F25-04: Drive Secure: Teaching Automotive Cybersecurity with RAMN

By: Brooks O’Hanlan, Colton Smith, Jonas von Stein, and William Min

SME: Dr. Tim Talty
Customer: Dr. Zeb Bowden at VTTI

Date: November 19th 2025

VIRGINIA TECH
TRANSPORTATION INSTITUTE

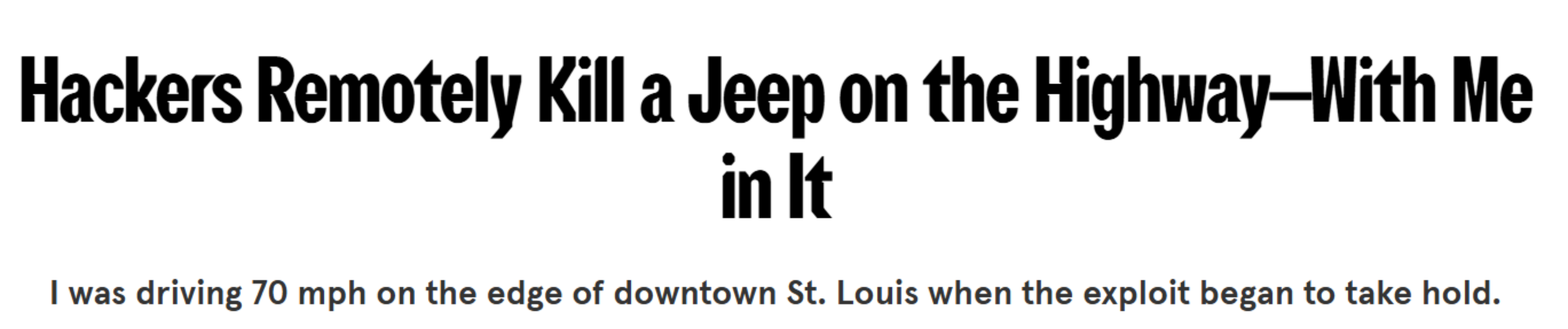
COLLEGE OF ENGINEERING
BRADLEY DEPARTMENT OF
ELECTRICAL AND COMPUTER ENGINEERING
VIRGINIA TECH

Introduction

- As cars become more modern, they face the same cybersecurity risks as computers
- Our project objective was to create **automotive cybersecurity challenges** and documentation for beginners i.e. junior/seniors in college

Why Our Project Matters

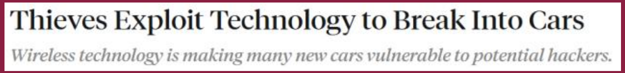
- Over 100 Electronic Control Units (ECUs) in vehicles
- Cars have critical features controlled by ECUs
  - Steering
  - Acceleration
  - Airbags
- This makes cars susceptible to cybersecurity attacks



Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

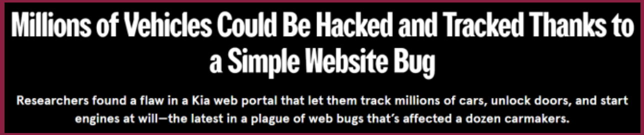
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/



Thieves Exploit Technology to Break Into Cars

Wireless technology is making many new cars vulnerable to potential hackers.

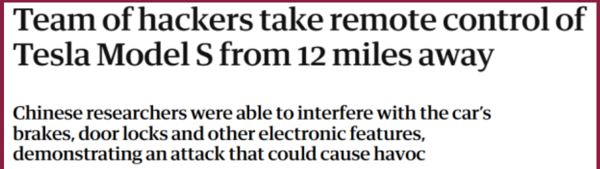
https://abcnews.go.com/world-news-tonight-with-david-muirT/video/thieves-exploit-technology-break-cars-39121081



Millions of Vehicles Could Be Hacked and Tracked Thanks to a Simple Website Bug

Researchers found a flaw in a Kia web portal that let them track millions of cars, unlock doors, and start engines at will—the latest in a plague of web bugs that's affected a dozen carmakers.

https://www.wired.com/story/kia-web-vulnerability-vehicle-hack-track/



Team of hackers take remote control of Tesla Model S from 12 miles away

Chinese researchers were able to interfere with the car's brakes, door locks and other electronic features, demonstrating an attack that could cause havoc

https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes

What is RAMN?

- Resistant Automotive Miniature Network
  - Electronic Control Unit (ECU) testbed
  - Cost effective
  - Open source
  - Portable

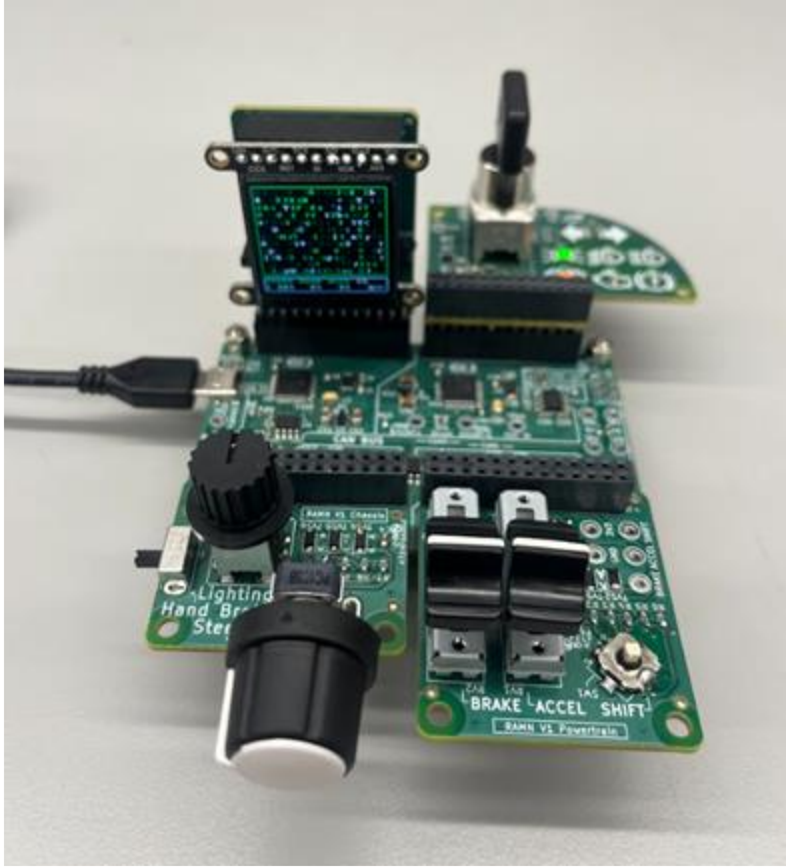


Figure 1. F25-04 RAMN board.

RAMN Expansions

- ECUs communicate over Controller Area Network (CAN)
- LCD Screen
- Chassis
  - Steering, Lights, Handbrake
- Powertrain
  - Brake, Accelerator, Gear shifter
- Body
  - Dashboard, Key ignition

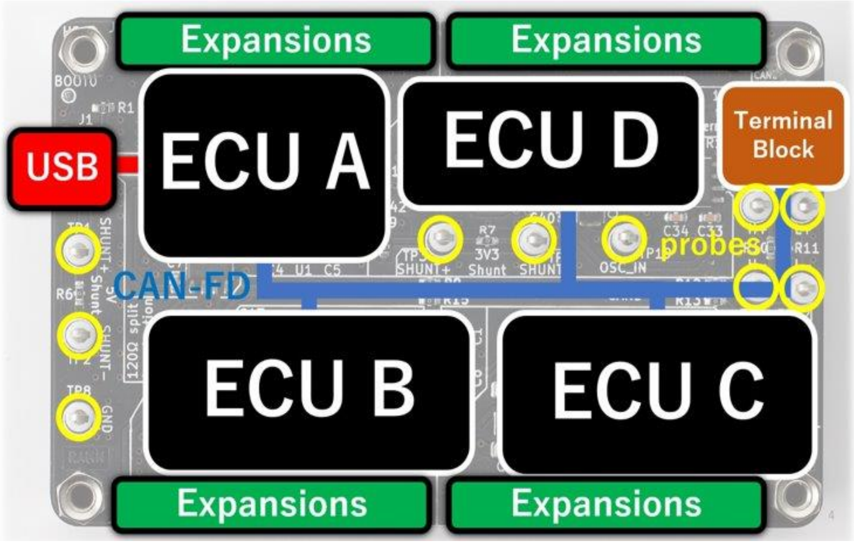


Figure 2. Overview of RAMN layout.

Image: "Documentation of ramn: Resistant automotive miniature network," Documentation of RAMN: Resistant Automotive Miniature Network - RAMN 1.0.0 documentation, https://ramn.readthedocs.io/ (accessed Feb. 24, 2025).

Problem Statement

- Dr. Zeb Bowden at Virginia Tech Transportation Institute wants to utilize the RAMN to help develop cybersecurity practices and facilitate a learning environment for future cybersecurity and automotive engineers.

Introduction & Objectives

- Goals and Objectives
  - Assemble RAMN
  - Create cybersecurity challenges for educational purposes
  - Provide documentation for future replication
- Importance and impact of solving the problem
  - Used in the future by VTTI as an educational tool
  - Documentation helps VTTI replicate and design their own challenges

Implications for Future Use

- Automotive Industry
  - Explore vulnerabilities of ECUs
  - Provide security measures against malicious hackers
  - Ensure safety of automotive users
- Education
  - Teach automotive vulnerabilities and how they are exploited
  - Understand malicious interactions between devices

Our Approach

- Understand RAMN configuration with existing documentation
- Reverse engineer cybersecurity challenges based on previous examples
- Create an educational tool for beginner cybersecurity students

CARLA

- Autonomous driving simulator using Unreal Engine
- Used with RAMN scripts to control a vehicle's
  - Driving
  - Steering
  - Dashboard
  - Gear shifts
  - Headlights
  - Etc.

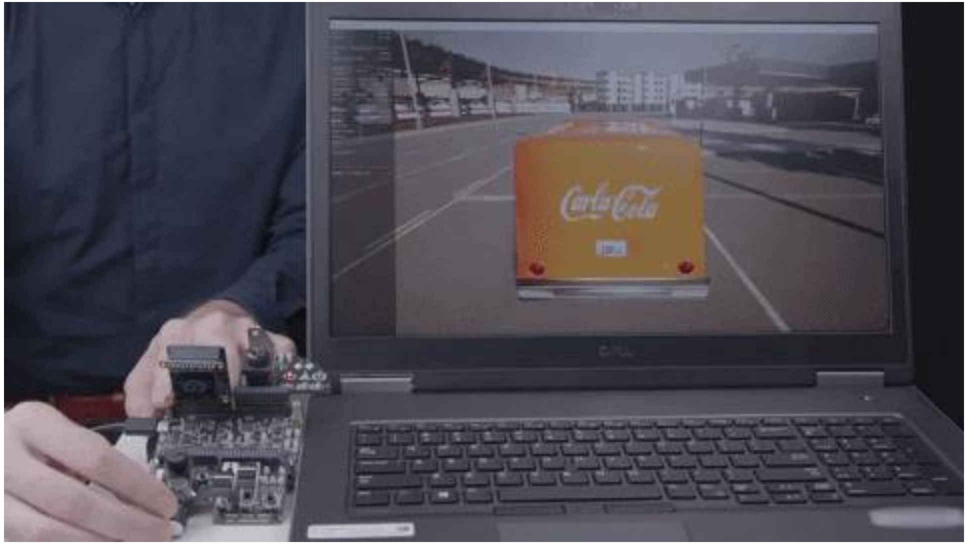


Figure 3. RAMN controlling a vehicle in CARLA

Challenges We Encountered

- We received the RAMN parts unassembled
  - Most of the soldering require surface mount soldering.
- RAMN documentation is not detailed
  - The documentation assumes the user has a good amount of experience with Linux and ECUs.
    - Minimal experience with Linux and ECUs
    - Tasked to make instructions clear enough for a new user to understand our cybersecurity challenges
- CARLA
  - Using can-utils and CARLA with RAMN simultaneously

RAMN Parts, Unassembled

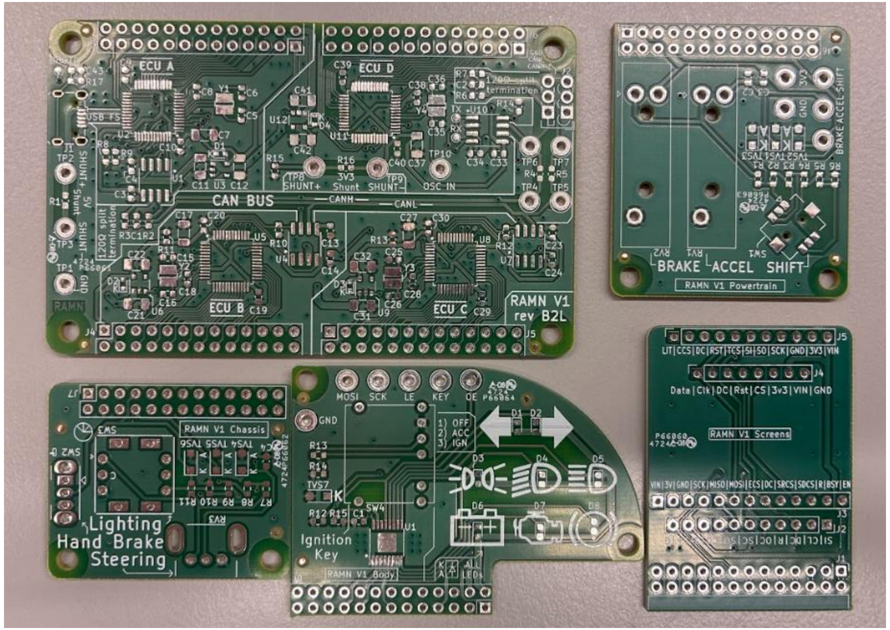


Figure 4. Unassembled RAMN parts

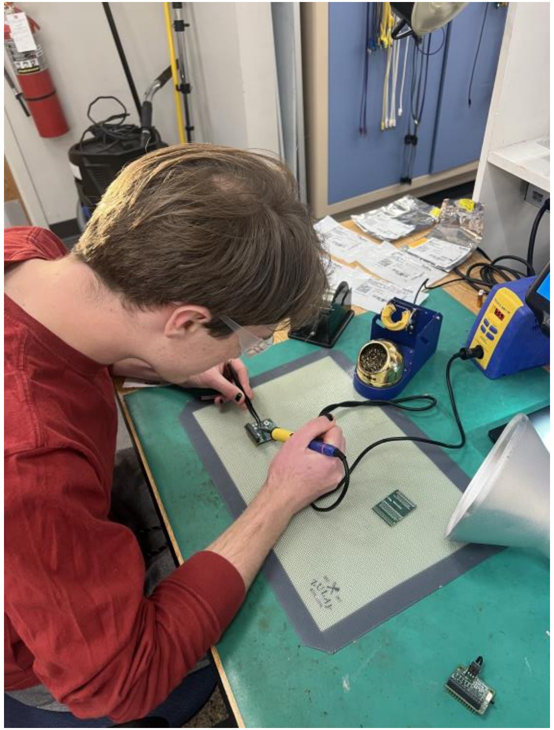


Figure 5. Soldering the parts

Schedule Milestones

- Solder training (February – April)
- Assemble the RAMN system (March – April)
- Have CARLA work with RAMN (March – November)
- Documentation of the RAMN (March – November)
- Test and replace the soldered parts (April – May)
- Assemble backup RAMN (September – October)
- Create cybersecurity challenges (September – November)

Proposed Solution

Documentation

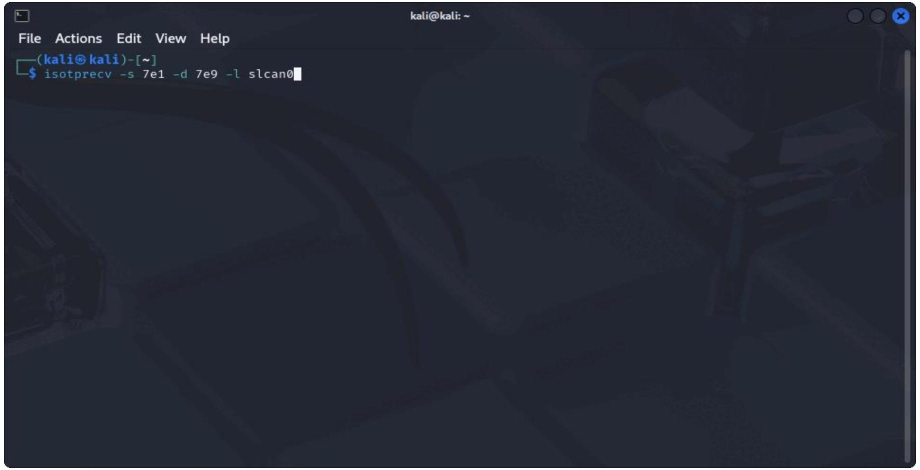
- Beginner-level Cybersecurity challenges
  - Capture the Flag
  - Brute Force Scripting
  - ECU Manipulation
- Documentation
  - Examples:
    - How to install RAMN Firmware
    - How to fix RAMN Firmware when installed incorrectly
    - How to write a Python script and run it on the RAMN
    - Overall guidance on how to set up challenges without the user being left into the unknown

Capture The Flag Challenges

SCAN ME

Documentation

- What is a Capture the Flag Challenge?
- How do they relate to vehicles?
- We use diagnostic services to identify a string
  - "Attackers" can use the data to learn more information about the vehicle

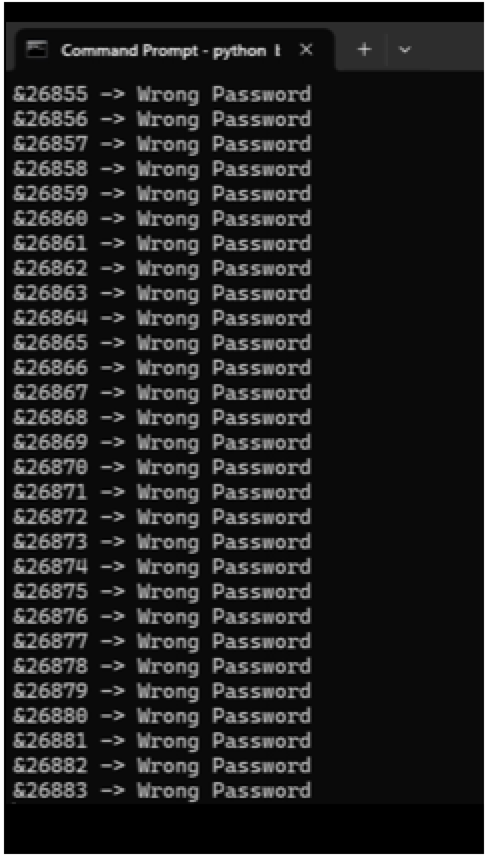


```
┌──(kali㉿kali)-[~]
└─$ isotprecv -s 7e1 -d 7e9 -l slcan0
```

Figure 6. CTF challenge demo

Brute Force Scripting

- Go through every possible password until a flag is found
  - Create a Python script for brute forcing in the RAMN
  - Results from each attempt is shown until correct password is entered



```
&26855 -> Wrong Password
&26856 -> Wrong Password
&26857 -> Wrong Password
&26858 -> Wrong Password
&26859 -> Wrong Password
&26860 -> Wrong Password
&26861 -> Wrong Password
&26862 -> Wrong Password
&26863 -> Wrong Password
&26864 -> Wrong Password
&26865 -> Wrong Password
&26866 -> Wrong Password
&26867 -> Wrong Password
&26868 -> Wrong Password
&26869 -> Wrong Password
&26870 -> Wrong Password
&26871 -> Wrong Password
&26872 -> Wrong Password
&26873 -> Wrong Password
&26874 -> Wrong Password
&26875 -> Wrong Password
&26876 -> Wrong Password
&26877 -> Wrong Password
&26878 -> Wrong Password
&26879 -> Wrong Password
&26880 -> Wrong Password
&26881 -> Wrong Password
&26882 -> Wrong Password
&26883 -> Wrong Password
```

Figure 7. Output from brute force script

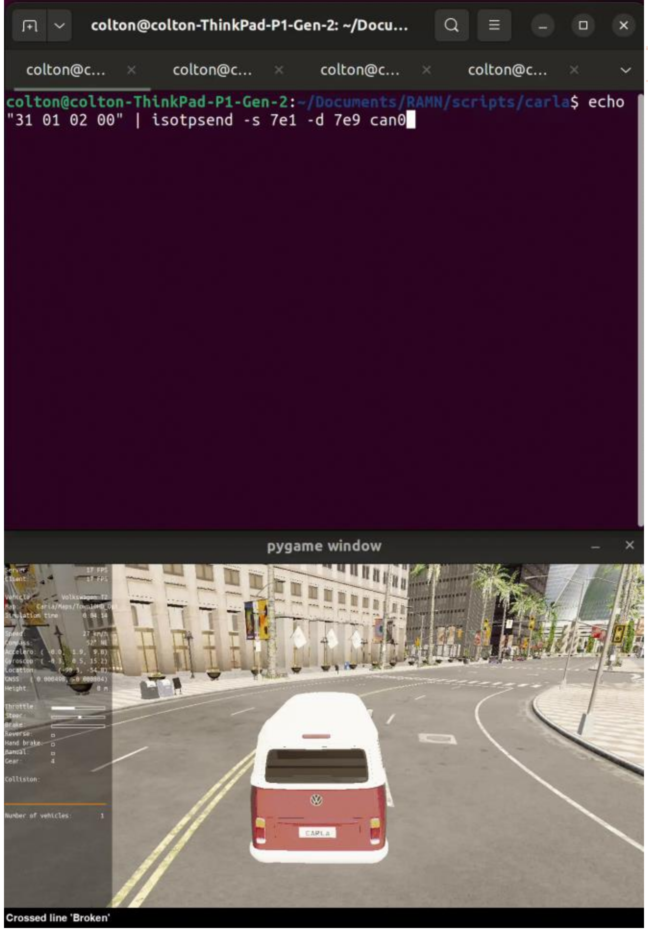
SCAN ME

Documentation

COLLEGE OF ENGINEERING
BRADLEY DEPARTMENT OF
ELECTRICAL AND COMPUTER ENGINEERING
VIRGINIA TECH

ECU Manipulation

- Change input values at data layer
  - Linux
    - Set up attack
    - Disable ECUs
    - Modify ECU values
  - Show output on CARLA / LCD Screen expansion
    - CARLA is an open-source driving simulator that we use to visualize the output

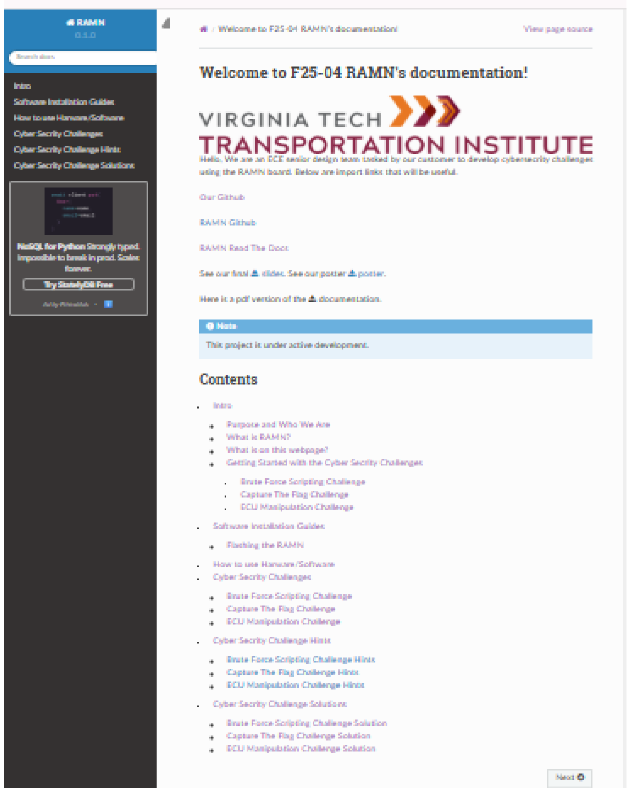


```
colton@colton-ThinkPad-P1-Gen-2:~/Documents/RAMN/scripts/carla$ echo
"31 01 02 00" | isotpsend -s 7e1 -d 7e9 can0
```

Figure 8. Visual representation of ECU manipulation

Documentation

- Streamlined process
- Step-by-step instructions
- Debugging instructions
- Entry-level Oriented



RAMN
0.1.0

Search docs

Intro
Software Installation Guides
How to use Hardware/Software
Cyber Secrity Challenges
Cyber Secrity Challenge Hints
Cyber Secrity Challenge Solutions

/ Welcome to F25-04 RAMN's documentation!　　View page source

Welcome to F25-04 RAMN's documentation!

VIRGINIA TECH TRANSPORTATION INSTITUTE

Hello. We are an ECE senior design team tasked by our customer to develop cybersecurity challenges using the RAMN board. Below are import links that will be useful.

Our Github

RAMN Github

RAMN Read The Docs

See our final slides. See our poster poster.

Here is a pdf version of the documentation.

Note

This project is under active development.

Contents

Figure 9. Read-the-Docs Website

SCAN ME

Documentation

COLLEGE OF ENGINEERING
BRADLEY DEPARTMENT OF
ELECTRICAL AND COMPUTER ENGINEERING
VIRGINIA TECH

Resource Planning

- Resources Used
  - Soldering Equipment in the AMP Lab
  - Outsourced the main RAMN board to be soldered
  - Used the RAMN documentation made by the creators to download the RAMN code and necessary firmware
  - JTAG Debugger
  - Spent $37.30 to buy extra parts

Our Solution

- What makes our solution innovative?
  - Our work is focused on the automotive industry
  - Our work offers beginner-level challenges as an educational tool
  - Our work provides more detailed documentation than other resources

Contributions

- Soldered RAMN boards for future cybersecurity students
- Contributed to documentation made by the creators
  - Created a website to introduce beginners to the RAMN
- Created our own challenges with hints and solutions
- Make existing resources more accessible
  - Lowered the bar to entry

Acknowledgments

- Sponsor: Virginia Tech Transportation Institute
- Customer: Dr. Zeb Bowden
- SME: Dr. Tim Talty
- Mentor: Dr. Joe Adams
- Creator of RAMN: Camille Gay, Toyota
- ECE purchaser: Kim Medley
- Solder trainer: Rusty Stewart

Questions?