DSCI 519 LAB-2 Report: CyberCIEGE Introduction

Rishit Saiya (rsaiya@usc.edu)

The CyberCIEGE Introduction Part of the lab has gone through several basic elemental MAC scenarios which help organizations to maintain their sanctity of security. Some of the scenarios enforces the MAC policy using security labels and explores how security, particularly confidentiality and integrity is maintained under various circumstances. In here Part-1 is Mandatory Access Control Part and Part-2 is MAC Integrity Part as per the

Part - 1: Objective - 1: Connect the two LANs to the server

While doing the network configurations, LAN-1 and LAN-2 were connected using the Multi-Level Networks (mistake). Post this, I connected Joe's and Jill's systems with servers using LAN-1 and LAN-2 respectively. This was done using the Single-Level Network. It is so because Joe and Jill have two security levels named Unclassified and Secret assigned to sharing of a single object.

Part - 1: Objective - 2: Assign proper MAC labels

While assigning the MAC labels, both the LANs were assigned label: secret which eventually led to Joe accessing Jill's files (mistake). Similarly, also the case where both the LANs were assigned label: unclassified resulted in Jill's confidential files being read by Joe (mistake). When Joe (LAN-1) was assigned unclassified and Jill (LAN-2) was assigned secret, this led to a zombie computer gaining access to Jill's system and all the confidential secrets were leaked (mistake). Eventually, this led to the assumption that LAN-1 be unclassified and LAN-2 be secret. This is true because it supports the fact that Jill's network has to be at a higher security level than Joe's so the conditions BLP properties (simple security, *-property) are satisfied and the scenario isn't lost.

Part - 1, Q1. Ans: [***Secret Label***]
Part - 1, Q2. Ans: [***The confidential files can get leaked from Jill's system via various subversions. In practice of the game, all other assignments of labels resulted in scenarios as mentioned in the above paragraph such as unauthorized access to Joe, attack by zombie system, etc.***]

Part - 1: Objective - 3: Running the simulation for a while
The scenario is made to run in the simulation for some time which later leads up to winning it.

Part - 2: Objective - 1: Connect both LANs to server
While doing the network configurations, LAN-1 and LAN-2 were connected using the Multi-Level Networks (mistake). Post this, I connected Grace's and Sean's systems with servers using LAN-1 and LAN-2 respectively.

Part - 2: Objective - 2: Allocate the server connections with MAC Integrity and Secrecy labels
The referencing to understand the below table is as: LAN-1 (rows in table), LAN-2 (columns in table)
1 - {S, C}, 2 - {S, G}, 3 - {U, C}, 4 - {U, G} [Secrecy Labels: (S: Secret, U: Unclassified) | Integrity Labels: (C: Critical Operations, G: General Operations)].

In here, **E1** and **E2** are the error messages/prompt given by the game upon going through that particular scenario.
E1: Penalty -$20,000 per month: Sean cannot maintain Logistics Database
E2: Attacker has corrupted asset Critical Logistics Database.

A cell in the table represents the combination of connections to LAN-1 and LAN-2 respectively.

LAN-1/LAN-2	**1**	**2**	**3**	**4**
1	E1 (mistake)	E1 (mistake)	***Won*** (mistake)	E1 (mistake)
2	E1 (mistake)	E2 (mistake)	E2 (mistake)	E2 (mistake)
3	E1, E2 (mistake)	E2 (mistake)	E2 (mistake)	E2 (mistake)
4	E1 (mistake)	E1 (mistake)	***Won***	E1 (mistake)

I tried out all the possible scenarios of the combinations available for different connections. Out of 16 possible combinations, only 2 eventually win the game. Learning from this, the configuration where, LAN-1 is assigned Unclassified, General Operations and LAN-2 is assigned Unclassified, Critical Operations wins the scenario because Grace's secrecy level had to be same or higher than and integrity level same or lower than object (Critical Logistics DB)'s to maintain READ access to it. Also, Sean's secrecy level had to be the same or lower than integrity level, same or higher than Critical Logistics Database's to maintain EDIT/WRITE access. This is because of the BLP and Biba model properties.

Part - 2, Q2. Ans: ***[Secrecy Label: Unclassified, Integrity Label: General Operations]***
Part - 2, Q2. Ans: [***If the integrity label of Critical Operations is assigned to Grace, then she would have WRITE access to the object with high integrity which is Critical Logistics DB which is not the objective. All other scenarios led to loss of the game as shown above in the table. According to the game objective, Grace only possesses READ access to high integrity objects, and granting unwanted WRITE access can lead to unauthorized access like subversion like in one of the above lost cases in table.***]

Part - 2: Objective - 3: Wait and run the simulation

The scenario is made to run in the simulation for some time which later leads up to winning it.

The above steps enabled me to get a gist of the Mandatory Access Control policies of systems and organization secure as a whole. This lab helped to understand MAC and Integrity Labels' importance through the CyberCIEGE game. Sequential executions of above objectives with the aid of prompts from the game, helped to achieve the necessary objectives.