Mobile Vehicle Cybersecurity with On-board Key Management

FINAL DESIGN REPORT

sdmay23_15

Client: John Potter and the Iowa State DigiAg Team

Advisor: Joseph Zambreno

Team Email

Doc Version: v1.0

Main Webpage

Executive Summary

Development Standards & Practices Used

List all standard circuit, hardware, software practices used in this project. List all the Engineering standards that apply to this project that were considered.

Summary of Requirements

- Vehicle Manufacturers
  - Secure CAN network; no replicability (e.g., keys).
- Maintenance Technicians
  - Replacing Controllers
    - Ensuring their acceptance.
  - Detecting the OBD Message
- Vehicle Users
  - Operate the vehicle safely
  - Rapid responses (5 ms)

Applicable Courses from Iowa State University Curriculum

List all Iowa State University courses whose contents were applicable to your project.

- COM S 252: Linux Operating System Essentials
- CPR E 331: Applications of Cryptographic Concepts to Cybersecurity
- CPR E 288: Embedded Systems I - Introduction
- E E 330: Integrated Electronics
- E E 324: Signals & Systems II

New Skills/Knowledge acquired that was not taught in courses

List all new skills/knowledge that your team acquired which was not part of your Iowa State curriculum in order to complete this project.

- As this vulnerability is one that is still being actively worked on in the industry, we realized that if we didn't learn a little bit more about how to apply our knowledge to what we can find out about CAN communication we weren't going to be able to get anywhere. Each group member took several hours to read research articles, thesis papers, lab journals, etc. to learn as much about CAN bus and the vulnerabilities that the lack of security measures cause as we possibly can.
- Along with the technical knowledge that we picked up along the way, we also inevitably worked on many soft skills as well. The ability to be comfortable enough with the people you are working with to the point where you are not afraid to state your thoughts or ideas even if you're wrong is a practice that we have very much fallen into. We aren't afraid to voice our thoughts and give constructive feedback to each other when necessary since we all know that by giving each other this kind of criticism we can not only get a better grade in the class and the project, but also come up with a much more thought out algorithm that we can be proud of developing, while still learning plenty along the way.

Table of Contents

List of figures/tables/symbols/definitions (This should be the similar to the project plan)

1. Team 15 General Information

1.1. Team Members

Alex Freiberg

Aayush Chanda

Baganesra Bhaskaran

Brian Goode

Chau Wei Lim

Michael Roling

1.2. Required Skill Sets for Your Project

Needed to refresh skills and knowledge in basic cryptography, since the main bulk of this project heavily involves applying those concepts with our prior experience in scripting and general security topics to come up with the desired solution. After all, this entire project will require us to apply cryptographic security to develop a script/algorithm that would securely exchange a public/private key pair completely encrypted, so if anyone were to sniff into the packets of communication they'd be greeted with incomprehensible ciphertext.

Received firsthand experience into why using search engines correctly for research purposes is such an underrated skill in engineering. Due to the complexity of this project, along with our admittedly limited experience in this specific concept, the first thing we needed to start doing to tackle this project was to read and learn as much as we can about CAN bus so we could better develop a theory on how to solve the vulnerability this technology contains.

1.3. Skill Sets covered by the Team

Most of the group (Aayush Chanda, Brian Goode, Chau Wei Lim, Baga Bhaskaran) consists of cybersecurity engineering students, so we are fairly well-versed in security concepts, especially the fundamentals of cryptography. More importantly, we are even more experienced in needing to learn multiple different concepts and/or techniques and comprehending them to a level in which we can then apply them to a scenario which we otherwise might've been slightly more unprepared for.

One of our bigger initial concerns for the majority of our group was how we were going to learn all the inner workings of the CAN bus technology, and how/why all the hardware connects together in the ways that it does. As cybersecurity students, we haven't really had a chance to dive deeper into applied electronics, but luckily we have

our token Electrical Engineering student to help us out with that. Using a simple high-level explanation and helping us find sources that would help us understand the technology even further, Michael has already helped the rest of us software-leaning folks learn a lot more about the hardware aspect of the CAN bus even further. We've learned to break out of our own two shoes and now we're a lot more comfortable attacking this problem from multiple different perspectives if need be. Although it wasn't exactly our specialty, the hardware-related concepts were a lot less daunting when we learned that Michael Roling was an electrical engineering student, therefore being much better educated on electrical topics than the rest of us. We know he can be our go-to "specialist" if a hardware related question arises in the future.

Alex Freiberg has quite a bit of professional and academic experience when it comes to cybersecurity and technology in general. However, this field appears to be quite new to all of us, so we're all going to have to be very careful with how we. Alex is quite proficient and has also received planty of exposure to project management, especially of the software variety. Although it may not be the most prevalent skill experienced, it would most definitely help keep us organized. This will especially help towards the end of the project, where the rush and heat of the upcoming deadlines can often lead to students making plenty of rookie mistakes that could've easily been avoided with a little more care or practice. Due to his experience, however, we do trust that he can guide us towards staying organized through the development stages of this project.

1.4. Project Management Style Adopted by the team

Agile will be the primary means to our group's software development. Possessing a high-level of what is needed to be accomplished will allow several sprints to be defined. Breaking these sprints into user-stories will allow individual team members to take responsibility for specific tasks. Delegating these prompts will ensure efficiency and enable members to better understand the full scope of the project. The waterfall approach, although sequential and straightforward, is not flexible for our anticipated modifications. Using Agile will permit our client to be closely involved with the process - a characteristic not supported by the waterfall approach.

1.5. Initial Project Management Roles

Alex Freiberg

- Chief Client Liaison

Aayush Chanda

- Senior Advisor Liaison
- In charge of communicating any necessary information, questions, concerns, etc. to Dr Zambreno, and then relaying the feedback to my group to use in future meetings/implementations.

- In case of meetings with Dr. Zambreno, must inquire about potential availabilities from his side and then comparing them to ours to determine best meeting times.

Michael Roling

- Principal Documentor
- Creates a library of files to faciliate understanding for the project's material.
- Compiling a series of research documents on key management will encourage innovative ways to confirm handshakes between controllers on CAN.

Baganesra Bhaskaran

- Executive GitLab Administrator
- In charge of git repositories and version control.
- Prepare and update the repositaries and drives to keep the documents and code files up-to-date
- Compile and organize team documents time-to-time

Brian Goode

- Lead Team Organizer

Chau Wei Lim

- Head Strategist
- In charge of discussing, developing, and implementing strategies to satisfy client's needs.
- Gather team ideas and make sure they meet the project's requirements.
- Find out a common time for each meeting with the advisor and the client.

2. Introduction

2.1. 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 main purpose of this project is to implement 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.

Problem Statement:

Over the years, the increase of cyber attacks on the communication protocol used in most standard automobiles/vehicles, also known as CAN bus, has been increasing at a steep rate due to the lack of a secure method to encrypt the public/private key exchange between the control units in many vehicles that use this protocol, causing the extrapolation of data being sent to and from each component in a vehicle using CAN bus becoming concerningly too simple. On top of that, security engineers have also found that such an attack could also lead to remote code exeuction, so a malicious actor with access to this communication could also send data to the vehicle, which then enables them to control the vehicle remotely whenever they like once they gain access to the communication itself. With the risk that this vulnerability carries and how directly it compromises the safety of drivers and other vehicle end-users, security engineers and professionals all around the world are now racing towards developing an algorithm in charge of encrypting the keys for each control unit in the vehicle on the CAN Bus. This would include creating a network of controllers that can detect and communicate with the other units that are on the bus and then implementing a method to determine when they are authenticated.

2.2. Intended Users and Usages

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.

Vehicle Manufacturers

- Key Characteristics:
  - Securing data transmission between ECUs
  - Ensures software cannot be controlled by an outside source
  - Ensuring replacement parts do not tamper with the vehicle's intended functionality; achieved by utilizing VIN numbers
- Needs:
  - To offer safety to the vehicle user
  - Not to be controlled by a third-party user

    - Secures software to ensure it is not stolen/replicable (keys, for example).

- Uses/Benefits:
    - Offers credibility to their product
    - Outside sources cannot control the business' vehicles
    - Obtained data would be connected to performance; this information is desired to stay internal

Maintenance technicians

- Key characteristics:
    - Replacing controllers and verifying they belong on the CAN Bus
    - Ensure the vehicular system is safe and secure to be driven or operated by the driver

- Needs:
    - To be able to replace components.
    - To be able to detect the right place and error or flaw occurred.

- Uses/Benefits:
    - We will be able to save cost, by replacing the right components
    - Will be able to provide a secure fix/repair to the respective components
    - Ensure that their vehicular analysis system doesn't get affected by external malware from the tapped CAN bus frames

Vehicle User

- Key characteristics
    - Wants trust in their purchased vehicle
    - Desires safety; trusting a third party cannot operate the vehicle remotely
    - 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
- Needs:
    - To operate the vehicle safely and securely
    - To know their data is protected; how much of a crop they are harvesting, how often they are running their vehicles, etc.
- Uses/Benefits:
    - Will affect customers/end-users; allows verification to know their data is safe ii. Will know they can operate their vehicle as expected
    - Will know third-party users cannot operate their vehicle remotely

2.3. Requirements & Constraints

List all requirements for your project. Separate your requirements by type, which may include functional requirements (specification), resource requirements, physical requirements, aesthetic requirements, user experiential requirements, economic/market requirements, environmental requirements, UI requirements, and any others relevant to your project. When a requirement is also a quantitative constraint, either separate it into a list of constraints, or annotate at the end of requirement as "(constraint)." Ensure your requirements are realistic, specific, reflective or in support of user needs, and comprehensive.

- Functional Requirements:
    - The product should have a secure On-Board Key Management system for vehicular CAN communication
    - Implement secure protocols for message exchange defined in the SAE J1939-19C standard.
    - Determine the integrity of data flowing through the vehicle network (verify whether it is intentionally or unintentionally modified)
    - Constraints:
        - Limited computational power in the ECU
- Physical Requirements:
    - CAN adapters/cables to connect each component
    - Constraints:
        - Strong adapters/cables that don't break easily
- Resource Requirements:
    - Virtual Simulation Environment to simulate traffic on a CAN bus using J1939
    - Constraints:
        - Some physical conditions or properties of CAN bus can't be simulated
- User Experiential Requirements:

        - Must be fast enough to work on a real piece of large machinery and the user doesn't have to wait for key management to take place upon startup
        - Constraints:
            - This must be true on both new and old CAN buses in J1939
    - Economic/Market Requirements:
        - All the funding for resources and materials required for the project will be provided by the client.

2.4. Engineering Standards

What Engineering standards are likely to apply to your project? Some standards might be built into your requirements (Use 802.11 ac wifi standard) and many others might fall out of design. For each standard listed, also provide a brief justification.

- Standard: **SAE J1939-19C**
    - Justification: SAE J1939-19C is the communication standard developed by the Society of Automotive Engineers to standardize communication on the CAN Bus used to communicate between ECUs or Control Units in an automobile or on a piece of heavy machinery.

- Standard: **CAN Bus**
    - Justification: CAN Bus or Controller Area Network Bus is a widely used standard in automobiles and heavy machinery used to transfer information between control units or ECUs throughout the piece of equipment.

- Standard: **X.509 Certificates**
    - Justification: We will likely be using X.509 Certificates for authentication of each ECU on the CAN bus to ensure that there are no unauthorized nodes on the bus.

3. Project Plan

3.1. Project Management/Tracking Procedures

Agile will be the primary means to our group's software development. Possessing a high-level of what is needed to be accomplished will allow several sprints to be defined. Breaking these sprints into user-stories will allow individual team members to take responsibility for specific tasks. Delegating these prompts will ensure efficiency and enable members to better understand the full scope of the project. The waterfall approach, although sequential and straightforward, is not flexible for our anticipated modifications. Using Agile will permit our client to be closely involved with the process - a characteristic not supported by the waterfall approach.

What will your group use to track progress throughout the course of this and the next semester. This could include Git, Github, Trello, Slack or any other tools helpful in project management.

- GitHub - for scripts/codes
- Google Drive - for research papers and professional documentation
- Discord - for communication
- Asana - track agile progress

3.2. Task Decomposition

In order to solve the problem at hand, it helps to decompose it into multiple tasks and subtasks and to understand interdependence among tasks. This step might be useful even if you adopt agile methodology. If you are agile, you can also provide a linear progression of completed requirements aligned with your sprints for the entire project.

- Researching concepts and standards for CAN communication
- Setting up Virtual Machine environments in virtualBox to run CAN simulation.
- Determine what key management standard to use for the project.
- Implement and test the standard and determine if it'll work.
- Liaising and meeting with Advisor and Clients.
- Setting up a simulation environment for testing and implementation of concepts on CAN communication.

3.3. Project Proposed Milestones, Metrics, and Evaluation Criteria

What are some key milestones in your proposed project? It may be helpful to develop these milestones for each task and subtask from 2.2. How do you measure progress on a given task? These metrics, preferably quantifiable, should be developed for each task. The milestones should be stated in terms of these metrics: Machine learning algorithm XYZ will classify with 80% accuracy; the pattern recognition logic on FPGA will recognize a pattern every 1 ms (at 1K patterns/sec throughput). ML accuracy target might go up to 90% from 80%.

In an agile development process, these milestones can be refined with successive iterations/sprints (perhaps a subset of your requirements applicable to those sprint).

- Milestones
    - Design J1939 key management protocol
    - Design message security protocol
    - Design ECU Authentication protocol
    - Implement virtual CAN Bus simulation environment
        - Set up Ubuntu Virtual Machine
        - Implement simulated control unit
        - Implement CAN Sniffer
        - Implement simulated instrument cluster
    - Implement key exchange, authentication, and message security protocols on virtual CAN environment
    - Test J1939 key management protocol
    - Test message security protocol
    - Test ECU Authentication protocol
    - Migrate to physical CAN environment
    - Test protocols on physical CAN environment
- Metrics
    - The Gantt Chart and the Asana, agile progress tracking platform are used to measure and keep in track the progress of each tasks. This makes sure that the team is consistent with their work force.

- Evaluation Criteria
    - The whole team reviews each tasks in the weekly meeting, to verify and ensure that we meet our requirements.

3.4. Project Timeline/Schedule

Link to the Gantt chart:

Gantt Chart

Summary of the Gantt chart:

For this semester, there are five major tasks to be completed. We completed the research on the concepts and standards for CAN communication for the first two weeks. We configured a virtual machine using VirtualBox to run CAN simulations in the virtual environment. Currently, we are installing the configured VM on each of our computers. After that, we will take about three weeks to determine the key management standard that should be used for our project. Then, we will start the implementation of the standard and run through some testing till the end of the semester. The task of liaising and meeting with the advisor and client will last throughout the semester. For the next semester, we will fully focus on the implementation and testing of Simulink.

3.5. Risks And Risk Management/Mitigation

Consider for each task what risks exist (certain performance target may not be met; certain tool may not work as expected) and assign an educated guess of probability for that risk. For any risk factor with a probability exceeding 0.5, develop a risk mitigation plan. Can you eliminate that task and add another task or set of tasks that might cost more? Can you buy something off-the-shelf from the market to achieve that functionality? Can you try an alternative tool, technology, algorithm, or board?

Agile project can associate risks and risk mitigation with each sprint.

Having an Agile project development structure (like the one we are implementing through Asana) can actually help deal with risks and risk mitigation with each sprint, as the principles of the methodology itself were created in part to help in mitigating risk through the usage of cross-functional teams, continuous improvement/feedback, and good engineering practices in general. For example, instead of overwhelming an

entire team by attempting to correct all risks at the end of development, the Agile structure allows us to incrementally reduce risk with each release or version of our product, which in turn mitigates risk in a more gradual sense, allowing for more focus on the risk contained in smaller, individual sections to decrease our own human error.

3.6. Personnel Effort Requirements

Include a detailed estimate in the form of a table accompanied by a textual reference and explanation. This estimate shall be done on a task-by-task basis and should be the projected effort in total number of person-hours required to perform the task.

Tasks	Members Involved	Hours Needed (Week)
Reseraching concepts and standards for CAN communication	Aayush Chanda Baganesra Bhaskaran Chau Wei Lim Brian Goode Michael Roling	2.0
Setting up CAN VM on everyone's computer	Alexander Freiberg	5.0 (only once)
Key Management on CAN	Alexander Freiberg Aayush Chanda Baganesra Bhaskaran Chau Wei Lim Brian Goode Michael Roling	3
Testing with inputs	Alexander Freiberg Aayush Chanda Baganesra Bhaskaran Chau Wei Lim Brian Goode Michael Roling	3.0
Liasing and meeting with Advisor and Clients	Alexander Freiberg Aayush Chanda	2.0

Setting up simulation environment for testing and implementation of concepts on CAN communication	Alexander Freiberg Aayush Chanda Baganesra Bhaskaran Chau Wei Lim Brian Goode Michael Roling	4.0
Version control and professional documentation activities	Baganesra Bhaskaran Michael Roling	1.0

3.7. Other Resource Requirements

Identify the other resources aside from financial (such as parts and materials) required to complete the project.

- We might need support from the client on knowledge and some level understanding for some of the concepts and implementation (currently the client is providing some presentation on new concepts and ideas)
- Research papers and research inputs from various online sources
- Online tutorials (Youtube, Geeks for Geeks, TutorialsPoint, Code Academy, W3 Schools) to learn how to convert our conceptual understandings into code
- Reach out to our advisor (Dr Zambreno) to fill in the lapses (that we will definitely experience) in our conceptual understanding
- Virtualbox VM with our CAN Sim imported into it so we can test
- Physical Apparatus to be used during prototype testing.

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.	• 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

	• 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.	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)

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

Prior to this project, our team had a significant lack of experience in applied cryptography. We had members with basic understanding of

cryptographic concepts, but the project contained a huge learning curve with numerous subjects to research extensively.

Discussed with advisor on where to start, and were told to read research papers, most of which are written by and for graduate students and/or industry experts

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

4.3. Proposed Design

4.3.1. Overview

Provide a high-level description of your current design. This description should be understandable to non-engineers (i.e., the general public). Describe key components or sub-systems and how they contribute to the overall design. You may wish to include a basic block diagram, infographic, or other visual to help communicate the overall design.

The design that we are implementing is inspired from a research paper that we came across during our research phase for the project. There is no authenticated security message exchange implementation for now in the CAN communication network where all the ECUs (computers) in a vehicular systems transmit data packets (communicate) within each other. We figured out that the CAN frame has a 15-bit CRC (Cyclic Redundancy Check) field, which provides error detection support only. The CRC field was used to send checksum code. However, some proposed security solution allows us to apply cryptography in ensuring the integrity of the message being passed, which makes the error detection unnecessary. Our team design makes use of this CRC field to place the hashed key, and also Message Authentication Code in this 15-bit part of the CAN frame. Since it is placed within the CAN frame, this ensures there is no additional load of traffic which requires more bandwidth in the CAN network. The CAN frame then reaches out to all the ECUs connected to the network. The receiving ECU can use the hash to decrypt the key and verify the MAC code to check for the authenticity of key. This will be treated as a symmetric key exchange as only one hashed ley is being passed through the CAN frame.

Figure 2.2: Standard CAN frame format.

The diagram above shows the CAN frame format and how we would be able to fit the hashed key and MAC within the frame to be passed across the CAN network. The design is still under review and multiple testing and implementation ideas are being worked to ensure the designs fit the project and ensures the secure key exchange in CAN network.

4.3.2. Detailed Design and Visual(s)

Provide a detailed, technical description of your design, aided by visualizations. This description should be understandable to peer engineers. In other words, it should be clearly written and

sufficiently detail such that another senior design team can look through it and implement it.

The description should include a high-level overview written for peer engineers. This should list all sub-systems or components, their role in the whole system, and how they will be integrated or interconnected. A visual should accompany this description. Typically, a detailed block diagram will suffice, but other visual forms can be acceptable.

The description should also include more specific descriptions of sub-systems and components (e.g., their internal operations). Once again, a good rule of thumb is: could another engineer with similar expertise build the component/sub-system based on your description? Use visualizations to support your descriptions. Different visual types may be relevant to different types of projects, components, or subsystems. You may include, but are not limited to: block diagrams, circuit diagrams, sketches/pictures of physical components and their operation, wireframes, etc.

Our final design is still under development and revision, therefore we do not have much of a lower level design analysis developed yet. However, as mentioned above, our implementation will be very similar to the aforementioned research paper explaining a Lightweight Authenticated Encryption algorithm to be implemented to secure the transfer of messages via the CAN protocol.

The specific algorithm to be used is known as a lightweight AEAD (Authenticated Encryption with Additional Data) cipher. This is a cipher that can check integrity and validate the data communicated within the messages, more specifically the CAN payload, to ensure confidentiality and integrity are maintained.

The first step to implementing such a cipher would be to choose a type of block or stream cipher, and from research we were able to determine that the ChaCha20-Poly1305 has great credibility in low powered ECUs.

We also have to think about the added delay that the security algorithm would cause for the transmission of messages over a period of time. To minimize this, we can implement an algorithm

responsible for forward keystream glock generation so that the required key stream would be ready to be encrypted during the transfer of the previous message.

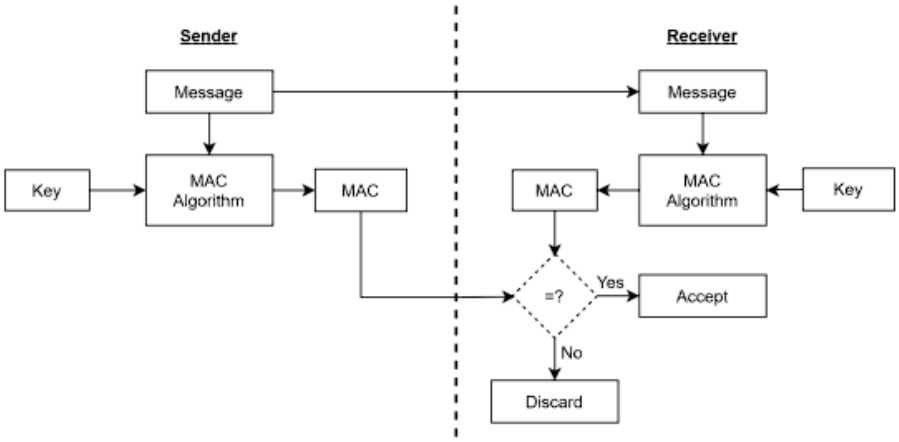


Figure 2.4: Message authentication process.

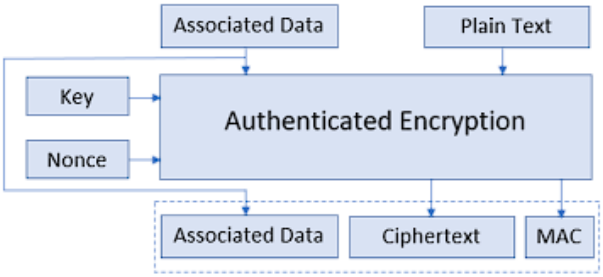


Figure 2.5: Design of an AEAD cipher.

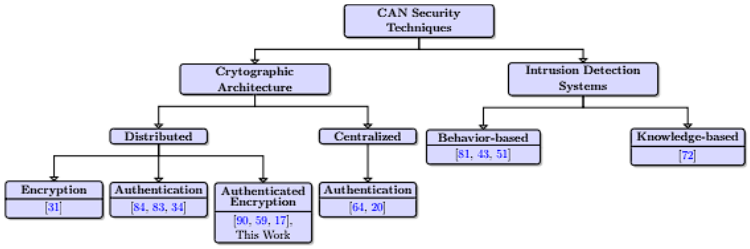


Figure 3.1: Classification of CAN security solutions.

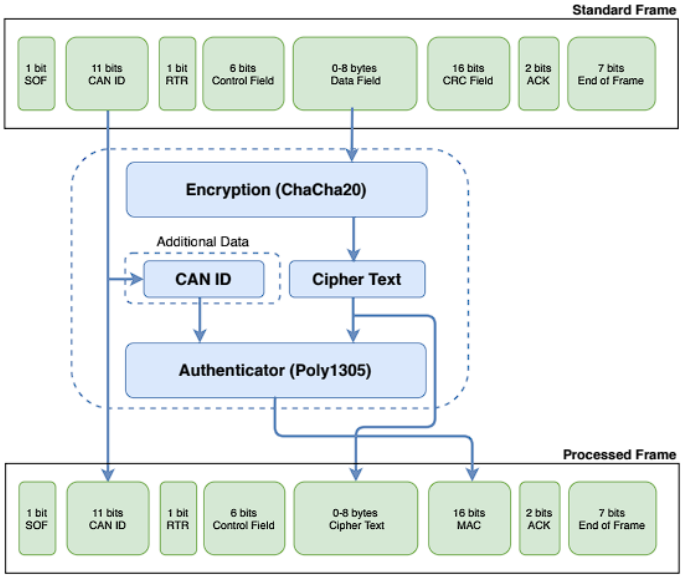


Figure 4.1: Design of the authenticated encryption.

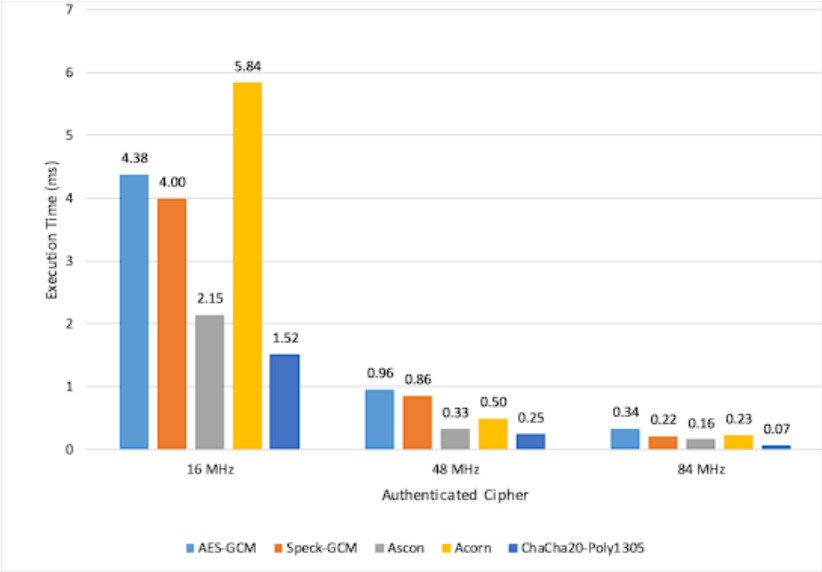
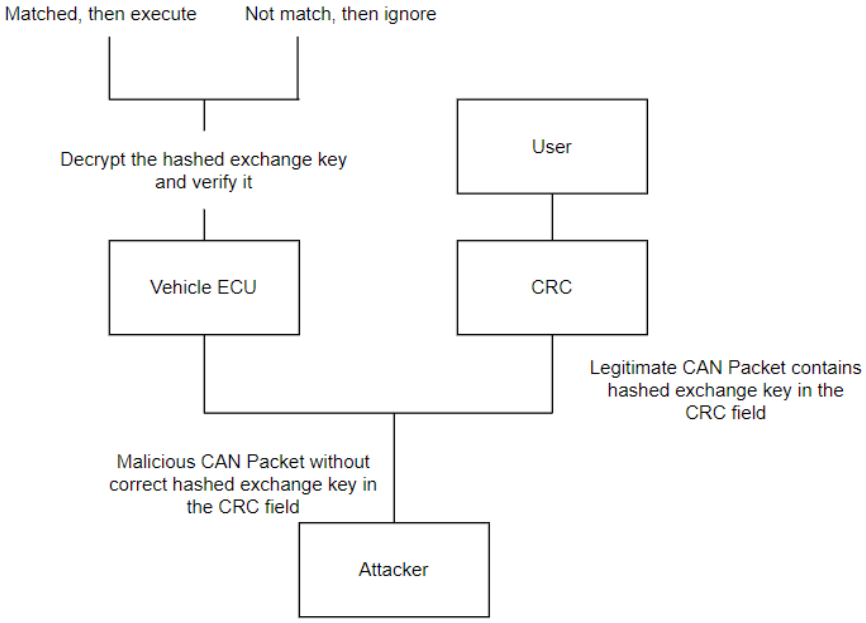


Figure 4.2: Execution times of authenticated ciphers.

4.3.3. Functionality

Describe how your design is intended to operate in its user and/or real-world context. What would a user do? How would the device/system/etc. respond? This description can be supplemented by a visual, such as a timeline, storyboard, or sketch.

Our design is intended to ensure the ECU communication in the CAN Bus network of a vehicle will not be interrupted or compromised by unintended traffic/messages. The user will not need to do anything since our design is already integrated into the ECU on the vehicle. The user might need to replace the original ECU with our CRC integrated ECU to secure their vehicle CAN Bus network. Having our design integrated in the ECU of a vehicle, the vehicle would only respond to those CAN packets that are sent from the user but not any other malicious packets. In that way, we could make sure that an incident such as the driver not being able to brake while driving at a high speed would not happen again.



4.3.4. Areas of Concern and Development

How well does/will the current design satisfy requirements and meet user needs?

Based on your current design, what are your primary concerns for delivering a product/system that addresses requirements and meets user and client needs?

What are your immediate plans for developing the solution to address those concerns? What questions do you have for clients, TAs, and faculty advisers?

By utilizing NaCl encryption and Cyclical Redundancy Checks to authenticate ECUs on the CAN bus and ensure message security, our current design will undoubtedly satisfy the design requirements and meet the user's needs. Since the NaCl encryption protocol is very lightweight, it should not add a substantial amount of latency in communication on the bus. Additionally, since CAN frames are so small, Cyclical Redundancy Checks will ensure that the ECUs can authenticate each other by replacing checksums with encrypted public keys.

Based on your current design, what are your primary concerns for delivering a product/system that addresses requirements and meets user and client needs?

Our primary concern in delivering our key management and message security systems is increase in communication latency. Since vehicles require near-instantaneous communications, any increase in runtime could be detrimental. Encryption is inherently slow, so even a lightweight protocol like NaCl could cause the system to be too slow to function properly. Additionally, safety on any vehicle system is a paramount concern. If our CRC or encryption protocol cause any errors in communication could cause a catastrophic failure.

What are your immediate plans for developing the solution to address those concerns? What questions do you have for clients, TAs, and faculty advisers?

In the immediate term, we plan to finish the initial implementation of our design to analyze how runtime and communication accuracy are affected by our solution. If our design causes negative effects to either of these aspects of the system, we will need to re-evaluate our design to remove the encryption protocol and implement some sort of implicit encryption protocol that does not affect communication latency. As of right now, we don't have any pressing questions for the client, TAs, or faculty. As we approach a testable implementation, we will surely need to evaluate what guidance we need from all parties involved.

4.4. Technology Considerations

Describe the distinct technologies you are using in your design. Highlight the strengths, weakness, and trade-offs made in technology available. Discuss possible solutions and design alternatives.

Throughout the process of determining our product plan, we had a few main requirements to consider while looking at different technologies, those being integrity, and speed. When trying to secure the communications between ECUs on a vehicle, it's important that these messages are unchanged and that they arrive fast enough for the vehicle to act on any potentially dangerous events.

Maintaining integrity ensures that information is changed by authorized subjects and in a consistent fashion. We want to be able to show that no outside threat has changed the information between the time it has left one ECU and arrived at another. Additionally, we want to ensure that our security implementation is consistent and always carried out in the same manner. This ensures that the ECU reading the incoming information knows how to decode the message and that it'll always be done the same way to the decoding process isn't thrown off. The amount of time taken to carry out a certain security measure (hash, encryption, etc.) is extremely important as vehicle chips require extremely quick communication as increased time can be deadly for the vehicle operator, other drivers, etc.

CRC: In the standard CAN frame, the CRC field provides only error detection and allows for a way to transport a key within the standard frame. We will be adding a hashed key and also the message authentication code (MAC) to the CRC field in the CAN frame. The MAC provides Interity of the message/ sender for the receiver. Another consideration we considered was potentially using a second frame to send the MAC because of limited message space within the CAN frame. This would take an extended amount of time for the receiving ECU to receive both frames and decode the added hash message to determine the authenticity and integrity of the message and sender. We determined that this would add too much time and potentially take too much time to decrypt and read vital messages.

4.5. Design Analysis

Discuss what you have done so far, i.e., what have you built, implemented, or tested? Did your proposed design from 4.3 work? Why or why not? Based on what has worked or not worked (e.g., what you have or haven't been able to build, what functioned as expected or not), what plans do you have for future design and implementation work? For example, are there implications for the overall feasibility of your design or have you just experienced build issues?

Simulating CAN Bus traffic with Ubuntu was our group's initial step. Initializing the software allowed the vehicle's dashboard to be displayed, controllers to simulate the vehicle's basic functions, and a device to monitor the CAN Bus traffic. Wireshark was the software used to capture the CAN data packets, therefore, enabling our group to visualize the actual data being sent through the vehicle. The focal point of this data was the CRC bits

being passed as these bits are to be encrypted. Each of these systems functioned as needed and offered great support to our development. The following steps are to replace the CRC field with the hashed key using NaCl. Creating a means to pass it into binary without retransmitting the packets, due to an error or large packet size, are the consequent initiatives.

5. Testing

Testing is an **extremely** important component of most projects, whether it involves a circuit, a process, power system, or software.

The testing plan should connect the requirements and the design to the adopted test strategy and instruments. In this overarching introduction, given an overview of the testing strategy and your team's overall testing philosophy. Emphasize any unique challenges to testing for your system/design.

In the sections below, describe specific methods for testing. You may include additional types of testing, if applicable to your design. If a particular type of testing is not applicable to your project, you must justify why you are not including it.

When writing your testing planning consider a few guidelines:

- Is our testing plan unique to our project? (It should be)
- Are you testing related to all requirements? For requirements you're not testing (e.g., cost related requirements) can you justify their exclusion?
- Is your testing plan comprehensive?
- When should you be testing? (In most cases, it's early and often, not at the end of the project)

5.1. Unit Testing

What units are being tested? How? Tools?

The units being tested in our design are the NaCl encryption protocol and the CRC authentication mechanism.

To test the NaCl encryption protocol, we will assume that the authentication protocol has been passed by each ECU by populating each with the correct public key and a valid private key. We will then utilize our simulated CAN bus to ensure that the ECUs are able to communicate with one another effectively by monitoring input and output using the cansniffer function on our Linux VM.

To test the CRC authentication mechanism, we will begin our simulation on our simulated CAN bus in a state where three ECUs are connected to the system. One ECU will have a valid private key and the correct public key.

The other ECU will have an invalid private key and the correct public key. The third ECU will also have a valid private key and the correct public key, and it will be used to show the output on a simulated vehicle from the information being relayed by the bus. The ECU with the valid private key will ideally be able to control the virtual vehicle's output. The ECU with the invalid private key, on the other hand, will ideally not be able to control the virtual vehicle's output.

5.2. Interface Testing

What are the interfaces in your design? Discuss how the composition of two or more units (interfaces) are being tested. Tools?

The project is based off a key exchange method development which makes use of algorithms and scripts. The interface that we would ideally deal with would be Simulink, CAN Sniffer and multiple ECUs that has dedicated computer boards running to send and receive packets through the CAN network. We might deal with a physical CAN network (hardware) as we progress into next semester where we get to test the algorithms and design that we came up with. The interface that we have been using for current testing purposes is a Linux VM that simulates the CAN network, a sniffer tool and data from multiple ECUs as they are being controlled with sample data. The interfaces involved help the testing of the design more than putting them to test. We assume there no vigorous testing needs to be done on the interface itself rather than the script and the design we have for CAN frames.

5.3. Integration Testing

What are the critical integration paths in your design? Justification for criticality may come from your requirements. How will they be tested? Tools?

We have decided to use the Big Bang Integration testing approach. This approach requires us to finish developing all components and modules in order to start testing the system. It is convenient for our project since our implementation will be done in a small CAN Bus network system, which requires each node in the CAN network to have a good connection. It also covered all modules that we developed to ensure that they integrate well with the original CAN Bus network.

For testing, we will first use the virtual environment that was given by the client to test the functionalities of our implementation to make sure the

result is what we expected. After integrating our implementation with the original CAN Bus network, we will then use Simulink to test the connectivity between each node in the CAN network with some test cases and analyze the response or behavior of the ECU after receiving different kinds of packets. If everything goes as planned, the final step will be to test our design implementation on the physical hardware model.

5.3.1. Acceptance Testing

How will you demonstrate that the design requirements, both functional and non-functional are being met? How would you involve your client in the acceptance testing?

Acceptance testing will largely come into play closer to the end of the project when we are demonstrating the overall working project to our client. That being said, we want to work throughout the project duration to ensure that we are meeting the requirements put forward by the client and his desires. Our client has an example CAN bus & ECU system set up in sukup that we will use to demonstrate our protocols on hardware. When demonstrating in person, key testing results include:

- Successfully importing the algorithm into the CAN system.
- Successfully sending input (accelerate, brake, turning, etc) to the controller.
- Ensure that messages between ECU units are getting to the correct destination.
- Analysing packets to determine the encryption from NaCl

5.3.2. Security Testing

To security test our project, we will need to test both the message security and ECU authentication aspects of the system. For our security testing mechanism, we plan to connect 2 ECSs to the simulated CAN bus. One of the ECUs will have a valid private key which will allow it to be authenticated via CRC, and it will be able to read messages by decrypting the NaCl encryption protocol. The second ECU will not have a valid private key, so it will be unable to be authenticated via CRC, and it will not be able to decrypt messages due to the NaCl encryption protocol. Thus, the first ECU will be able to monitor and/or control the systems on the CAN bus, but the second ECU will not.

5.4. System Testing

Describe system level testing strategy. What set of unit tests, interface tests, and integration tests suffice for system level testing? This should be closely tied to the requirements. Tools?

The system level testing requires end-to-end testing of all units, interfaces and design that we have developed so far in par with the design we have proposed. To strategic approach on testing the system would be having the physcial CAN bus system setup (hardware) with multiple ECUs and implementing our design (algortihm) for secure key exchange and message passing. This level of system test is only feasible next semester as the client would be able to provide us access to the Simulink (simulation environment) to test our design implementation and then proceed with the physical CAN network. In the testing phase, we should be able to sniff the packets and no key is revealed in the sniffer, and ECUs should be able to function according to the command sent/received between each other. This make the whole system testing (end-to-end testing) successful.

5.4.1. Regression Testing

How are you ensuring that any new additions do not break the old functionality? What implemented critical features do you need to ensure do not break? Is it driven by requirements? Tools?

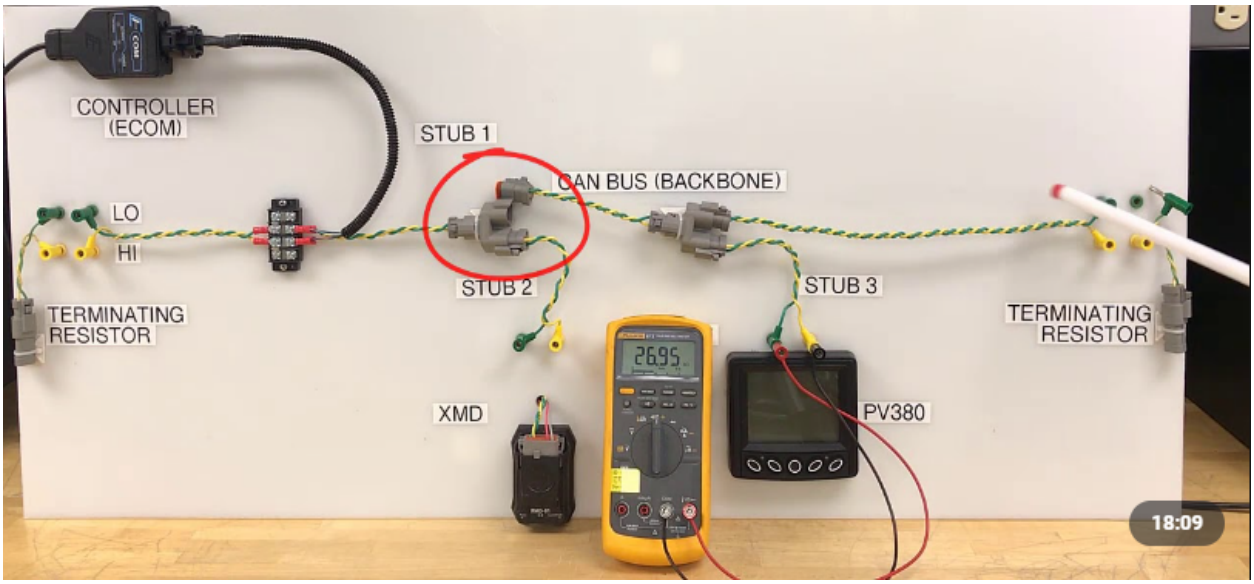
Regression testing will be the primary means to ensure added functionality does not break previous software. These assessments will iterate through dependencies and other conditional statements with respect to existing code. Running regression tests at the end of each software development sprint will guarantee all behaviors are captured. It is worth noting, at a minimum, regression tests will be run after critical features have been added; CAN communication, CRC exchanges between ECUs, and decrypting the messages following the NaCl protocol. GitLab will be used to assist regression tests through its version control capabilities. Other tools - such as the CAN sniffer, Simulink, etc. - will be used to verify the code's functionality. Each of these steps will facilitate our software development and will be used as needed.

5.5. Results

What are the results of your testing? How do they ensure compliance with the requirements? Include figures and tables to explain your testing process better. A summary narrative concluding that your design is as intended is useful.

While we have not tested a final design just yet, the way we are planning to do this is detailed above. If the algorithm is implemented correctly via the design process explained in the previous sections, then what we will be expecting is a fully encrypted stream of communication between each ECU. This entails having every input signal lead to a different ciphertext output, so that any malicious listener wouldn't be able to decipher which outputs came from which inputs.

Our testbed will look similar to what is shown in this image below:



6. Implementation

Describe any (preliminary) implementation plan for the next semester for your proposed design in 3.3. If your project has inseparable activities between design and implementation, you can list them either in the Design section or this section.

7. Professional Responsibility

This discussion is with respect to the paper titled " Contextualizing Professionalism in Capstone Projects Using the IDEALS Professional Responsibility Assessment", *International Journal of Engineering Education* Vol. 28, No. 2, pp. 416–424, 2012

7.1. Areas of Responsibility

Pick one of IEEE, ACM, or SE code of ethics. Add a column to Table 1 from the paper corresponding to the society-specific code of ethics selected above. State how it addresses each of the areas of seven professional responsibilities in the table. Briefly describe each entry added to the table in your own words. How does the IEEE, ACM, or SE code of ethics differ from the NSPE version for each area?

7.2. Project Specific Professional Responsibility Areas

For each of the professional responsibility area in Table 1, discuss whether it applies in your project's professional context. Why yes or why not? How well is your team performing (High, Medium, Low, N/A) in each of the seven areas of professional responsibility, again in the context of your project. Justify.

7.3. Most Applicable Professional Responsibility Area

Area of Responsibility	**Definition**	**NSPE Canon**	**IEEE Code of Ethics (Engineers shall act for each employer or client as faithful agents or trustees)**	**Level of Importance**	**Team's Current Level of Importance**

Work Competence	Perform work of high quality, integrity, timeliness, and professional competence.	Perform services only in areas of their competence; Avoid deceptive acts.	This code of ethics states in line with the NSPE since acting for each member or client is part of performing high-quality work, as it avoids potential conflicts of interest. An avoidance in conflict of ideas and interest would ensure the quality of service or product delivered.	High A high-quality work is required as a team, to provide reliable and effective project outcomes to the client. This ensures that we are responsible for the work that is assigned to us.	Med We are not able to provide a firm design and implementation as the concept is still new to adapt and work on for most of the teammates. For example, the whole team only get to know about what CAN network and CAN communication is after extensive individual research and multiple client presentation.
Financial Responsibility	Deliver products and services of realizable value and at reasonable costs.	Act for each employer or client as faithful agents or trustees.	The ethics also talks about not accepting compensation or any additional finances from more that one party for services. This disrupts the trust and financial responsibility between the	Low In the context of this project, there is not much of a financial constraint or requirement present. This made the importance lower as it is a conceptual approach and more research	Low There is not much financial responsibility as most of the cost (if needed) for the project is born by the client. The project has a major software and cyber

			client and the team. NSPE also states the same, as providing services or products without any breach is encouraged.	on an existing problem, where all materials and tools that we would need funding for are already provided.	contribution which limits the financial need and responsibility for this.
Communication Honesty	Report work truthfully, without deception, and understandable to stakeholders.	Issue public statements only in an objective and truthful manner; Avoid deceptive acts.	The ethic chosen from IEEE has a similar approach to portraying honesty and communication. The ethic emphasizes on engineers not accept or solicit financial or other valuable consideration, in connection with the work for which they are responsible.	High This is important in any professional work, as this establishes trust between us and the client. Good communication is also a major component of a proper effective deliverable in a project.	Med The team has good reporting progress to date as we are updating our client and advisor through weekly status reports. The medium level was chosen due to the lack of in-person meetings and communication with clients or advisors to get opinions or feedback on the team's progress.
Health, Safety, and Well-Being	Minimize risks to safety, health, and well-being of stakeholders.	Hold paramount the safety, health, and welfare of the public.	The ethic doesn't have a say on the health, safety, and well-being.	Med Mental and well-being of both the clients and team is	Med Within the team, each individual is responsible on member's

				important for the good progress of any project.	physical and mental health as in directly impacts the project's progress. In every weekly meeting, we reserve a few minutes to talk about how the week went for everyone and share some interesting topics towards the end.
Property Ownership	Respect property, ideas, and information of clients and others.	Act for each employer or client as faithful agents or trustees.	In par with the NSPE statement, the IEEE states engineers act for each employer or client, where respecting each other opinions and feedback is encouraged.	Med This is important as each idea and opinion of the members and even the clients plays a big role in the development of a project. Respect towards ideas and ownership of the work done by each individual is a major component of the team's health.	Med Major portion of the ideas is developed from the research papers and articles read. With proper reference to it, within the team, we tend to listen and respect to each other's ideas and opinions for the project.
Sustainability	Protect environment		IEEE ethic chosen has no	Low	Low

	and natural resources locally and globally		relatable ideas or say regarding sustainability.	It is important to be concerned about the impact on environment as it is our responsibility to protect and nurture the resources that are abundant to us. With the context of this project, it does not have a direct impact on the environment.	The project does not impose an impact on the environment.
Social Responsibility	Produce products and services that benefit society and communities.	Conduct themselves honorably, responsibly, ethically, and lawfully so as to enhance their honor, reputation, and usefulness of the profession.	Being faithful agents or trustees to the employer or client is the biggest social responsibility in a profession. Both NSPE and IEEE relates and emphasizes equally on this aspect for engineers in their professional career.	High Providing products or services that are reliable and secure to society will help the progress and growth of the nation as a whole. It is a responsibility of an individual in any profession to be able to contribute to the well-being of the community that he/she belongs to.	High The project works on an onboard key management system for vehicular communicati on. With the success of this project, vehicles could be secure from getting hacked. This shows how important the project the team is working on for the community.

- **Question 4:**
    - The team agreed on most of the areas as discussed in the weekly team meeting.
    - There was a slight disagreement in the Communication Honesty and Social Responsibility area where the team emphasized that as a team our communication within the team is effective and there is not much of a need to be highly reliable on advisors and clients. Though the concept introduced for the project is new for the team, the team was convinced that it is the main purpose of the senior design project, to actually learn how to work together learning and share knowledge.
    - I agreed with their facts, but still decided to stick to my perception of the team's current level of importance shown in each area described in Table 1.

- **Question 5:**
    - Health, Safety, and Well-Being.
    - The team has demonstrated a moderate level of importance in this area of responsibility.
    - In this context, the mental health of each team member in a way impacts the progress of the project. Each individual in the team should be fully involved, providing respectful and effective insights which could contribute to the team's productivity.
    - The well-being of each team member and team spirit is important in such group projects where each individual is responsible for their work which results in the idea, process, design, and development of the project.
    - The general practice of us, checking on each other during weekly meetings has a good impact on our team bond and spirit which helped in a way to be more involved and interested to work on the project.
    - We tend to be comfortable in sharing ideas and putting in more effort to make design implementations and testing on the current finding that we have for the project without any lack of interest.

- **Question 6:**
    - Communication Honesty

- I still feel that the team should show some aspect of contribution or responsibility in establishing better communication with the advisor and client.
- In my opinion, there are certain gray areas in our design implementation that we need to address to the client asking for his perception and feedback on it. Getting some advise from the advisor might help improve the current proposal that we have as a team too.
- The team has decided to set up meetings with both advisor and client before we proceed on developing the design of the project going forward.

8. Closing Material

8.1. Discussion

The main requirement of this on-board key management project was to come up with a design that will be able to address the security key exchange issue between each electrical boards in the CAN network which is a peer-to-peer network. Our initial design was able to address this issue by making use of the error detection field (16 bit CRC field) to pass the message authentication code and hashed key. This reduced the traffic in the CAN network at the same time managed the key exchange between different ECUs to send/receive data packets securely. The initial design was not able to be achieved as we would not be able to have access to modify/alter the bit field from the hardware level. With client feedback and ideas, the newest design that we have proposed would be able to address the project requirement as now it takes advantage of the extended bytes of the data field where now an overhead can be attached to each data packets that is being passed in a CAN frame where the salt encrypted public-private key pair and a nonce will be utilizing it. This way we can establish a secure key exchange between the ECUs in the CAN network. We were unable to test the newer design at this point of the project as we just had a major changes made to it. We have implementation and testing plans laid out for the upcoming semester to work on the newer design.

8.2. Conclusion

Throughout the duration of this project thus far, we have learned an immense amount about mobile cybersecurity and the CAN system. While a large portion of our time spent this semester has been focused on learning what CAN is and how it works, we have also been able to design on-board key management, ECU authentication, and message security systems.

With keys embedded in ECU firmware by the manufacturer, our current design utilizes the CRC field to embed a hashed key into packets destined for each of the correct ECUs to effectively exchange keys for NaCl encrypted communication. With the use of a “master” ECU, we will be able to log a list of the approved keys on the network to ensure that no malicious or unauthenticated devices will be allowed to connect to the network. While this design is currently still under review by both our team and our client, we believe that it is on the verge of becoming successful.

This solution satisfies the goals laid out by both our team and our client. Once our design is refactored slightly, especially in the key-exchange protocol, we will have learned an immense amount of knowledge that we were not able to obtain in our coursework here at Iowa State. Additionally and more importantly, we will have implemented the design requirements of the client as a team. In the road ahead, we must make use of our virtual testbed, Simulink, and our physical testbed from the client to test the effectiveness of our implemented design to ensure that the system runtime is acceptable especially in such a fast-moving and high-stakes environment such as a vehicle.

Throughout this semester, there were two main things that prohibited us from achieving a successful design especially in the area of key-management. First off, the CAN protocol is highly complex. In addition, none of our team members had any experience with embedded encryption or CAN. This produced a very steep learning curve for our team in which we had to scale our knowledge as quickly as possible around both topics to a level in which we could then augment CAN's protocol with a higher level of security. Secondly, our communication level was less than ideal. While communication is a two-way street, we accept a majority of the responsibility for infrequent communication with the client. This caused us to develop an original design that was not completely feasible. As a result of late communication of this design to our client, we are currently working diligently to alter the design in a way that will be feasible given the client's feedback regarding the system parameters. To address these two issues going forward, we intend to incorporate weekly or semi-weekly meetings with our client to clarify and ask more questions as we dive deeper into our design adjustments. This way, we will be able to increase our knowledge of the requirements of an embedded encryption system on a CAN network, and we will be able to ensure that there are no more design oversight issues like we've had in this semester.

8.3. References

List technical references and related work / market survey references. Do professional citation style (ex. IEEE).

Giust, Alberto. *A Study of Automotive Security - CAN Bus Intrusion Detection Systems, Attack Surface, and Regulations*, *University of Turku*, July 2022,

https://www.utupub.fi/bitstream/handle/10024/154560/Giust_Alberto_Thesis.pdf?sequence=1&isAllowed=y.

Hridoy, Syed Akib Anwar. *Lightweight Authenticated Encryption for Vehicle Controller Area Network, Queens University; Kingston, Ontario, Canada*, May 2020, https://www.proquest.com/docview/2525649670?pq-origsite=gscholar&fromopenview=true.

Murvay, Pal-Stefen. "Security Shortcomings and Countermeasures for the SAE J1939 Commercial ..." *IEEE Xplore*, Institute of Electrical and Electronics Engineers, 18 Jan. 2018, https://ieeexplore.ieee.org/document/8263125.

8.4. Appendices

Any additional information that would be helpful to the evaluation of your design document.

If you have any large graphs, tables, or similar data that does not directly pertain to the problem but helps support it, include it here. This would also be a good area to include hardware/software manuals used. May include CAD files, circuit schematics, layout etc,. PCB testing issues etc., Software bugs etc.

9. Team Contract

Team Members

1. Aayush Chanda
2. Alexander Freiberg
3. Baganesra Bhaskaran
4. Brian Goode
5. Chau Wei Lim
6. Michael Roling

Team Procedures

1. Day, time, and location (face-to-face or virtual) for regular team meetings:

   The team has decided to meet weekly throughout the semester.

   - Day: Thursday
   - Time: 2.00 - 3.00pm
   - Location: TBD (based on the team needs, virtual or in-person)

2. Preferred method of communication updates, reminders, issues, and scheduling (e.g., e-mail, phone, app, face-to-face):

   - Primary Communication: Discord
   - Official Communication: Email (sdmay23-15@iastate.edu)
   - Scheduling: Google and Outlook Calendar

3. Decision-making policy (e.g., consensus, majority vote):

   - All decisions made should follow the majority vote among the team members, and should be comfortable for each member. Any disagreements, concerns or opinions are welcomed to be voiced out.

4. Procedures for record keeping (i.e., who will keep meeting minutes, how will minutes be shared/archived):

   - All meetings (internal, client, and advisor) will be recorded via meeting minutes (Word Document) which will then be shared via Email among the team, client and advisor.

5. Participation Expectations:
    - Expected individual attendance, punctuality, and participation at all team meetings:

Base Guidelines

- Attendance is required for all meetings and group discussions
- Members are expected to provide early notice on their absence for meetings or discussions (at least 24-hour prior)
- All members are expected to be punctual to the meetings by showing up on agreed time
- All members are expected to be aware of meeting schedules and any updates/changes made to it

Expectations

- All members are expected to complete the assigned task by the deadline
- Members should seek help in tasks or inform the team earlier if any difficulties or challenges faced to meet the deadlines
- Each member is responsible for the whole deliverables of the team
- Expected level of communication with other team members:
    - All members are expected to have a respectful manner of communication
- Expected level of commitment to team decisions and tasks:
    - All members are expected to proactively provide feedback and include themselves in all team decisions and tasks.

Leadership

- Leadership roles for each team member (e.g., team organization, client interaction, individual component design, testing, etc.):

Role	**Responsibility**
Client Liaison	Alexander Freiberg

Advisor Liaison	Aayush Chanda
Documentor	Michael Roling
Gitlab Administrator	Baganesra Bhaskaran
Team Organizer	Brian Goode
Strategist	Chau Wei Lim

Strategies for Working

Strategies for supporting and guiding the work of all team members:

- Gitlab Issues and Tasks assignments for project management
- All team members must be actively involved in team Discord channel
- All project tasks will be documented on both Gitlab and Google Calendar for issue and appointment tracking
- Any issues that arise will be handled internally to the best of our ability before escalating the issue to a higher level of authority

Strategies for recognizing the contributions of all team members:

- Gitlab Board & Issues
- All team members should know each other roles and tasks throughout the project

Collaboration and Inclusion

Describe the skills, expertise, and unique perspectives each team member brings to the team.

Aayush Chanda:

- What I may lack in professional skills/experience, I more than make up for with my positive attitude and drive to keep digging and learning. When something sparks my interest like this project has, I can't seem to stop obsessing over it. I truly believe that sometimes the smallest of details can have the biggest of impacts, so I am more than happy to be the guy digging deep enough to make a difference.

Alexander Freiberg:

- I am a seasoned veteran in the area of project management. My most useful quality beyond any technical knowledge that I bring to the table is my interpersonal communication skill. I take our team's success very seriously, and I will make sure that our team has all of the resources that we need to be successful.

Baganesra Bhaskaran:

- I am a cyber-security engineer with distinctive problem-solving skills and good time management skills.

Brian Goode:

- An organized student with experience working through security alerts, vulnerabilities, and incidents.

Chau Wei Lim:

- I am good at working with people as a team and also solving any conflict that occurs in the team. I have good time management skills and tend to finish my task ahead of the due dates to make sure everything goes smoothly throughout the project.

Michael Roling:

- An electrical engineer with experience bringing controllers onto the CAN bus; primarily programmed in C. Developing embedded software for a fatigue tester has been a recent project as well. Designing and engineering a digital potentiometer and a programmable amplifier at transistor level will be a strong reference project, too.

Procedures for Identifying and Resolving Collaboration or Inclusion Issues

(e.g., how will a team member inform the team that the team environment is obstructing their opportunity or ability to contribute?)

- Communicate and discuss the problem with team members
- Members should not hesitate to talk out their problems and communicate with their team members via Discord or any form.

- Goal-Setting, Planning, and Execution

Team Goals for this Semester

- Developing communication team management skills
- Complete the design for applied cryptography for vehicular on-board key management
- Integrate cryptography standard through J1939 for CAN communication
- Meet class & team deadlines
- Learn real-world problem solving skill by solving the client's problem

Strategies

Strategies for planning and assigning individual and team work

- Meeting weekly to discuss project progress; talk through action items
- Gitlab Issues and Tasks Assignments

Strategies for keeping on task

- Make sure we keep each other accountable for each others' work to ensure that deadlines are being met within reasonable time and effort.

Consequences for Not Adhering to Team Contract

How will you handle infractions of any of the obligations of this team contract?

- Discuss within the team how to solve any issues that come up.
- If necessary, the matter will be brought up to the advisor.

What will your team do if the infractions continue?

- We'll see about that when we get there. At the end of the day, we all know we're on the same team and trying to strive for the same goal in this class. We also understand that because of the expectations we have set for ourselves, whatever incidents or conflicts that may occur down the line must be solved fast, as we need to focus on working together to develop this algorithm and deliver an amazing demonstration of it towards the end of the school year.

****

a) I participated in formulating the standards, roles, and procedures as stated in this contract.

b) I understand that I am obligated to abide by these terms and conditions.

c) I understand that if I do not abide by these terms and conditions, I will suffer the consequences as stated in this contract.

1) Brian Goode	DATE 9/15/22
2) Aayush Chanda	DATE 9/15/22
3) Baganesra Bhaskaran	DATE 9/15/22
4) Alex Freiberg	DATE 9/15/22
5) Chau Wei Lim	DATE 9/15/22
6) Michael Roling	DATE 9/15/22