Syracuse University

IST-623 Assignment#2 BLP Analysis

ThulasiRam RuppaKrishnan

IST 623

Professor Joon Park

BLP Case Study:

We can walkover 3 scenarios from the below table and validate them according to MAC policy

Possible Cases	Direction of Information flow	Is this information flow allowed by MAC?	Can the Trojan horse send any information from Victim to Attacker?	As a result, is there any security violation based on MAC in the case?
Case 1 (top-secret attacker and unclassified victim)	(H) Attacker → Victim (L)	No	Yes	No
	(H) Attacker ← Victim (L)	Yes		
Case 2 (top-secret attacker and top-secret victim)	(H) Attacker → Victim (H)	Yes	Yes	No
	(H) Attacker ← Victim (H)	Yes		
Case 3 (unclassified attacker and top-secret victim)	(L)Attacker → Victim (H)	Yes	No	No
	Attacker ← Victim (H)	No		

The simple-security property solves the obvious problem that subjects should not read data that is above their security class. That is, the BLP policy identifies unauthorized subjects for data as subjects whose security class is dominated by the object's security class. Thus, the simple-security property prevents unauthorized subjects from receiving data.

The*-security property handles the more subtle case that results when the user runs malware, such as a Trojan horse. This property prevents any process from writing secrets to a security class that they dominate, so even if the process is a Trojan horse, it cannot leak data to unauthorized subjects.

Based on the above MAC policy, please find my rationalization on Case 1, Case 2 and Case 3 as follows

Case 1:

According to MAC policy information flow from High to Low is not allowed but from Low to High and High to High is allowed. In this case Attacker is top-secret (High) and Victim is unclassified (Low), hence (H) Attacker → Victim (L) is not allowed whereas (H) Attacker ← Victim (L) is allowed. Also, Trojan horse can send information from Victim to Attacker, if the attacker has got some other means to install Trojan Horse in Victim's machine. According to MAC policy, this information flow is accepted and as a result there is no security violation

Case 2:

According to MAC policy information flow from High to Low is not allowed but from Low to High and High to High is allowed. In this case both Attacker and Victim are top-secret (High), hence (H)Attacker → Victim(L) and (H)Attacker ← Victim(L) is allowed. Also, Trojan horse can send information from Victim to Attacker, as the Attacker can also send information to Victim and install Trojan Horse in Victim's machine. According to MAC policy, this information flow is accepted and as a result there is no security violation

Case 3:

According to MAC policy information flow from High to Low is not allowed but from Low to High and High to High is allowed. In this case Victim is top-secret (High) and Attacker is unclassified (Low), hence (L)Attacker → Victim(H) is allowed whereas (L)Attacker ← Victim(H) is not allowed. Also, Trojan horse **cannot** send information from Victim to Attacker, even if the attacker can send information to victim and install Trojan Horse in victim's machine. According to MAC policy, this information flow from Victim to Attacker is not allowed and as a result there is no security violation.