Introduction: Part 1

Team Name: sdmay23-15

Team Members: Aayush Chanda, Alexander Freiberg, Baganesra Bhaskaran, Brian Goode, Chau Wei Lim, Michael Roling

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.

- Implementing a key exchange procedure and message securing protocol on the CAN Bus
    - Using cryptography to secure a controller's private and public keys
    - Implementing a procedure to allow communication between 2+ controllers
    - Configuring a way to output data on the CAN Bus; are we in need of a CAN Driver?
    - Then read the keys to ensure the controller is supposed to be on the CAN Bus; if its data can be utilized.
- Who has the problem?
    - Vehicle manufacturers and end-users
- What is the problem?
    - Data being extrapolated from the vehicle without the user's knowledge
    - Data is placed on the vehicle without the user's knowledge; a third-party user controlling the vehicle remotely
- Where is the problem occurring?
    - Problem is occurring on the CAN Bus (how data is transferred between controllers within a vehicle)
- When is the problem occurring?
    - Problems can occur at any time - would potentially be up to the malicious user when the attack would occur, or when they would pull data.
- Why is it important?
    - If the vehicle can be controlled by an outside source without the user's knowledge; the user's safety could be jeopardized (along with the hundreds-of-thousands dollars worth of equipment)
- How will it be solved?
    - Encrypting keys for controllers on the CAN Bus; creating a network of controllers who understand who is on the bus, and have the ability to know they are authenticated.

We are trying to solve the problem of insecure CAN bus systems in vehicular systems.

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 user 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.

1. Vehicle manufacturers
    a. Key characteristics
        i. Securing data transmission between ECUs
            - Ensures software cannot be controlled by an outside source
        ii. Ensuring replacement parts do not tamper with the vehicle's intended functionality; achieved by utilizing VIN numbers
    b. Need:
        i. To offer safety to the vehicle user
        ii. Not to be controlled by a third-party user
        iii. Secures software to ensure it is not stolen/replicable (keys, for example).
    c. How they will benefit:
        i. Offers credibility to their product
        ii. Outside sources cannot control the business' vehicles
        iii. Obtained data would be connected to performance; this information is desired to stay internal
2. Maintenance technicians
    a. Key characteristics:
        i. Replacing controllers and verifying they belong on the CAN Bus
        ii. Ensure the vehicular system is safe and secure to be driven or operated by the driver
    b. Needs:
        i. To be able to replace components.
        ii. To be able to detect the right place and error or flaw occurred.
    c. Uses/ Benefits:
        i. We will be able to save cost, by replacing the right components
        ii. Will be able to provide a secure fix/repair to the respective components
        iii. Ensure that their vehicular analysis system doesn't get affected by external malware from the tapped CAN bus frames
3. Vehicle User
    a. Key characteristics
        i. Wants trust in their purchased vehicle
        ii. Desires safety; trusting a third party cannot operate the vehicle remotely
        iii. Wants to know it will function as it; that another controller cannot be placed on the CAN Bus and extrapolate data to be used in a fraudulent manner
    b. Needs
        i. To operate the vehicle safely
        ii. To know their data is protected; how much of a crop they are harvesting, how often they are running their vehicles, etc.
    c. Uses/Benefits

i. Will affect customers/end-users; allows verification to know their data is safe
ii. Will know they can operate their vehicle as expected
iii. Will know third-party users cannot operate their vehicle remotely