The University of Newcastle
School of Information and Physical Sciences

SENG2250/6250 System and Network Security
Week 7 Lab

Part 1: Multi-Factor Authentication

Multi-factor authentication (MFA) is a security approach that goes beyond using just a password to protect your accounts and information. With MFA, you need to provide two or more different types of evidence to prove your identity before you can access your account. This could involve:

- Something you know (like a password),
- Something you have (like a smartphone or a security token), or
- Something you are (like your fingerprint or face recognition).

MFA adds an extra layer of security, making it much harder for unauthorized individuals to gain access to your accounts, even if they know your password.

Case Study: Michael, a college student, utilizes the university's online portal to access their class materials, assignments, and grades. They frequently log in from various devices, including their laptop, smartphone, and the on-campus computer lab. In response to a recent data breach attack and the subsequent ransom payment, the university has taken the decision to implement a stringent cybersecurity policy. Your role as a 'Cybersecurity Engineer/Expert' involves devising a solution for the implementation of a multi-factor authentication (MFA) system to bolster the security of student accounts.

Q1: Could you propose an initial solution for the university to implement MFA on its online portal?

Q2: Could you conduct research on the implementation of Multi-Factor Authentication (MFA) at the University of Newcastle? Your task is to identify both the advantages and disadvantages of this specific implementation.

The University of Newcastle: Multi-Factor Authentication

https://www.newcastle.edu.au/current-staff/working-here/it-and-computing/information-security/multi-factor-authentication-mfa

Part 2: Access Control

Access control is a fundamental concept in cybersecurity that involves managing and regulating user permissions to access resources within a system. It aims to ensure that only authorized individuals or entities can access specific data, applications, or functionalities, while unauthorized users are restricted. ***Mandatory Access Control*** (MAC) is a specific access control model that enforces a centralized policy-driven approach to access permissions. In MAC, access decisions are primarily determined by the system's security policy rather than the discretion of individual users. ***Each resource is assigned a classification level, and each user or process is assigned a clearance level.*** Access is then granted based on predetermined rules, with ***higher classification levels requiring higher clearance levels for access***. This approach is often used in environments where confidentiality and data protection are paramount, such as government and military systems.

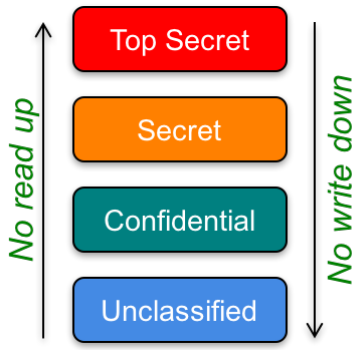


Figure: The Bell-LaPadula (BLP) Access Control Model

The BLP Model: The Bell-LaPadula (BLP) access control model focuses on maintaining ***data confidentiality***. Named after its creators, David Bell and Leonard LaPadula, this model is widely used in secure systems and environments where data protection is crucial. The BLP model operates on the principle of the "no read up, no write down" policy. This means that users with a certain security clearance (or classification level) are only allowed to read data at or below their clearance level. Similarly, they can only write data at or above their clearance level. The model enforces a strict hierarchy of security levels, preventing information from flowing in unauthorized directions.

Q1: Wite a program to implement the **BLP model** which takes as input: (1) access control matrix (ACM); (2) security label of subjects; (3) security label of objects. Output the accessible objects (with the permissions) of each subject. Test your program using the following input.

"-" means no permission is granted; "r" → read; "w" → write.

	Key File	Sys Log	Banner Info
Alice	rw	rw	rw
Bob	rw	r-	-w
Carrie	--	-w	-w

Access Control Matrix

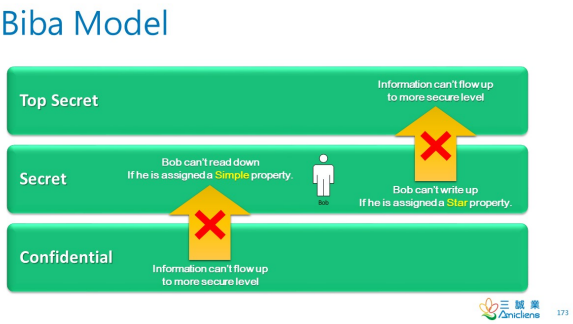
	Security Label
Alice	Top-Secret
Bob	Secret
Carrie	Secret

Subject Labels

	Security Label
Key File	Top-Secret
Sys Log	Secret
Banner Info	Unclassified

Object Labels

The Biba Model: The Biba Access Model is a comprehensive access control framework designed to ensure ***data integrity*** in computing systems. Named after its creator, Kenneth Biba, this model enforces a "no write up, no read down" policy. It prioritizes preventing unauthorized data modification while allowing read access to lower integrity levels. The Biba Model is particularly useful in environments ***where maintaining the integrity of data is critical***, such as financial systems or healthcare applications. It serves as a valuable tool for preventing malicious data tampering and unauthorized modifications, contributing to robust data security measures.



Q2: Wite a program to implement the **Biba model** which takes as input: (1) access control matrix (ACM); (2) security label of subjects; (3) security label of objects. Output the accessible objects (with the permissions) of each subject. Test your program using the following input.

"-" means no permission is granted; "r" → read; "w" → write.

	Key File	Sys Log	Banner Info
Alice	rw	rw	rw
Bob	rw	r-	-w
Carrie	--	-w	-w

Access Control Matrix

	Security Label
Alice	Top-Secret
Bob	Secret
Carrie	Secret

Subject Labels

	Security Label
Key File	Top-Secret
Sys Log	Secret
Banner Info	Unclassified

Object Labels

Part 3: **Role-based Access Control**

Role-Based Access Control (RBAC) is an access control model that simplifies the process of managing and enforcing permissions within an organization's digital systems. In RBAC, access to resources is determined by the roles that individuals hold within the organization, rather than assigning permissions to each user individually. Users are assigned specific roles based on their responsibilities and job functions. Each role is associated with a set of permissions that define what actions or operations can be performed. Instead of granting permissions directly to users, administrators assign users to roles, and those roles determine their access rights.

Refer to the file: "rbac.pdf" under Week07 Module.

Case Study: A large urban hospital, "CityCare Medical Center," is experiencing challenges in managing access to patient records and sensitive medical information. The hospital has multiple departments, including medical staff, administrative staff, and IT personnel. Ensuring the confidentiality of patient data while allowing appropriate access for different roles has become a priority. CityCare Medical Center decides to implement a Role-Based Access Control (RBAC) system to streamline access management and enhance data security.

Q1: Identify the roles and different accesses for CityCare Medical Center.