Team: sdmay23-15

4 Design

4.1 Design Context

4.1.1 Broader Context

Describe the broader context in which your design problem is situated. What communities are you designing for? What communities are affected by your design? What societal needs does your project address?

List relevant considerations related to your project in each of the following areas:

Area	**Description**	**Examples**
Public health, safety, and welfare	- This on-board security key exchange design for vehicular CAN communication impacts the growth and reliability of modern vehicle manufacturing companies - The implementation of on-board key management for vehicles ensure the public safety (anyone who is able to operate a vehicle)	- Increases the job opportunity in the information security sector for vehicle manufacturing - Vehicle manufacturing companies can ensure safety on their products by establishing such robust security key exchange implementation - Increase the reliability of manufacturers among the community - Reduces the risks of threats on public (drivers), hackers would not be able to launch targeted attacks
Global, cultural, and social	Implementation of a secure key exchange system on CAN communication would ensure the reliability and trust that the public has on vehicle manufacturers. This helps the welfare and wealth growth of both community and motor manufacturing companies.	With reliable security in modern vehicles, the trust in companies would increase and the public would feel safe to invest. The project would provide jobs for the blue-collar community in the information security sector of the vehicle manufacturing industry as the demand increases.
Environmental	The implementation of a secure key exchange protocol in CAN communication relies on the software aspect. This would not have any environmental impact rather than helping the manufacturing industry to grow and produce environmentally friendly modern motor vehicles.	This design implementation has no environmental impact.

Economic	Secure motor vehicles would increase reliability, which has an impact on the increase of motor vehicle demand among consumers This ensures the growth of the motor manufacturing industry, which allows expansion in job scope and also opportunities. This would help the economy to boost as more revenue is gained from the companies which produce secure motor vehicles with help of the onboard key management implementation.	The system doesn't require additional development costs as it is just an upgrade done on existing security for key exchange in CAN communication More people would tend to invest as now it is safer to drive a modern vehicle embedded with multiple computer systems. Companies upscale their production to match the demand would tend to pay more taxes based on the revenue they make This contributes to the growth in the country's economy where the money can be channeled to the nation's welfare and wealth.

4.1.2 Prior Work/Solutions

Include relevant background/literature review for the project

Source: https://cancrypt.net/index.php/en/

One piece of technology that has been developed in the past is a software package known as CANcrypt. CANcrypt is a consolidation of largely scalable security features meant to implement security into CAN protocols including CANopen, J1939, and many other CAN protocols.

Like all pieces of software, there are many advantages and disadvantages to this method, or in this particular context strengths and limitations.

Strengths:

- Supports the grouping of multiple devices and supports authenticated communication between them based on a secure heartbeat
- Minimal in comparison to traditional cryptography methods
- Can also be scaled towards the application's security requirements
- Protocol Independent
    - Can be used by a wide variety of higher-layer CAN protocols.
- Manager only required for generation and authentication of keys, not every regular operation

Weaknesses:

- If an intruder has unlimited physical access to the entire network including device PCBs, then security options available are very limited. Having potential access to all debug ports of the microcontrollers of a system provides many other attack vectors besides CAN
- Once an intruder has direct bus access to a CAN/CANopen system, he has read access to ALL communication on the network. If he has write access, then "denial of service" style attacks

(swamping the bus with messages so that nothing else gets through) are easy and cannot be prevented

- Still vulnerable to remote access through a device that is a gateway to other networks
    - For example, a remote diagnostic device

4.1.3 Technical Complexity

Provide evidence that your project is of sufficient technical complexity. Use the following metric or argue for one of your own. Justify your statements (e.g., list the components/subsystems and describe the applicable scientific, mathematical, or engineering principles)

1. The design consists of multiple components/subsystems that each utilize distinct scientific, mathematical, or engineering principles –AND–
2. The problem scope contains multiple challenging requirements that match or exceed current solutions or industry standards.

4.2 Design Exploration

4.2.1 Design Decisions

List key design decisions (at least three) that you have made or will need to make in relation to your proposed solution. These can include, but are not limited to, materials, subsystems, physical components, sensors/chips/devices, physical layout, features, etc. Describe why these decisions are important to project success.

3 Key Design Decisions:

- Create a new node on CAN network to run the key encryption before sending to the Vehicle ECU
    - The packet will go through many nodes that existed on the CAN network before executing it at the Vehicle ECU. We will design a new node to encrypt the CAN packet using a salt as a key to ensure that the CAN packet that is going to be executed at the ECU is the intended packet. With this, we can eliminate the possibility of an attacker injecting a malicious packet/messages into the CAN network and try to compromise the ECU.
- Salt as a key for the encryption
    - In practice, Salt as a cryptographic concept is random data that is appended to the end of a plaintext string before encryption. By doing this, even if two strings may be equal (the same), after hashing and salting both strings will encrypt to different values. The reason this is important to our design is because usually in CAN protocols the same signals are sent to the same ECUs for each control. By salting the keys these signals create we can mask the values of two different instances of the same control since the created ciphertexts would be different, even if, in plaintext, the signals are equal.
- Cyclic Redundancy Check (CRC) in CAN packet to verify the integrity of data
    - Instead of sending checksum in the CRC field on the packet, we add an encrypted key in the field and send it through the CAN network and it can be decrypted at the destination (Vehicle ECU) to verify the integrity of data. This is a safe way to send our encrypted key together with the CAN packet in the CAN network.

4.2.2 Ideation

For at least one design decision, describe how you ideated or identified potential options (e.g., lotus blossom technique). Describe at least five options that you considered.

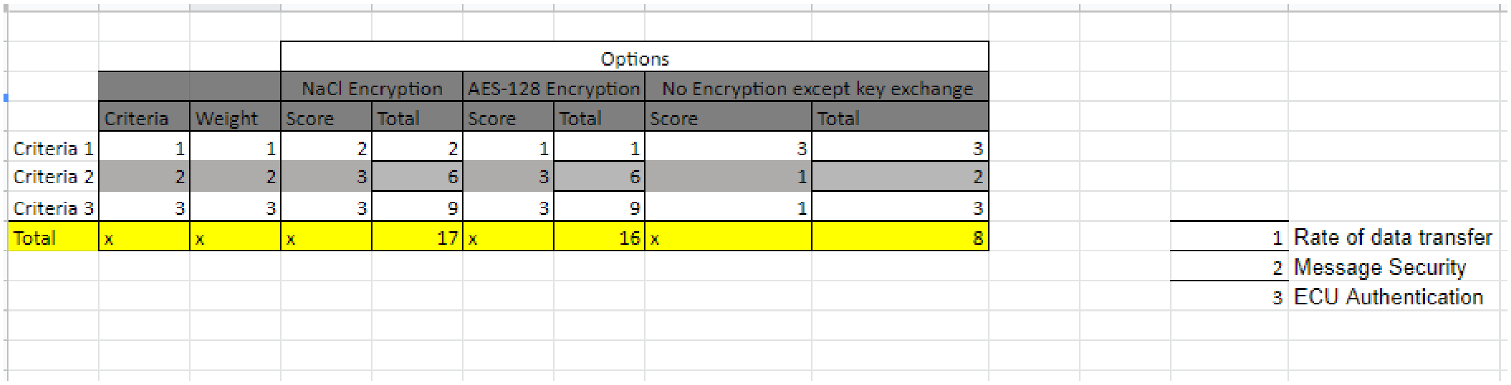
Cyclic Redundancy Check (CRC) was one of the primary design decisions our group focused on. The CRC portion of a CAN packet can be used to detect accidental errors in data communication between controllers on the bus. Taking CRC a step further, encrypting messages within the data packet was the initial proposal. Ideation for the concept was then facilitated by the Lotus Blossom technique. Each of these brainstormed concepts compounded which allowed our group to form other viable options. It should be noted, too, options which may not be directly feasible still contribute to a Lotus Blossom's development. These exercises are shown below.

Uses an existing bit field; keeps data transfer constant.	Rate at which data is transferred will stay the same.	CAN communication (encrypted) will be private.
Will build confidence in the data and ECU.	**CRC**	Encrypt key prior to passing into the data field.
Salt, therefore, could be used for reception to decrypt.	Use Salt as a tool to encrypt the key prior to transfer.	Replacing checksum error code with an encrypted key.

4.2.3 Decision-Making and Trade-Off

Demonstrate the process you used to identify the pros and cons or trade-offs between each of your ideated options. You may wish you include a weighted decision matrix or other relevant tool. Describe the option you chose and why you chose it.

For our encryption protocol that we will be using for this project, we chose NaCl(salt) encryption. We chose this opinion for a few reasons. First of all, NaCl uses an encryption algorithm which implements vastly more message security than just utilizing a key-exchange protocol for ECU authentication. This ensures that each time an ECU sends a message, it will inherently be authenticated. Secondly, NaCl is a form of encryption which means that traffic on the network cannot be intercepted. Thus, this protocol implements a form of message security which the client has expressed to us is important. Lastly, NaCl is a faster encryption algorithm than AES-128 meaning that NaCl will nearly maintain the rate of data transfer already achieved on the CAN bus. Ultimately, this criteria caused us to decide on using NaCl encryption for our security protocol on the CAN bus. Our weighted decision matrix can be viewed below:



			Options					
			NaCl Encryption		AES-128 Encryption		No Encryption except key exchange	
	Criteria	Weight	Score	Total	Score	Total	Score	Total
Criteria 1	1	1	2	2	1	1	3	3
Criteria 2	2	2	3	6	3	6	1	2
Criteria 3	3	3	3	9	3	9	1	3
Total	x	x	x	17	x	16	x	8

1	Rate of data transfer
2	Message Security
3	ECU Authentication