School of Computing & Information Technology

CSCI262 System Security
SIM-2024-S4

Assignment 2 (12 marks, worth 12%)

Due date: November 14, 2024 9:00 pm Singapore time.

Make sure you include referencing for answers where it would obviously be needed.

1. You have two puzzles with parameters as follows:

   Puzzle A: One sub–puzzles. $k = 6$.

   Puzzle B: Six sub-puzzles. $k = 4$.

   You should provide, for both cases other than part (b), the following:

   (a) The distribution of the number of cases that require each number of hashes. **1.0 Mark**

   (b) Explain the method you used to obtain your distributions. Don't go into too many details or show working, it's more "I wrote a C++ program to ... and then using ... I ...". **0.5 Mark**

   (c) A graph of the distribution of the data above. **0.5 Mark**

   (d) The average number of hashes needed. **0.5 Mark**

   (e) The standard deviation for the distribution of the number of hashes needed. **0.5 Mark**

   You should assume that if there are N possible solutions you check the N^{th} by hashing even if all others have failed and there has to be a solution.

2. In a TCP SYN spoofing attack, the attacker seeks to exhaust a server's connection request table, preventing it from responding to legitimate connection requests. Here are the details of this scenario:

   i. **Server Configuration:** The server has a table that can hold up to 512 TCP connection requests.

   ii. Retry and Timeout Mechanism:

   - If the server does not receive an ACK in response to its SYN-ACK, it retries the SYN-ACK five times, with each retry occurring at 30-second intervals.

   - After five retries without an ACK, the server purges the request, meaning each connection request remains in the table for:

$$6 \times 30\ seconds = 180\ seconds\ or\ 3\ minutes$$

   iii. **Attack Assumptions:** No countermeasures are in place against this attack, and the attacker has initially filled the connection request table completely.

Problem Statement:

1. **Attack Rate Requirement:**

   - At what rate (in requests per minute) must the attacker continue sending TCP connection requests to keep the table full? **0.5 Mark**

2. **Bandwidth Consumption:**

   - Assuming each TCP SYN packet is 64 bytes in size, what is the bandwidth consumed by the attacker in bits per second? **0.5 Mark**

3. Consider the database below and answer the questions based on it.

Name	Gender	School	Position	Salary
Adams	Male	Computing	Lecturer	$70,000
Bob	Male	Mathematics	Lecturer	$60,000
Carol	Female	Mathematics	Lecturer	$100,000
Debbie	Female	Computing	Lecturer	$68,000
Edward	Male	Physics	Lecturer	$72,000
Fiona	Female	Physics	Lecturer	$80,000
Gary	Male	Computing	Administrator	$50,000
Humphry	Male	Mathematics	Lecturer	$72,000
Iris	Female	Computing	Tutor	$18,000
Jeff	Male	Physics	Administrator	$80,000
Karen	Female	Mathematics	Lecturer	$90,000
Lucas	Male	Computing	Lecturer	$70,000
Mandy	Female	Engineering	Tutor	$12,000

Assume you only have a statistical interface, so only aggregate queries will be successful. You know Debbie is a female Computing Lecturer. The questions below explore how we might determine her salary using inference, in the presence of various query size restrictions.

(a) Assume there is no limit on the query size. Give a sequence of two queries that will identify the salary of Debbie. **1.0 Mark**

(b) Suppose that there is a lower and upper query size limit that satisfies

$$k \leq |X(C)| \leq N - k$$

with $k = 2$. Show a sequence of queries that could be used to determine Debbie's salary. **1.5 Mark**

4. Methods of protecting against denial of service (DoS) attacks:

(a) Comparison of Protection Methods:

Describe how SYN cookies and client puzzles protect against denial of service (DoS) attacks. In what ways are these methods similar, and how do they differ in their approach and application? **1.0 Mark**

(b) Properties of Client Puzzles:

What are the main properties that make client puzzles effective as a protection method? Describe these desirable properties and provide examples where appropriate. **1.0 Mark**

5. Analyzing the Spread and Counteraction of Worms X and W

(a) **Initial Spread of Worm X**:

Worm X spreads from each infected computer to one previously uninfected computer each hour. Starting from **t = 0**, where only one computer is infected $(N = 1)$, complete the following tasks:

- Construct a table showing the number of infected computers at each hour over a **24-hour period**. Clearly explain the process you used to determine the spread pattern of Worm X. **0.5 Mark**

(b) **Deployment and Spread of Counter-Worm W**:

By **t = 6.5 hours**, counter-worm W is developed and deployed on one of the computers infected with Worm X. Counter-worm W has the following characteristics:

- W removes Worm X from any host it infects.
- W spreads at a slightly faster rate than Worm X, with each W spreading to two X inftected hosts each hour, provided such hosts are available.

Construct a second table showing:

- The spread of counter-worm W, starting from **t = 6.5**, and its effect on the number of Worm X-infected computers over time.
- Note that at **t = 6.5**, the number of Worm X-infected computers decreases by 1. As a result, the number of X infections will **increase on the hour and decrease on the half-hour** after $t = 6.5$.

0.5 Mark

(c) **Explanation of Patterns**:

- Provide an explanation of how the spread patterns of Worm X and counter-worm W change over time, especially the alternating increase and decrease in Worm X infections due to the spread of Worm W. **0.5 Mark**
- Graph the two cases against each other, clearly indicating on it where $N = 0$. **0.5 Mark**

(d) **A twist in an attack**:
Assume that at time $t = 9$, X evolved to spread to three uninfected computers each hour. What subsequently happens? **0.5 Mark**

6. Design a logging/audition system for public transport in Singapore. Consider:
    - The type of information you would gather.
    - When or where you would gather the information from.
    - The format you would store the information in and where this information would be stored.
    - The types of problems you would look for in analyzing the data.
    - How you would identify some of those problems based on the storage.

    You don't need to be completely exhaustive in this exercise, but you need to justify what you are doing. If you would collect information differently to how it is currently collected that is okay but justify doing so! **1.0 Mark**

Notes on submission

1. Submission is via Moodle.
2. Late submissions will be marked with a 25% deduction for each day, including days over the weekend.
3. Submissions more than three days late will not be marked unless an extension has been granted.
4. If you need an extension, apply through SOLS before the assignment deadline.
5. Plagiarism is treated seriously. Students involved will receive zero.