

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

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

SME: Dr. Tim Talty

Customer: Dr. Zeb Bowden at VTTI

Date: November 19th 2025



Introduction

- Our project objective was to create **automotive cybersecurity challenges** and documentation for beginners i.e. junior/seniors in college.

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>

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
- How do you increase awareness of automotive cybersecurity risks?

Why it matters cont.

- Talk about the cost and size difference of getting into automotive security?
 - Cars are big, expensive, and proprietary

What is RAMN?

- Resistant Automotive Miniature Network
 - Electronic Control Unit (ECU) testbed
 - An ECU is an embedded system in automotive electronics that controls one or more of the electrical systems or subsystems in a car

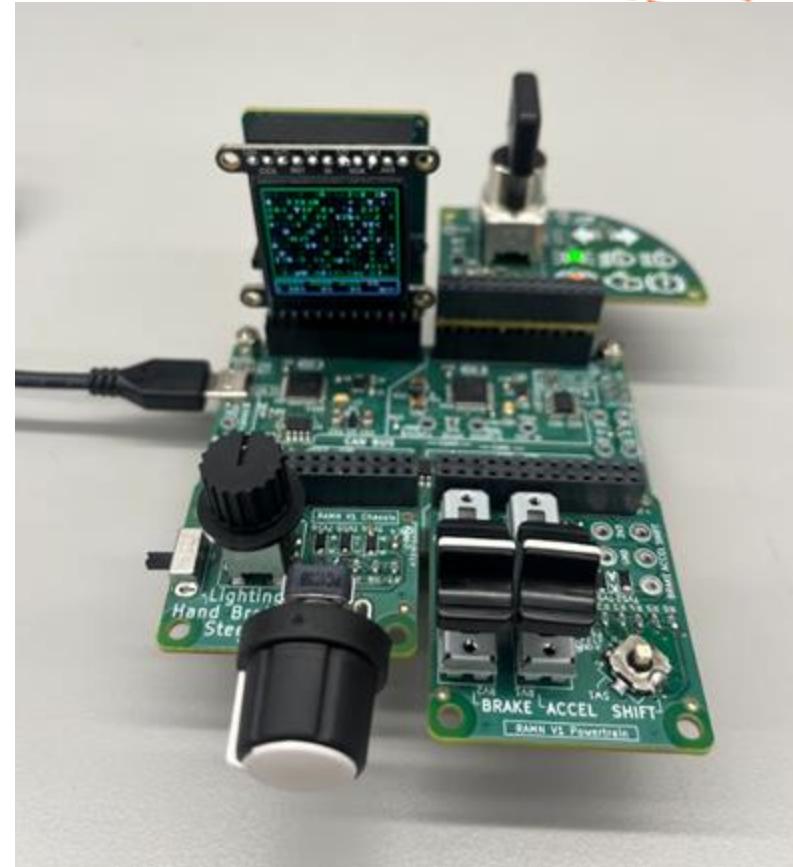


Figure 1. F25-04 RAMN board.

Pic/Explanation of Pods

- ECUs communicate over CAN
- Body pod does this
- Powertrain does this
- Blablabla
- **expansion and/or pod

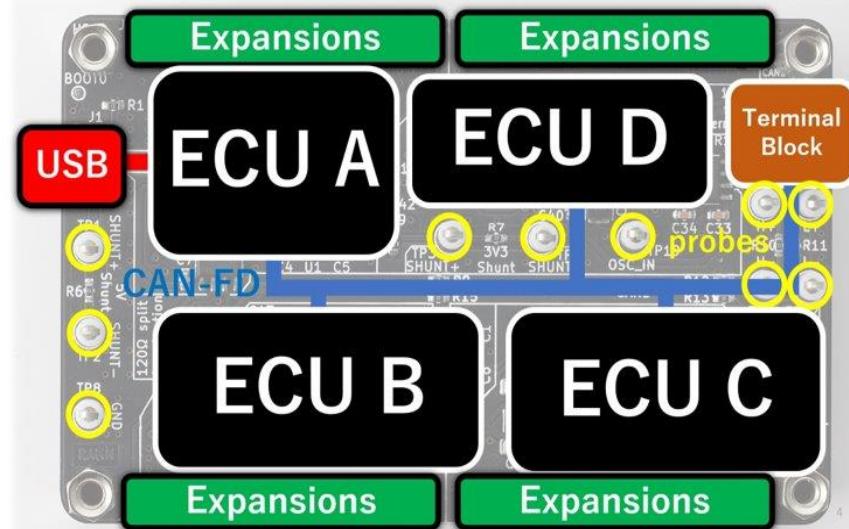


Figure 2. Overview of RAMN layout.

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).

Introduction & Objectives

- Overview
 - RAMN to be used as educational tool for cybersecurity at Virginia Tech Transportation Institute (VTTI)
- Goals and Objectives
 - Assemble RAMN
 - Create cybersecurity challenges for educational purposes
 - Provide documentation for future replication

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.

Problem Statement

- Problem Description
 - 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.
- 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.

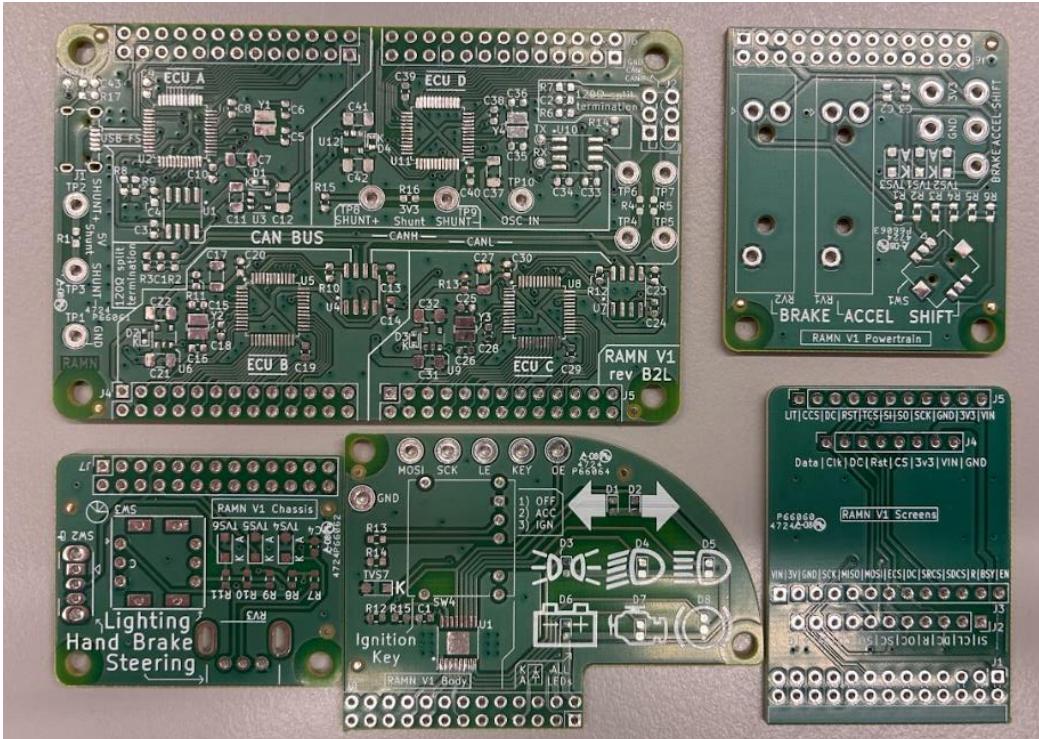
Our Approach

- Use existing RAMN documentation to understand how to use RAMN
- Use existing example code to help develop challenges
- Create documentation to fill gaps in RAMN documentation

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 of a new user to understand our cyber security challenges

RAMN Parts, Unassembled



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

RAMN Documentation, Missing Details

- Insert pic

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)
- Make the poster and presentation (October – November)



Our Solution

- Beginner-level Cybersecurity challenges
 - Capture the Flag
 - Brute Force Scripting
 - ECU Manipulation
- Documentation
 - Examples:
 - How 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 how to set up challenges without the user being left into the unknown



Documentation

Capture The Flag Challenge

- Brooks
 - Brooks
- DIDs can contain sensitive information for different vehicles:



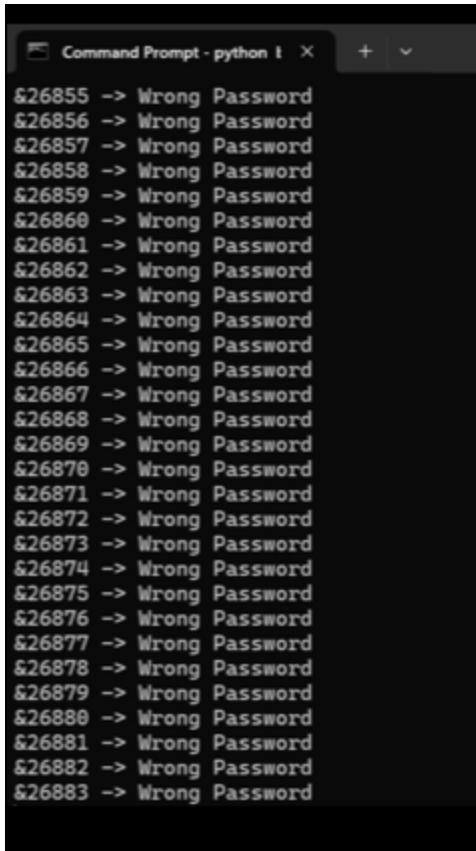
Documentation

Memory & file editing						
	Address	Value	Width	Type	Format	Unit
0x20000000	17138802	4C344F10	32	uint32_t	41524513	0x10000000000000000000000000000000
0x20000010	17138457	9C783004	32	uint32_t	17066773	0x10000000000000000000000000000000
0x20000020	17138458	9C783004	32	uint32_t	30364700	0x10000000000000000000000000000000
0x20000030	17138459	95469730	32	uint32_t	42562129	0x10000000000000000000000000000000
0x20000040	17138460	5776A637	32	uint32_t	18644612	0x10000000000000000000000000000000
0x20000050	17138461	7703E7D0	32	uint32_t	17066774	0x10000000000000000000000000000000
0x20000060	17138462	43C4C56B	32	uint32_t	20781935	0x10000000000000000000000000000000
0x20000070	17138472	2030E6A8	32	uint32_t	40199930	0x10000000000000000000000000000000
0x20000080	17138473	A0000000	32	uint32_t	17066775	0x10000000000000000000000000000000
0x20000090	17138474	00000000	32	uint32_t	17066776	0x10000000000000000000000000000000
0x200000A0	17138475	97321354	32	int32_t	70344949	0x10000000000000000000000000000000
0x200000B0	17138476	98C56145	32	int32_t	10047394	0x10000000000000000000000000000000
0x200000C0	17138477	73500480	32	int32_t	24000023	0x10000000000000000000000000000000



Brute Force Scripting

- Go through every possible password combination until the correct one is found
 - Create a python script for brute force in the RAMN
 - The output will be shown by running the script in Linux and will stop at the password that gives the flag



```
Command Prompt - python 3
S26855 -> Wrong Password
S26856 -> Wrong Password
S26857 -> Wrong Password
S26858 -> Wrong Password
S26859 -> Wrong Password
S26860 -> Wrong Password
S26861 -> Wrong Password
S26862 -> Wrong Password
S26863 -> Wrong Password
S26864 -> Wrong Password
S26865 -> Wrong Password
S26866 -> Wrong Password
S26867 -> Wrong Password
S26868 -> Wrong Password
S26869 -> Wrong Password
S26870 -> Wrong Password
S26871 -> Wrong Password
S26872 -> Wrong Password
S26873 -> Wrong Password
S26874 -> Wrong Password
S26875 -> Wrong Password
S26876 -> Wrong Password
S26877 -> Wrong Password
S26878 -> Wrong Password
S26879 -> Wrong Password
S26880 -> Wrong Password
S26881 -> Wrong Password
S26882 -> Wrong Password
S26883 -> Wrong Password
```



Documentation

ECU Manipulation

- Change values of physical inputs without utilizing physical controls.
 - Linux
 - Set up attack
 - Disable ECUs
 - Modify ECU values
 - Show output on CARLA / LCD Screen pod.
 - CARLA is an open-source driving simulator that we use to

```
colton@colton-ThinkPad-P1-Gen-2: ~
colton@colton-ThinkPad-P1-Gen-2:~$ candump can0 | grep 062
can0  062      [2]  0F FF
```

Figure X. CAN frame sent to change steering value.



Documentation



Documentation

- Streamlined process.
- Step-by-step instructions.
- Resources (hyperlinks).
- Debugging instructions.
- Entry-level Oriented.



Documentation

Documentation

The screenshot shows a web browser window with the following details:

- Title Bar:** Welcome to F25-04 RAMN's documentation!
- Address Bar:** f25-04-drive-secure-teaching-automotive-cybersecurity-with-ramn.readthedocs.io/en/latest/index.html
- Page Content:**
 - Header:** RAMN 0.1.0
 - Search Bar:** Search docs
 - Navigation:** Intro, asd
 - Image:** A screenshot of a mobile application interface titled "AWS Student Learn > Share challenge".
 - Text:** AWS Student Learn > Share challenge
Ad by EthicalAds
 - Section:** Welcome to F25-04 RAMN's documentation!
 - Image:** Virginia Tech Transportation Institute logo
 - Text:** Hello, We are an ECE senior design team tasked by our customer to develop a cybersecurity challenge using the RAMN board. Below are import links that will be useful.
 - Links:** Our Github, RAMN Github, RAMN Read The Docs
 - Note:** This project is under active development.
 - Table of Contents:**
 - Intro
 - What is RAMN?
 - What is on the Read the Docs?
- Bottom Right:** latest dropdown menu

Proposed Solution Cont.

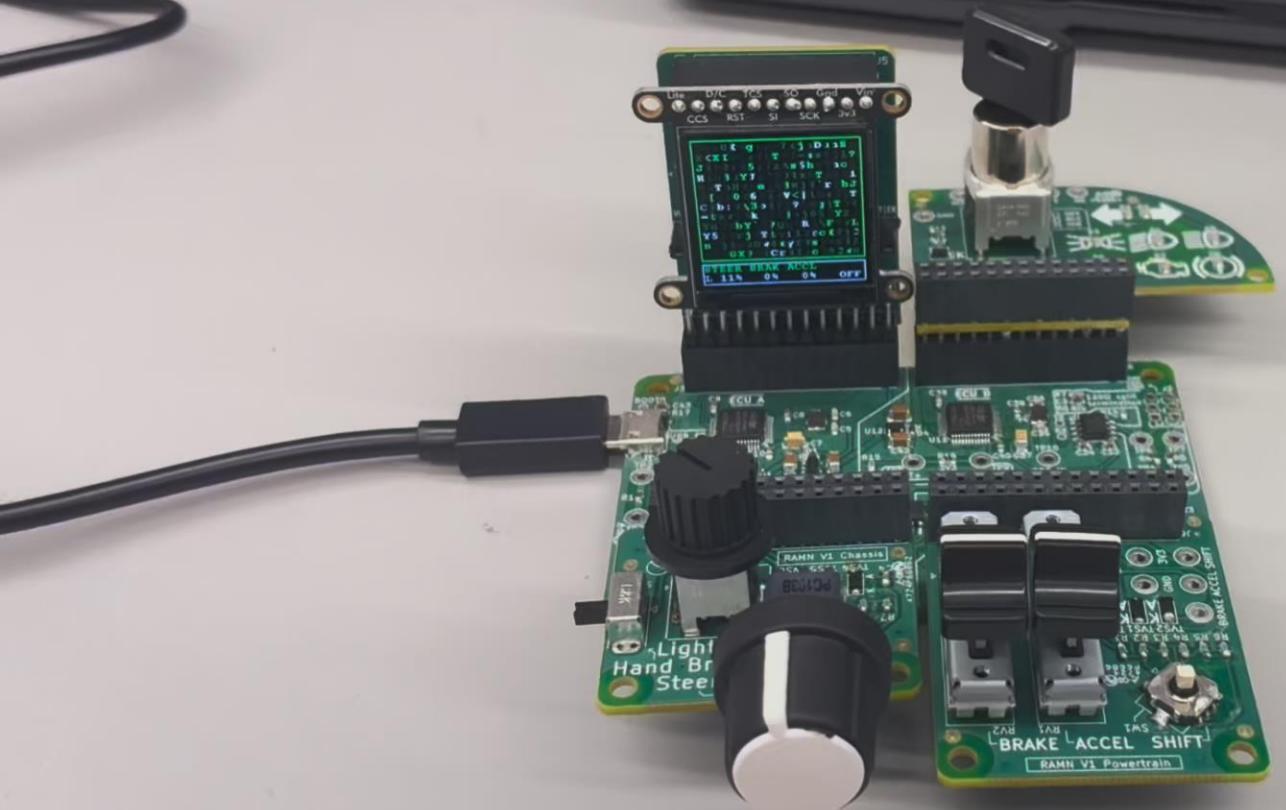
- What makes your solutions innovative?
 - Our work is focused on the automotive industry
 - Our work offers beginner level challenges as an educational tool
 - Our work provides more detailed documentation than other resources

Technical Requirements & Constraints

- What are the high-level requirements?
 - Assemble hardware
 - CARLA - Driving Simulation
 - Create cybersecurity challenges(CTFs)
- What are the high-level constraints?
 - Training Time (solder training)
 - Missing components for 2 RAMN systems (backup)

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
 - ST-Link V2 Debugger
 - Spent \$37.30 to buy extra parts



Summary of Results & Conclusions

Contributions

- Contributed to existing documentation
- Filled in the gaps with our own website
- Created our own challenges

Acknowledgments

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