IMT4123 - Assignment 2

Ole André Hauge

January 8, 2022

Task 1

Why is it meaningless to have compartments at the UNCLASSIFIED level (such as (UNCLASSIFIED, NUC) and (UNCLASSIFIED, EUR))?

Answer: Compartments are used to restrict access to certain security levels. The information at the UNCLASSIFIED level contains data that every user can access, not any confidential data. Thus, having compartments at the UNCLASSIFIED level would be contradictory.

Task 2

Assume a confidentiality policy. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

Simple Security Condition: S can read O iff S dom O and S has discretionary read access to O.

**-property:* S can write to O iff O dom S and S has discretionary write access to O.

1. Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).

   Answer: Given the *scc* and **-property* Paul is not allowed to access the document with read or write access, as he does not dominate the document:

   SECRET $\leq$ TOP SECRET and { C } $\subseteq$ { A, C } but { B } $\not\subset$ { A, C }.

2. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).

   Answer: Anna is not allowed to access the documents as she only has read access, while the document requires write access. Thus, she does not dominate the document and is refused access:

   CONFIDENTIAL $\leq$ CONFIDENTIAL and { B } $\not\subset$ { C }.

3. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).

   Answer: Jesse is allowed to read the document as he dominates the document. But he is not allowed to write to the document, as the *-property states that, in case of write access, the object should dominate the subject:

   CONFIDENTIAL $\leq$ SECRET and { C } $\subseteq$ { C }.

4. Samuel, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).

Answer: Samuel is allowed to read but not write to the document as he only dominates the document, but the document does not dominate him:

CONFIDENTIAL $\leq$ TOP SECRET and { A } $\subseteq$ { A, C }.

5. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).

   Answer: Robin is not allowed to read the document, but he can write to it as the document dominates him (*given that* { B } $\not\subset \emptyset$ *can be seen as dominates?*):

   CONFIDENTIAL $\not\leq$ UNCLASSIFIED and { B } $\not\subset \emptyset$.

Task 3

Declassification effectively violates the *-property of the Bell-LaPadula Model. Would raising the classification of an object violate any properties of the model? Why or why not?

Answer: We can see that this property will be broken based on tranquillity, which stipulates that subjects and objects may not modify their security level once they are instantiated. Raising an object's security level means that information that was previously available only to those with no-high level clearance is now considered high level, yet this knowledge is already known. The no-read-up property is now broken because low-level subjects already have this information, which is now categorized as high-level.

Task 4

In the DG/UX system, why is the virus prevention region below the user region?

Answer: By implementing a mechanism to disable write-down, the integrity of the programs in the virus prevention region is ensured. These programs can only be read or executed; they cannot be overwritten.

Task 5

In the DG/UX system, why is the administrative region above the user region?

Answer: This is done as a security mechanism to prevent read-up. As a result, the administrator region's confidentiality is preserved, and users are unable to view or access sensitive or critical information such as that required for authentication.

Task 6

Prove Theorem 5.4 in edition 2. (Hint: Proceed along lines similar to the proof of Theorem 5.3.)

Theorem 5.4: $\sum(R,\ D,\ W,\ z_0)$ satisfies the *-property relative to $S' \subseteq$ S for any secure state z_0 if and only if, for every action $(r,\ d,\ (b,\ m,\ f,\ h),\ (b',\ m',\ f',\ h'))$, W satisfies the following for every s $\in S'$:

(a) Every $(s,\ o,\ p) \in b - b'$ satisfies the *-property with respect to S'.

(b) Every $(s,\ o,\ p) \in b'$ that does not satisfy the *-property with respect to S' is not in b.

Answer: As both theorem 5.3 and 5.4 in edition 2 have similar conditions (a and b) which have to be satisfied, the proof of theorem 5.4 can be based on the proof of theorem 5.3. I have taken the liberty to copy the proof of theorem 5.3 and modify it to fit theorem 5.4. I did so to practice the correct wording, syntax, and structuring of the proof. In doing so I also gained a better understanding of the *simple security condition* and the **-property.*

Proof Let $(x,\ y,\ z) \in \sum(R,\ D,\ W,\ z_0)$ and write $z_t = (b_t,\ m_t,\ f_t,\ h_t)$ for $t \in$ N.

($\Rightarrow$) By contradiction. Without loss of generality, take $b = b_t$ and $b' = b_{t-1}$. Assume that $\sum(R,\ D,\ W,\ z_0)$ satisfies the *-property for some secure state z_0, and that either some $(s,\ o,\ p) \in b - b' = b_t - b_{t-1}$ does not satisfy the *-property with respect to S' or some $(s,\ o,\ p) \in b' = b_{t-1}$ that does not satisfy the *-property with respect to S' is in $b = b_t$. If the former, there is some $(s,\ o,\ p) \in b_t$ that does not satisfy the *-property with respect to S', because $b_t - b_{t-1} \subseteq b_t$. If the latter, there is some $(s,\ o,\ p) \in b_{t-1}$ that does not satisfy the *-property with respect to S' but that is in b_t. In either case, there is some $(s,\ o,\ p) \in b_t$ that does not satisfy the star property relative to S', which means that $\sum(R,\ D,\ W,\ z_0)$ does not satisfy the *-property for some secure state z_0, contradicting the hypothesis.

($\Leftarrow$) By induction on t.

Basis. $z_0 = (b_0,\ m_0,\ f_0,\ h_0)$ is secure, by the hypothesis of the claim.

Induction Hypothesis. $z_{i-1} = (b_{i-1},\ m_{i-1},\ f_{i-1},\ h_{i-1})$ is secure for $i < t$.

Induction Step. Let $(x_t,\ y_t,\ z_t,\ z_{t-1}) \in$ W.

By (a), every $(s,\ o,\ p) \sum b_t$ - b_{t-1} satisfies the *-property with respect to S'.

Let $b_{t-1} = \{(s,\ o,\ p) | (s,\ o,\ p) \in b_{t-1} \wedge (s,\ o,\ p)$ does not satisfy the *-property with respect to $S'\}$.

By (b), $b_t \cap b_{t-1} = \emptyset$; so, $b_{t-1} \cap (b_t \cap b_{t-1}) = (b_{t-1} \cap b_t) \cap b_{t-1} = \emptyset$.

This means that if $(s,\ o,\ p) \in b_t \cap b_{t-1}$, then $(s,\ o,\ p) \notin b_{t-1}$ and so $(s,\ o,\ p)$ satisfies the *-property. Hence, if $(s,\ o,$ p$) \in b_t$, then either $(s,\ o,\ p) \in b_t \cap b_{t-1}$ or $(s,\ o,\ p) \in b_t$ - b_{t-1}.

In the first case, the induction hypothesis ensures that $(s,\ o,\ p)$ satisfies the *-property in respect to S'.

In the second case, (a) ensures that $(s,\ o,\ p)$ satisfies the *-property in respect to S'. Hence, $z_{i-1} = (b_{i-1},\ m_{i-1},\ f_{i-1},\ h_{i-1})$ is secure.

This completes the proof.

Task 7

Consider Theorem 5.6. Would the theorem hold if the requirement that z_0 be a secure state were eliminated? Justify your answer.

Theorem 5.6. ***Basic Security Theorem***: $\sum(R,\ D,\ W,\ z_0)$ is a secure system if z_0 is a secure state and W satisfies the condition of Theorems 5.3, 5.4, and 5.5

Answer: If the requirement for z_0 to be a secure state was eliminated, it would mean that the conditions for theorem 5.3, 5.4, and 5.5 of which theorem 5.6 is reliant upon, are not met. If we are to assume that the requirement for z_0 to be a secure state was eliminated for all the related theorems as well, then that would mean that there would be no way to say if we had a secure state or not, and thus be hard to state if we have a secure system. This is given by the fact that a state is secure if the only permitted access modes between subjects and objects are controlled by a security policy. If the initial state, z_0, is not a secure state then there would be no way of knowing if the transition between states was or are secure. Theorem 5.3, 5.4, and 5.5 rely on the states of the system to define it as secure, *"[...] satisfy the conditions for any state iff, for every action (r,d,(b,m,f,h),(b′,m′,f′,h′)), W satisfies the [...]"*, which mean that if there is no way ensure that the system is in a secure state at the beginning, it will be hard to identify if the system is secure after transitions.