IST 623 - Intro to Information Security

Homework Assignment 2

Ryan Timbrook
NetID: RTIMBROO
Term: Winter, 2020
Date: 1/28/2020
Topic: BLP model against Trojan Horse

Table of Contents

1 Introduction

DAC (Discretionary Access Control) policy is vulnerable to the Trojan horse attack, while the **MAC** (Mandatory Access Control) **policy can limit the confidentiality violation that a Trojan horse may cause**. The BLP model was introduced by Bell and LaPadula in order to support the MAC policy, whose fundamental goal is "***information MUST NOT flow from High to Low***". Meaning, even if there is an information flow, if it is not from High to Low, there is no security violation.

Discuss how the **BLP model** works against a **Trojan horse**, considering the following three cases. (MAC policy and BLP model focus on Confidentiality.)

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)

Confidentiality: Protects information from unauthorized disclosure (means that people who intercept messages cannot read them)

Trojan horse: A nonmobile malware program that hides itself by deleting a system file and taking on the system file's name.

1.1 Scope

In each case, consider the two directions of information flow:

1. From Attacker (Subject) to Victim (Object) - (Transfer the Trojan horse to the victim)

2. From Victim (Object) to Attacher (Subject) - (Transfer the target victim's information to the attacker)

Then, in each case analyze if the Trojan horse is allowed to work as planned. (assume the trojan horse is already loaded on the victim's machine.)

Finally, if the Trojan horse is running as planned, analyze if there is any security violation according to the MAC policy.

1.2 Assumptions

The trojan horse needs only read privilages of the target object based on the confidentiality property being analyzed in this exercise.

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 informat flow allowed by MAC?	Can the Torjan horse send any information from the Victim to Attacker? (assume it's already installed)	As a result, is there any security violation based on MAC in the case?
Case 1	Attacker(S-H) **--(Trojan Horse)-->** Victim(O-L) Access Type: **Write**	No	**Yes**, because information is flowing from Low to High policy acess levels.	**No,** because the information is flowing in a direction from Object to Subject that is within the limits of the MAC policy.
	Attacker(S-H) **<--(Info)--** Victim(O-L) Access Type: **Read**	Yes		
Case 2	Attacker(S-H) **--(Trojan Horse)-->** Victim(O-H) Access Type: **Write**	Yes	**Yes**, because the information is flowing from High to High policy access levels.	**No**, because the information is flowing in a direction from Object to Subject that is within the limits of the MAC policy.
	Attacker(S-H) **<--(Info)--** Victim(O-H) Access Type: **Read**	Yes		
Case 3	Attacker(S-L) **--(Trojan Horse)-->** Victim(O-H) Access Type: **Write**	Yes	**No**, because the information is flowing from High to Low policy access levels which	**Yes**, because the information is flowing a direction from Object to Subject that is outside of
	Attacker(S-L) **<--(Info)--** Victim(O-H)	No		

	Access Type: **Read**		MAC protects against.	the limits allowed by the MAC policy. Information can NOT flow from High to Low.