1 Introduction: Part 1

1.1 Problem Statement

What problem is your project trying to solve? Use non-technical jargon as much as possible. You may find the Problem Statement Worksheet helpful.

The problem that our project is intended to solve is the lack of security in mobile vehicle networks that run CAN: controller area network, rather than ethernet. CAN is an older implementation of how Electronic Control Units (ECUs) in cars, such as windshield wipers, transmission, brakes, radio, all work. When this type of vehicle network was created, they originally were just happy that they got something to work, and security wasn't even an afterthought. Now, it is Team 14's duty to implement a security device that will prevent the electronic signals being sent from the main control unit in the vehicle from being tampered with by malicious instructions. Some of these malicious things could be but not limited to: causing the car to drive into the ditch, blasting the radio, disengaging the brakes from use, locking the car in a specific gear on the transmission, or even unlocking the car and stealing it.

1.2 Intended Users and Uses

Who will use the product you create? Who benefits from or will be affected by the results of your project? Who cares that it exists? List as many users or user groups as are relevant to your project. For each use or user group describe (1) key characteristics (e.g., a persona), (2) need(s) related to the project? (e.g., a POV/needs statement), and (3) how they might use or benefit from the product you create. Please include any user research documentation, empathy maps, or other artifacts as appendices.

Car Manufacturers:

Characteristics

This is a broad group of users involving anyone who builds and manufactures vehicles for a company.

The **demographic** for car manufacturers are generally going to be older (21+), of any race and origin, both male and female, varying education, various living situations and various families. For example, some manufacturers may have a mechanical engineering degree, some may have an industrial engineering degree, or some may have gone to UTI and went through their mechanic program there. How their families vary could be the fact that some have spouses and kids while others may not, and they could live anywhere for manufacturing, i.e. Asia, Europe, North America.

Their **hobbies** are realistically several different things, but it is safe to assume that people who pursue a car manufacturing career are involved with cars in some way on their own time, so being a Car Enthusiast is one of their hobbies.

The car manufacturers **work motivations** could be a multitude of things: a high volume of sales, creating a reputable car brand for notoriety, and to stray away from any civil lawsuits that could arise from selling vehicles that could be vulnerable to a simple exploit of sending the main control unit artificial instructions.

The **personality** of those that are care manufacturers could vary widely. For example, someone who is the CEO of a company like Ford, Chevy, Dodge etc…. May be very strict when it comes to rolling out new vehicles, where they might be the most passionate about the project, as well as the engineers (which also fall under this category) who design the actual car and features. On the other hand, we will have the line workers / blue collar workers who might not care as much about the product as they (most likely) don't get paid as much as the engineers or CEOs do.

The **values** that those who fall under this category may have are, but not limited to: creating a valuable career to support their lives and their families' lives if applicable. To create a product that will be valued by the people purchasing it without the worry of it being hacked.

Needs

Many car manufacturers today are currently looking for a solution that prevents their vehicles from being hacked. Manufacturers know that an unsafe car means unsafe customers. This in turn results in bad press for the company well as loss of money due to lawsuits and damages to products. If a car manufacturer isn't looking for a solution to this problem they likely will be as soon as an incident involving one of their vehicles happens.

Benefits

These manufacturer will gain an increase of profit knowing that the solution provided will work in a backwards compatible manner. It will also allow them to apply this solution to many other cars that use the CAN FD system since it can be used universally and isn't necessarily locked to one specific branding.

Distribution Companies:

Characteristics

These companies would be able to send out their semi-truck drivers across the country and back for thousands of miles, knowing and confident that their trucks have the latest security on them. If there is one thing that is important in the United States in the transmission of goods, a vast majority of them get transmitted by semi-trucks. These trucks having the latest security would prevent lives being in danger, companies losing a lot of money, and companies not receiving their products etc.

Needs

A distribution company wants to be able to send drivers and products out with the peace of mind that both will arrive safely and on time. Currently without security on their trucks, these companies are at a large risk of their product being damaged or stolen in a hacking related attack. Even a single hacking related attack on a distribution company would result in a major loss of money. Knowing vehicles aren't safe to drive would slow the transmission of goods, so distribution companies want the latest and best security on their trucks.

Throughout the world trucks are the most common way of transporting goods. Keeping this supply chain in good health is vital.

Benefits

With our product distribution companies will have peace of mind knowing their vehicles are not susceptible to CAN network attacks.

Drivers:

Characteristics

These are everyday people that do pretty everything and anything. So any user can use one particular thing more than another. However, all of them use the whole vehicle even if they aren't thinking about it. However, safety is often a concern of most vehicle users. These users often explore every possibly of a vehicle problem and can even be the people who are trying to break into other vehicles. Overall, this problem will effect all of the users in some fashion ranging from utilization to driving.

Needs

As fully electric cars are being rolled out from companies and are expanding rapidly to other companies. These cars need to have the latest security on them as well. Companies like Tesla are a step ahead with this, however this year there have been a few cases of Teslas being hacked.

Kay, Grace. "A 19-Year-Old Security Researcher Describes How He Remotely Hacked into over 25 Teslas." *Business Insider*, Business Insider, https://www.businessinsider.com/teen-security-researcher-describes-how-he-hacked-into-25-teslas-2022-1#:~:text=A%2019-year-old%20said,contacted%20them%20regarding%20the%20issue.

This document shows how a 19-Year-Old was able to hack into 25 Teslas just this year. This is not only a problem for Tesla, but for any company producing these electric cars.

So the security on these cars needs to be improved. Preventing the endangerment of lives for many people driving these cars is absolutely vital to us in this project.

Benefits

An everyday commuter will likely not even know that our product is installed in their vehicle unless specifically told. There is an expectation that their vehicle will be safe from remote hacking.

Car Enthusiasts:

Characteristics

These Enthusiasts like their cars to be excellent in all categories including the body, interior, and engine. The cars that they drive are extremely nice looking whether that would be an old vintage car or a brand new off the line vehicle. The securities of these vehicles are of the up-most important to these people due to the fact that they are made bigger targets. These people more than likely don't want to worry about their car being taken advantage of by some security risk.

Needs

The needs of a enthusiast are relatively the same as a regular driver, except they are expecting a slightly higher amount of security due the amount of time and money they are placing in their vehicles. This will prevent their expensive, custom, and unique cars from being taken control of without proper authentication with the increased cryptography.

Benefits

There are an infinite number of hobbies out there, and a car enthusiast is nothing short of one. Having a vehicle that is all-electric and claimed "unhackable" would be a very nice car to have, show off, or sell.

Original Equipment Manufacturers (OEMs):

Characteristics

Currently, OEMs that produce CANbus networks for heavy-duty vehicles use the J1939 standard, which defines a network which has been touted as open and unsecure. These OEM companies are in the industry of manufacturing a system in which various devices within a vehicle are able to communicate with each other. They are focused on the reliability and robustness of the CANbus network, ensuring their resilience in a harsh environment. Their main characteristic would be developing a lucrative device which is desirable to car manufacturers.

Needs

The needs of OEMs include a standard, or spec to which to base their CANbus products from. Also, with security being of bigger importance in the present day, they need to develop a system which is insusceptible to threats. There are now many examples of the

CANbus networks being compromised. With this in mind this new system needs to be inexpensive and easy to integrate.

Benefits

This is where the idea for a secure bridge comes in. As mentioned in the problem statement, the bridge will secure the data being sent between the CANbus networks. This will fulfill the need of having a more secure network, which will bring about many benefits. The most notable being the robustness of the network. Also, OEMs integrating security into their products will make it more desirable for the vehicle manufacturers to integrate them into their own products. At the end of the chain will be the customers of the vehicles who will benefit by having technology that is less susceptible to intrusions.