the principals.
3. **Security officers**.

The key features of the security measure include the following:

1. **Registration: I**ndividuals need to register at a designated centre by providing their personal information and IDs to confirm their identities. This will ensure that only eligible individuals are allowed to vote.
2. **Voting Credentials:** An individual will need a password, a username an a token to access the voting system. This serves proof of authorization to cast a ballot.
3. **ID cards, PIN and fingerprints:** Presenting an ID card, a PIN and fingerprint serves proof of authorization to access the server room by the electoral commissioners and system administrators.
4. **An access control list as monitor:** When individuals try to login, their credentials are checked against an access control list before they are allowed or denied access.
5. **A guard as monitor:** A user will need to insert his or her plastic ID card in the guard that is installed to lock the door of the server room. This guard c store the fingerprints and PINs of the administrators and electoral commissioners. The user will need to enter his or her PIN and provide their fingerprints. IF there is a match, the door will be open; it will not open otherwise.
6. **Security officers as monitor:** Security offices will check ID cards against a list to ensure authorized principals can access the server room. They also prevent spoofing attacks by unauthorized individuals.

By conducting all these checks, the monitors enforce complete mediation.

The part of the electronic voting system that cannot be enforced with a monitor is during the voting: There is no way to check if the right person voted since the voting is being done on personal devices.

## Part Two

# Rewriters

For this part of the project, you will identify which of the enforcement mechanisms designed previously are examples of rewriters. If none, identify one or more security policies in your system that could be enforced with a rewriter. For each, evaluate the trade-offs between using a rewriter and alternative enforcement mechanisms. Feel free to revise some of your designs from the previous module if appropriate.

Multi-level security is a security mechanism that allows classification of objects and users with labels based on the a system of hierarchical security levels and a system of non-hierarchical security categories which include sensitivity and integrity.

Multi-level security can be considered as a rewriter based on the classification of objected and users. When users what to read from or write to an object, there is a label placed on the user and the object according to the hierarchical security levels.  Thus a program has assign labels to the users and objects. This is a rewrite.  There is also the notion of reclassification when there is a drift of labels. That is when there is no clear relation among object and users. This is also a rewite.

## Part Three

# Isolation

The final step is to identify which of the enforcement mechanisms designed previously are examples of isolation. If none, identify one or more security policies in your system that could be enforced with isolation. Feel free to revise some of your designs from the previous module if appropriate. Would the security of your system benefit or suffer from being run on a cloud-based co-located virtual machine instead of on a dedicated server maintained by your organization?

Separation of duties and Role-based Access control are two example of enforcement mechanism that are examples of as isolation.

We have learned that

1. An isolation mechanism can prevent an environment from improperly influencing a system's operation.
2. An isolation mechanism also can prevent an environment from improperly being influenced by observing usage of system resources or by reading the system’s state.

Separation of duty, which is one of the enforcement mechanism in Mandatory Access Control, is a concept that involves assigning different duties and responsibilities to different individuals or team to reduce risk of fraud and error.

Assigning different duties and responsibilities to different individuals is an isolation mechanism that aims to ensure that no one individual can manipulate a system’s operation for the his or her gain.

Role-Based Access control is also one of the enforcement mechanism in Mandatory Access Control that restricts access based on an individuals role. For example in a company, there are roles such a C.E.O., accountant, security officer, operations manager, etc. These individuals have privileges and work based on their roles. This makes role-based access control  an isolation control mechanism.

*To submit this assignment, please refer to the instructions in the course.*