IST 623 - Introduction to Information Security

Homework Assignment 2

Marriah Lewis
Term: Summer, 2021
Topic: BLP model against Trojan Horse

Homework Assignment 2

Table of Contents

Homework Assignment 2

1 Introduction

The DAC (Discretionary Access Control) policy is vulnerable to a Trojan horse threat, whereas the MAC (Mandatory Access Control) policy can reduce the potential for a Trojan horse to compromise confidentiality. Bell and LaPadula created the BLP model to justify the MAC policy, which states that "information MUST NOT flow from High to Low." Below will convey how the BLP model operates against a Trojan horse. The following cases are:

1. Case 1. When the security level of the attacker is higher than that of the victim (e.g., top-secret attacker and unclassified victim)
2. Case 2. When the security level of the attacker is equal to that of the victim (e.g., top-secret attacker and top-secret victim)
3. Case 3. When the security level of the attacker is lower than that of the victim (e.g., unclassified attacker and top-secret victim)

Homework Assignment 2

2 Case Analysis

1. When the security level of the attacker is higher than that of the victim (e.g., top-secret attacker and unclassified victim)
2. When the security level of the attacker is equal to that of the victim (e.g., top-secret attacker and top-secret victim)
3. When the security level of the attacker is lower than that of the victim (e.g., unclassified attacker and top-secret victim)

2.1 Case Summary Table

Possible Cases	**Direction of Information Flow**	**Is this information flow allowed by MAC?**	**Can the Trojan horse send any information from the Victim to Attacker?**	**As a result, is there any security violation based on MAC in the case?**
Case 1	Attacker **--->** Victim	NO	Yes, the information is flowing low to high.	No, the information is flowing from object to subject within the limits of the MAC policy.
	Attacker **<---** Victim	YES		
Case 2	Attacker **--->** Victim	YES	Yes, the information is flowing from high to high.	No, the information is flowing from object to subject within the limits of the MAC policy.
	Attacker **<---** Victim	YES		
Case 3	Attacker **--->** Victim	YES	No, the information is flowing from high to low.	Yes, the information is flowing from object to subject outside the limits of the MAC policy.
	Attacker **<---** Victim	NO		