SUTD 51.505: 𝔽oundations of Cybersecurity (2018)

**Exercise Sheet 1**
September 14, 2018

- List your names (max 3 members for each group) on the answer sheet. 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.

## **Classwork** due on Friday September 14, 10:00 PM

---

**Exercise 1**
Classify each of the following as a violation of confidentiality, of integrity, of availability or of some combination thereof.

a) John copies Mary's Foundations of Cybersecurity homework.

b) Paul crashes Linda's iPhone remotely through Wi-Fi.

c) Carol changes the amount of Angelo's check from 1฿ to 100฿.

d) Gina forges Roger's signature on a deed.

e) Jonah obtains Peter's credit card number and has the credit card company cancel the card.

f) Henry guesses Julie's twitter password and tweets on her behalf.

**Exercise 2**
With the following mechanisms being implemented, state what policy or policies they might be enforcing and what informal security requirement might have inspired such policies.

a) A password changing program will reject passwords that are less than five characters long or that are found in the dictionary.

b) The login program will disallow logins of any students who enter their passwords incorrectly three times.

c) The permissions of the file containing Carol's homework will prevent Robert from cheating and copying it.

d) When too many connections to Facebook are detected from students enrolled to the Foundations of Cybersecurity class on Fridays from 7:00 PM to 10:00 PM, bandwidth should be throttled.

e) eDimension will stop accepting homework submissions after the due date.

**Exercise 3**

The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.

**Exercise 4**

Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file *alicerc*, and Bob and Cyndy can read it. Cyndy can read and write Bob's file *bobrc*, but Alice can only read it. Only Cyndy can read and write her file *cyndyrc*. Assume that the owner of each of these files can execute it.

a) Create the corresponding access control matrix.

b) Cyndy gives Alice permission to read *cyndyrc*, and Alice removes Bob's ability to read *alicerc*. Show the new access control matrix and spell out the commands needed to perform these changes.

**Exercise 5**

Consider the set of rights {*read, write, execute, append, list, modify, own*}.

a) Using the syntax in Section 2.3 of Bishop's, write a command *delete_all_rights(p,q,s)*. This command causes $p$ to delete all rights the subject $q$ has over and object $s$.

b) Modify your command so that the deletion can occur only if $p$ has *modify* rights over $s$.

c) Modify your command so that the deletion can occur only if $p$ has *modify* rights over $s$ and $q$ does *not* have *own* rights over $s$.

**Homework** due on Friday September 21, 6:59 PM

---

**Exercise 1**
Is it possible to design and implement a system in which no assumptions about trust are made? Why or why not?

**Exercise 2**
A respected computer scientist has said that no computer can ever be made perfectly secure. Why might she have said this?

**Exercise 3**
Give examples for situations in which:

a) A compromise of confidentiality leads to a compromise in integrity and vice versa.

b) A compromise of confidentality leads to a compromise in availability and vice versa.

c) A compromise of integrity leads to a compromise in availability and vice versa.

**Exercise 4**
The query-set-overlap mechanism requires a history of all queries to the database. Discuss the feasibility of this control. In particular:

a) How will the size of the history affect the response of the mechanism?

b) How practical is a system that enforces this mechanism?

**Exercise 5**
Let $c$ be a copy flag and let a computer system have the same rights as in Exercise 5 of the Classwork.

a) Using the syntax in Section 2.3 of Bishop's, write a command *copy_all_rights(p,q,s)* that copies all rights that $p$ has over $s$ to $q$.

b) Modify your command so that only those rights with an associated copy flag are copied. The new copy should not have the copy flag.

c) In part b), what conceptually would be the effect of copying the copy flag along with the right?

**Exercise 6**
This exercise asks you to consider the consequences of not applying the principle of attenuation of privilege to a computer system.

a) What are the consequences of not applying the principle at all? In particular, what is the maximal set of rights that subjects within the system can acquire (possibly with the cooperation of other subjects)?

b) Suppose attenuation of privilege applied only to *access* rights such as *read* and *write*, but not to rights such as *own* and *grant_rights*. Would this ameliorate the situation discussed in part a)? Why or why not?

c) Consider a restricted form of attenuation, which works as follows. A subject $q$ is attenuated by the maximal set of rights that $q$, or any of its ancestors, has. So, for example, if any ancestor of $q$ has $r$ permission over a file $f, q$ can also $rf$. How does this affect the spread of rights throughout the access control matrix of the system? Develop an example matrix that includes the ancestor right, and illustrate your answer.