CS590 DSP: Data Security and Privacy **Spring 2022**

Homework #2

Due date & time: 11:59pm on February 15, 2022. Please hand in your homework on Brightspace.

Late Policy: You have three extra days in total for all your homeworks and projects. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: (1) The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 0 (5 pts) Answer the following question about crypto background.

- Have you taken CS 555: Cryptography in Purdue? If so, which semester?
- How well do you know the following concepts: (1) Oblivious Transfer, (2) Yao's Garbled Circuit protocol, (3) the GMW protocol (Goldreich, Micali, and Wigderson), (4) Private Information Retrieval?
- For each topic, which of the following statement can best describe your familiarity: (1) you never heard of it, doesn't know how it works; (2) know the high-level idea, but not the details; (3) know it well enough to be able to implement it if needed.

Problem 1 (12 pts)

- Explain the following terminologies: discretionary access control, mandatory access control, role-based access control, trusted computing base.
- What are the differences between the concept of "trusted" and "trustworthy"?
- A hot term in recent years is "trustless systems". Do some investigation online and explain what it means.

Problem 2 (20 pts) BLP is designed to enable one to formally show that a computer system can securely process classified information. This problem asks you to assess how well this is done.

- (1) State the BLP notion of security. Start with "We say a system is BLP-secure when $\cdots$. "
  (2) Identify three reasons why a system whose specification is shown to satisfy the BLP notion of security can still have illegal information flows.
  (3) For each reason identified above, use one sentence to explain whether/how they can be addressed (either by enhancing the BLP model, or by identifying other components)?
- (4) In terms of modeling a system, how do BLP and the Goguen-Meseguer non-interference model differ?
  (5) Give an example that Goguen-Meseguer model allows an operation, but the BLP model would prevent. Which of BLP and Goguen-Meseguer better matches the high-level intuition of security?
  (6) Give an example that the BLP model allows an operation, but the Goguen-Meseguer model would prevent. Which of BLP and Goguen-Meseguer better matches the high-level intuition of

security?

Question 3 (15 pts) Explore the Biba integrity model.

Observe that in integrity protection, when a low-level subject attempts to write to a high-level object, there are three choices: (W1) Forbid it; (W2) Allow it, but drops the integrity level of object after the writing; (W3) Allow it, without changing the object's level.

Also, when a high-level subject attempts to read a low-level object, there are three choices; (R1) Forbid it; (R2) Allow it, but drops the integrity Level of subject after reading; (R3) Allow it, without dropping the subject's integrity level.

- **Describe the five integrity policies in the Biba model by identifying which of the three choices for reading and three choices for writing are used in each of the five models.**
- **For each of the six choices, identify (a) which kind of trust (if any) it places on the subject; (b) whether the object's integrity level indicate quality or importance?**

Problem 4 Clark-Wilson (15 points) Read the Clark-Wilson paper.

- D.D. Clark and D.R. Wilson. "A Comparison of Commercial and Military Computer Security Policies".

Answer the following questions.

- **How would you compare the Biba integrity models and the Clark-Wilson integrity model?**
- **List the two or three most significant new insights you took away from the Clark-Wilson paper and the most significant flaws or weaknesses of it (if any).**

Problem 5 (5 pts) Given three boolean input variables x, y, and z, each taking values in {TRUE, FALSE}. For each of following, answer whether there is information flow in the non-deducibility sense. (Circle yes or no.)

- $w = (x \text{ OR } y) \text{ AND } z$

  yes / no there is information flow between x and w

  yes / no there is information flow between z and w

  yes / no there is information flow between $\{x, y\}$ and w
- $w = x \text{ XOR } y \text{ XOR } z$

  yes / no there is information flow between $\{x, y\}$ and w

  yes / no there is information flow between $\{y, z\}$ and w

Problem 6 (12 pts) Assume that x, y, z are variables that take values either 0 or 1. Answer the following questions.

1. Give a deterministic function $f(x, y, z)$ such that $w = f(x, y, z)$ satisfies the following conditions: There **exists no** information flow in the non-deducibility sense between x and w, between y and w, between z and w, between $(x + y)$ and w, between $(x + z)$ and w, and between $(y + z)$ and w. But there **exists** information flow in the non-deducibility sense between $(x + y + z)$ and w.
2. Give a deterministic function $f(x, y, z)$ such that $w = f(x, y, z)$ satisfies the same conditions as above, except that now we require that there **exists** information flow in the non-deducibility sense between $(y + z)$ and w.
3. Prove that there does not exist a deterministic and non-constant function $f(x, y, z)$ (the function returns as least two values) such that there **exists no** information flow in the non-deducibility sense between $(x + y + z)$ and $w = f(x, y, z)$.

Problem 7 (16 pts) Read Part I.A of the "The Protection of Information in Computer Systems" by Saltzer and Schroeder.

For each of the 8 principles: (1) write your understanding of the principle; (2) if appropriate, give an instance where it should be applied but is not; (3) if available, give an instance where the principle is applied.