Blaine Swieder
CSC 6585: Secure Software Development
Dr. Prowell
3 September 2024

CSC 6585: Homework I

Pick a system. It can be a large, medium, or small system, and can be complex, but it should be something you feel comfortable thinking about. Examples are the national defense of a country, a regional hospital, a city traffic system, an automobile, a family, a fare system for a subway, a computerized slot machine at a casino, the card-activated lock at a neighborhood pool, and an MMORPG.

Consider each of the following aspects of your chosen system.

- Hardware/Biology
- Software/Automation
- Users/Participants
- Policy/Procedure
- Environment

Put the following in a document and submit a PDF.

1. Give an informal definition of your chosen system.
2. Define the system boundary by listing the interfaces necessary to your subsequent answers.
3. Pick three of the aspects of your system from the previous slide.
    - State a security property of the system and explain how a weakness in that aspect can be used to violate the given security property.
4. Pick two of the aspects of your system from the previous slide.
    - State a security property of the system and explain how a weakness in each of the two properties can be blended to violate the given security property.
5. Identify a side channel for your chosen system and describe what information might be inferred from observing the side channel.

CSC 6585 Homework I

Blaine Swieder

3 September 2024

1 Homework I

1.1 Question 1

Example 1.1. Give an informal definition of your chosen system.

1.1.1 Answer

Let us consider a city traffic system. A city traffic system is a network of roads, traffic signals, signs, as well as other infrastructure that is designed to manage the flow of vehicles and pedestrians within a given urban area. Its purpose is to ensure safe, efficient and orderly transportation.

1.2 Question 2

Example 1.2. Define the **system boundary** by listing the interfaces necessary to your subsequent answers.

1.2.1 Answer

The **system boundary** of a traffic system are as follows:

- Roads and Highways: Physical infrastructure for vehicle movement.
- Traffic Signals and Signs: Devices to control and guide traffic.
- Vehicles: Cars, buses, trucks, bicycles, etc.
- Pedestrians: People walking or using non-motorized transport.
- Traffic Management Centers: Facilities that monitor and control traffic flow.
- Communication Networks: Systems for data exchange between traffic signals, vehicles, and management centers.

1.3 Question 3

Example 1.3. Pick three of the aspects of your system from the previous slide.

- State a security property of the system and explain how a weakness in that aspect can be used to violate the given security property.

1.3.1 Answer

Let us consider the hardware/biology, software/autonomation, and users/participants of the traffic system.

1. Hardware/Biology: We can consider the integrity of the traffic signals. One potential weakness could be the physical tampering with traffic signals that could lead to malfunction. As a result, there could be an increase in accidents and traffic jams.

2. Software/Automation: The next thing we should consider the confidentiality of traffic data. A potential weakness here is a vulnerability in the traffic management software could result in unauthorized access to real-time traffic data. Hence, an increase in malicious activities.

3. Users/Participants: The next aspect to consider is the safety of pedestrians. The weakness of this aspect of the system could a deficit in proper pedestrian crossing or malfunctioning pedestrian signals that could threaten the safety of the pedestrians.

1.4 Question 4

Example 1.4. Pick two of the aspects of your system from the previous slide.

- State a security property of the system and explain how a weakness in each of the two properties can be blended to violate the given security property.

1.4.1 Answer

Let us consider two aspects of the system. More specifically, let us identify potential weaknesses of the system.

1. Software/Autonomation: A weakness of the availability of traffic management services could be a hypothetical cyber-attack on the traffic management software that could result in the disruption in the entire traffic system and there would be widespread chaos.

2. Policy/Procedure: There could be a weakness compliance with traffic regulations. More specifically, there could be an inadequate enforcement of traffic rules that could result in violations, leading to an increase in the risk of accidents and congestion.

1.5 Question 5

Example 1.5. Identify a side channel for your chosen system and describe what information might be inferred from observing the side channel.

1.5.1 Answer

In this system, we can consider the traffic camera information as the side channel of the traffic system. More specifically, the traffic camera information could infer traffic patterns, peak hours, as well as identifying specific vehicles. This information could be used for surveillance as well as possible malicious reasons.