Assignment#2

- Topic: BLP model against Trojan Horse
- Deliverables: 1) Fill in the template above with your case analysis; 2) Discuss the results of your analysis in 300 words.
- Submission: Attach one PDF file.
- Due Date: **Submit your work by** Next Week's Live Session.

Dear all,

First of all, please be informed that this assignment is an individual submission. Please **DO NOT POST** your comments in a public space. Instead, submit your individual report by Next Week's Live Session.

In the previous class we learned that the 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. This week we just learned that the BLP model was introduced by Bell and LaPadula in order to support the MAC policy. Now let us discuss how the BLP model works against a Trojan horse, considering the following three cases. (Remember that the MAC policy and BLP model focus on Confidentiality.)

In each case, you should consider the two directions of information flow: "from Attacker to Victim" and "from Victim to Attacker." (The former is needed to transfer the Trojan horse to the victim, while the latter is needed to transfer the target's information to the attacker.) Then, in each case you should analyze if the Trojan horse is allowed to work as planned. Finally, if the Trojan horse is running as planned, analyze if there is any security violation according to the MAC policy, whose fundamental goal is "information MUST NOT flow from High to Low." (This means, even if there is an information flow, if it is not from High to Low, there is no security violation. For instance, Low to High or High to High should be fine according to the policy.)

For your understanding I summarize the three possible cases as follows and provide the template for the expected deliverables below. In your Discussion #2, you are required to complete the table with your own analysis.

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

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)

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

Note You need to fill in the entire table below with your answers (i.e., Yes or No) and **explain your rationale for each case**.

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	Attacker → Victim	**Yes/No**	**Yes/No**	**Yes/No**
	Attacker ← Victim	**Yes/No**		
Case 2	Attacker → Victim			
	Attacker ← Victim			
Case 3	Attacker → Victim			
	Attacker ← Victim			