**Self-driving Vehicle Threat modelling and analysis**

**System Description**

The system taken for this modelling is a self-driving uber service.

**How does it work?**

1. A customer makes a profile on an app.
2. The customer then books an uber inputting the source and destination address.
3. The car picks them up and drops them at their destination.
4. Auto-payment after drop-off.

**Assets:**

1. Mobile app
2. Lidar (Like radar used for the detection of objects in the vicinity)
3. Internet
4. Bluetooth
5. Mechanical parts of the car (Like breaks, sensors)
6. Road traffic
7. Weather conditions
8. Traffic signs and signals

**STRIDE methodology of finding vulnerabilities**

1. Traffic sign modification: Slight modification in traffic signs would result in no recognition by the sensors in the car. For instance, if a malicious actor spray paints a stop sign just a little, a driver would recognise it, but a self-driving car would not be able to.
2. Car machinery damage: An attacker can damage the car machinery by posing as a customer resulting in accidents.
3. Information Leak: The database will contain information about the customer's destination. Consequently, an attacker could track the location by hacking into the GPS.
4. Denial of service: An attacker can fill the network with multiple pick-up requests and deny service to a legitimate customer.
5. Access to AI: An attacker can pose as a customer and gain access to privileged code through the services running in the car. They can insert malware through external input as well.
6. Weather conditions: Heavy rain and fog cause image recognition failure, which can lead to accidents.

**Threat Table**

Threat rated 1-3: 1 is least harmful while 3 is most harmful.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Threat | D | R | E | A | D | Total |
| Traffic sign modification | 3 | 3 | 2 | 2 | 3 | 13 |
| Car machinery damage | 3 | 3 | 3 | 1 | 1 | 11 |
| Information leak | 3 | 2 | 1 | 3 | 3 | 12 |
| Denial of service | 1 | 3 | 3 | 2 | 2 | 11 |
| Access to AI | 3 | 1 | 1 | 3 | 2 | 10 |
| Weather conditions | 3 | 3 | 1 | 2 | 2 | 11 |

**DREAD description**

1. Traffic sign modification: Undetected traffic signs (eg. stop signs) can cause major road accidents affecting pedestrians, passengers and other cars (D=3, A =2). The attack is easy to perform by spray painting over the signs and can be done without much skill or equipment (R=3, E =2). It is difficult to find one sign with damage from thousands of signs on the road(D=3).
2. Car machinery damage: An attacker can easily launch this attack by booking a ride and tampering with the vehicle equipment (R=3, E=3). The damage caused will end up affecting passengers (A=1). This type of attack is easy to identify as a noticeable change occurs in the car behaviour (D=1).
3. Information Leak: The attacker can know about the live location and destination of a passenger which can lead to stalking and other such dangers to the people (D=3). It would require tech expertise and a computer to execute the attack (R=2, E=1). It is difficult to detect this vulnerability as the attacker remains passive (D=3). It will affect all the passengers of Uber (A=3).
4. Denial of service: The damage caused by this vulnerability is the suspension of service which is not much compared to the loss of life(D=1). It is easy to reproduce (R=3, E=3). It affects all the users trying to find a ride at that time(A=2).
5. Access to AI: It is difficult to gain access to the system, but it can be done by entering code physically into the machine or hacking the system (R=1, E=1). Once an attacker gains access, they can change the route and cause potential accidents (D=3). It affects all the entities on the road and is somewhat difficult to detect (A=3, D=2)
6. Weather conditions: Extreme weather conditions can cause failure in image recognition and detection. Consequently, road accidents would be common during such weather(D=3). However, the extremity is not frequent, but the vulnerability is persistent every time it does occur (R=3, E=1). It can affect passengers and pedestrians (A=3). It is easy to identify bad weather conditions through weather reports(D=1).

**Quantitative to Qualitative mapping**

1. Low: Quantitative:10, Access to AI
2. Medium: Quantitative: 11-12, Weather conditions, Denial of service, Information Leak, Car machinery damage
3. High: Quantitative: 13, Traffic sign modification

**STRIDE elements**

1. Spoofing: Traffic sign modification
2. Tampering: Tampering with car machinery
3. Repudiation: All pick-up requests and their accounts are stored in a database, so repudiation vulnerability does not occur.
4. Information disclosure: Information leak
5. Dos: Denial of service by flooding the app with pick-up requests.
6. Elevation of privilege: Gaining access to the AI of the car

References:

<https://www.iriusrisk.com/resources-blog/stride-threat-modeling-methodologies>

<https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN>

<https://eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/>