SUTD 51.505: 𝔽oundations of Cybersecurity (2018)

Exercise Sheet 2
September 21, 2018

- List your names (max 3 members for each group) on the answer sheet, **if you have actually worked on the exercises.**
- Answer questions in the same order as in the exercise sheet.
- Type in 12pt font, with 1.5 line spacing.
- There can be multiple acceptable answers. Justify carefully your reasoning.
- Go to the point, avoid copying verbatim definitions from the slides or the book.
- Submit your classwork and homework solutions (in pdf file) to eDimension by the deadlines below. Each group only needs one submission.
- Grading: total 100 points for each classwork and homework, each exercise has equal points in the same classwork and homework.

Classwork due on Friday September 21, 10:00 PM

Exercise 1

Let a password checking program *auth* be a mechanism defined as $auth(u, p, d) = 1$ if the pair $(u, p) \in d$, and $auth(u, p, d) = 0$ otherwise. (u = username, p = password, d = database.) Is it a secure mechanism in the sense of Defintion 4-19 in Bishop's book $c(u, p, d) = (u, p)$? Why or why not?

Exercise 2

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.

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

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

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

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

Exercise 3

Give an example that demonstrates the integrity level of subjects decreases in Biba's low-water-mark policy. Under what conditions will the integrity level remain unchanged?

Exercise 4

Suppose a system used the same labels for integrity levels and categories as for security levels and categories. Under what conditions could one subject read an object? Write to an object?

Homework due on Friday September 28, 6:59 PM

Exercise 1
Prove Theorem 4–1 of Bishop's. Show all elements of your proof.

Theorem 4–1. Let m_1 and m_2 be secure protection mechanisms for a program p and policy c. Then $m_1 \cup m_2$ is also a secure protection mechanism for p and c. Furthermore, $m_1 \cup m_2 \approx m_1$ and $m_1 \cup m_2 \approx m_2$.

Exercise 2
Expand the proof of Theorem 4–2 of Bishop's to show the statement, and the proof, of the induction.

Theorem 4–2. For any program p and security policy c, there exists a precise, secure mechanism m^* such that, for all secure mechanisms m associated with p and c, $m^* \approx m$.

Exercise 3
In the DG/UX system, why is the virus prevention region below the user region? Why is the administrative region above the user region?

Exercise 4
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?

Exercise 5
Prove Theorem 6–1 of Bishop's for the strict integrity policy of Biba's model.

Theorem 6–1. If there is an information transfer path from object $o_1 \in O$ to object $o_{n+1} \in O$, then enforcement of the low-water-mark policy requires that $i(o_{n+1}) \leq i(o_1)$ for all $n > 1$.

Exercise 6
Explain why the system controllers in Lipner's model need a clearance of (SL, {D, PC, PD, SD, T}).