assignment-1

Assignment 1 - Noe Trevino

Task 1

The main assets for the attack will be the perception system, the control system, the CAN bus (responsible for the communication between the devices using this network), the human machine interface, and the monitor system.

Task 2

Entry points can be:

Perception system

Prediction, Planning

CAN Bus

HMI (Human to Machine Interface)

Task 3

Perception system

- Attacks can include: manipulation the visual inputs, spoofing the signals (gps spoofing) and injecting false data

Prediction, Planning

- Since this takes input from the perception system, these two modules will be directory affected by the attacks on it. The spoofing and injecting of data can result in bad predictions and planning. This could easily result in crashes by the automated car.

CAN Bus

- Since this stands for Controller Area Network, I assume injecting false messages can result in malicious behavior from the vehicle.

HMI

- If left vulnerable, the human to machine interface can result in the attack using this to manipulate the car. For example, the attacker can use this to set the setting to use the wrong camera, potentially a camera being fed a video that is not from the actual perception system at all, and false logging of data.

Task 4

Perception System: Spoofing, Tampering, Denial of Service

Attack Tree:

- Camera Spoofing
  - Use a different camera to feed false data to the perception system
  - Shine bright lights into camera, or cover it from time it time, or just completely
- Radar Spoofing
  - Broadcast malicious signals
  - Jam the signals
- DDoS attack
  - Send a huge amount of differing signals to confuse the car software

CAN Bus: Spoofing, Tampering, Information disclosure, Deinal of Service

Attack Tree:

- Spoofing
  - Tell the other cars we are in a different spot via sending incorrect signals on the carrier frequency
- DDos
  - Send a ridiculous amount of signals to confuse other cars on the network
- Release of Data
  - Send data without the user know for a period to time to another database, allowing a stalker to know where the user has been going to for some time

now

HMI: Tampering, Elevation, Denial of Service

Attack Tree: Tampering

- Make the setting on the car unreasonable and unsafe. Turning off auto brake etc Elevation
- Hack into the system and allow the use to make changes that they are not suppose to make. For example, connecting to the software and changing variable you are not suppose to. I did this on my Volkswagen to make the auto turn off engine to be off automatically

Prediction and Planning: Spoofing, Tampering, Denial of Service All of these are the same at the perception system attack Tree

Task 5

Reflection:

I learned that the attack tree is a good way to visualize the potential attacks a malicious user can make to the system. Coming up with the attack tree turns the attacks that "would never happen" into a very real threat that needs to be addressed.

I always thought the STRIDE strategy was unneeded and redundant. But, honestly when I started this assignment I started off thinking about the attacks and could not come up with anything. I started thinking "OK, Ill try STRIDE" and it came to me almost immediately. Spoofing, Tampering, and the others made easy to come up with potential attacks. Almost like it lead me to them.

Task 6