SIL765: Networks and System Security

Semester II, 2022-2023

Major Exam

May 06, 2023

Short Note on Honor Code

This is an open-book, but closed-internet exam. While participating in this exam, you confirm that you will not give or receive aid in this examination. You will do your share and take an active part in seeing to it that others as well as you uphold the spirit and letter of the IITD Honour Code. You understand that any violation of this code will lead to a severe penalty.

Problem 1 (25 Marks): Chat Application Security

Consider that you plan to develop a chat application where the sender can send a short message to a receiver. The users may expect the security feature like WhatsApp which provides end-to-end encryption with forward secrecy where each message is encrypted by a unique symmetric key. Answer the following questions.

1. Describe the architecture needed to support forward secrecy. You should include the discussion on all asymmetric/symmetric keys and all offline/online operations needed at the sender, the backend server, and the receiver. (10 Marks)
2. Identify all operations which introduce any delay in message delivery in your security mechanism as compared to the plaintext communication. (5 Marks)
3. Explain how improvements in computational and communication capabilities reduce such delays. (5 Marks)
4. Consider that the sender (with a 2023 model phone) is in Delhi (with 5G infrastructure) and the receiver (with a 2015 model phone) is in a remote Assam village (with 3G infrastructure). What operation could potentially be the bottleneck in your security mechanism and how can you mitigate that? (5 Marks)

Problem 2 (15 Marks): Automated Testing

These days, the Indian market has a lot of car variants that support clutch-less, speed-based automatic gear-change features. Let us consider the following scenario.

- To facilitate this application, a developer has written a function that takes three inputs (car speed, engine speed, and time duration after the last gear change) and generates the current gear number (1, 2, 3, 4, or 5) as the output.
- The function is called every second.

You are given the task of checking the function for any bug. Note that you can make any additional assumptions needed to answer the questions.

1. Design a static analysis framework. Also, provide an example of a potential bug that could be discovered by this framework. (5 marks)

2. Design a dynamic analysis framework. Again, provide an example of a potential bug that could be discovered by this framework. (5 Marks)

3. Compare and discuss the limitations of the two frameworks. (5 Marks)

Problem-3 (20 Marks): Intrusion Detection

In the previous problem, consider that the car utilizes electronic units to realize this application. The car speed is calculated at the body control unit and communicated to the engine control unit. Then, the function is executed at the engine control unit which can also compute the engine speed and the time duration after the last gear change. The result is communicated to the gear control unit which changes the gear of the car. These message exchanges occur over the controller area network (CAN) where the messages are neither encrypted nor authenticated and hence can be easily forged by an attacker.

1. Describe two potential ways by which an attacker connected to the CAN can manipulate the gear change. (5 Marks)

2. Describe a conventional ML-based intrusion detection system (IDS) to detect the two attacks. (5 Marks)

3. Discuss how an intelligent attacker can modify the two attacks for bypassing the detection mechanism of the IDS. (5 Marks)

4. Explain how the adversarial (re)training mechanism can help the IDS detect such intelligent attacks. (5 Marks)

Problem 4 (20 Marks): Blockchain

Let us consider that a courier service provider aims to utilize blockchain for creating a public ledger for its operations under the following conditions.

- The courier service consists of five transactions: (1) package registration at the source locality by a registration-agent, (2) collection from the source locality by a collection-agent, (3) aggregation at the storage facility by a manager, (4) distribution to the destination locality by a distribution-agent, and (5) delivery at the destination address by a delivery-agent.

- The courier services are provided in 10 localities and the couriers are booked at a rate of 1 courier per second per locality.

- The manager at the storage facility is solely responsible for creating and adding a block in the blockchain.

- Each hash computation takes an average of 1 ms and the proof of work can be generated after an average of 100 attempts.

Based on the blockchain architecture discussed in the class and the above application, present a detailed timeline of operations at the manager for one second.

Problem 5 (20 Marks): Digital Signature

Let us consider the following conditions in a vehicular network.

- We have two traffic scenarios: light and heavy. During the light traffic scenario, the traffic density is 5 vehicles per km, but during the heavy traffic scenario, the traffic density is 100 vehicles per km.
- Each vehicle broadcasts safety messages containing its location, speed, and other parameters at a periodicity of 100 ms.
- To facilitate privacy-preserving authentication, the messages are signed using the vehicle's private key, and the private-public key pair is changed every 5 minutes.
- On a vehicle, the hash computation takes 1 ms, the encryption/decryption using a public key takes 5 ms, and the encryption/decryption using a private key takes 10 ms. Any other operation takes negligible time, and no two operations can be executed parallelly.

Based on the above assumptions, answer the following questions.

1. List all operations executed by the sender. What will be the computation time spent by a sender in facilitating privacy-preserving authentication during light and heavy traffic scenarios? (5 Marks)
2. List all operations executed by the receiver. What will be the computation time spent by a receiver in facilitating privacy-preserving authentication during light and heavy traffic scenarios? Explain any observation related to a critical safety/security vulnerability with the calculated computation times. (15 Marks)