SUTD 51.505: 𝔽oundations of Cybersecurity (2018)

Exercise Sheet 3
September 28, 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 28, 10:00 PM

Exercise 1
Draw a finite state machine depicting the semantics of the 2-bit machine in the following Table 8-1 (State Transition Function) of Bishop's. Is this system secure? If yes, explain why. If not, show a counter example.

Commands	Input states (*H*, *L*)			
	(0, 0)	(0, 1)	(1, 0)	(1, 1)
xor0	(0, 0)	(0, 1)	(1, 0)	(1, 1)
xor1	(1, 1)	(1, 0)	(0, 1)	(0, 0)

Exercise 2
Consider the instruction `x:= y + z`. Assume that `x` does not exist in state s and that the probability distribution of y and z is uniform over their domain $y, z \in \{0, 1\}$. Confirm that information flows from `y` and `z` to `x` by computing $H(y_s|x_t), H(y_s), H(z_s|x_t)$ and $H(z_s)$ and showing that $H(y_s|x_t) < H(y_s)$ and $H(z_s|x_t) < H(z_s)$.

Exercise 3
Consider the *auth* mechanism from Classwork Exercise 1 (Week 2). Write that mechanism as pseudo-code, where the value of the output variable o equals to 1 if the username and password are correct and 0 otherwise. Is there an information flow from d to o? Would a compiler or enforcement time mechanism have detected this and if so how? What is the conditional entropy of o in terms of the secret d?

Homework due on Friday October 5, 6:59 PM

Exercise 1

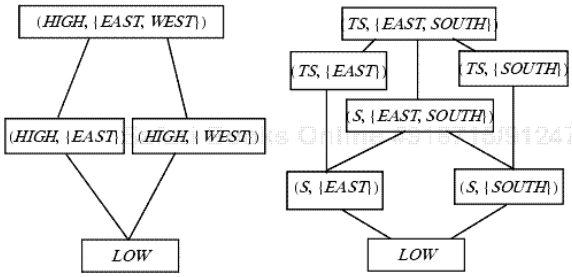
Consider a modification of the 2-bit machine of Classwork Exercise 1 (Week 3), where Holly can only alter the H bit and Lucy only the L bit. (Assume that the projection function for Lucy only shows the outputs she is supposed to see, and therefore has length equal to the number of commands issued by her.)

Draw the corresponding state machine. Is this system secure? If yes, expalin why. If not, show a counter example.

Exercise 2

Draw the lattice described in the following example of Bishop's (Section 8.1.1).

EXAMPLE: Consider two systems with policies modeled by the Bell-LaPadula Model. One, system *allie*, has two security levels, LOW and HIGH, and two categories, EAST and WEST. The other, system *son*, has three security levels, LOW, S, and TS, and two categories, EAST and SOUTH. (The two EAST categories have the same meaning, as do the two LOW security levels.) Figure below shows the lattices of these two systems. The relevant issues are (1) how S and TS compare with HIGH and (2) how SOUTH compares with EAST and WEST.



Assume that HIGH corresponds to a level between S and TS, and that SOUTH is a category disjoint from EAST and WEST. Then the composed lattice has four security levels (LOW, S, HIGH, and TS) and three categories (EAST, WEST, and SOUTH).

Exercise 3

Consider the following code snippet:

```
y := 0;
z := 0;
if x = 0 then z := 1;
if z = 0 then y := 1;
```

Assume x is a secret (high) variable, and y, z are public (low). Is there an information flow from x to y? If so why, and could have this been detected at compile

or runtime?

Exercise 4

Let *auth_long* be a modification of the password checker of Classwork Exercise 1 (Week 2), which, for efficiency reasons will now work as follows: if a username is found matching the input u, then the password p will be compared characte by character with the stored password p'. If a character does not match, then the program will stop executing. For instance, if supplied password p is *f0und4710n5* and the correct password p' is *f0undat10n4l*, then the password checker will stop executing after comparing the first 6 characters of p'.

Is there an information flow from d to the user's output? How is this different from the case of *auth* (of Week 2)?