Drive Secure: Teaching Automotive Cybersecurity with RAMN

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

Customer: Dr. Zeb Bowden at VTTI Mentor: Dr. Joe Adams

What is RAMN?

The Resistant Automotive Miniature Network (RAMN):

- Is a cost-effective and portable solution to teaching cybersecurity on modern vehicles.
- Utilizes four open-source STM32 microcontrollers.
- Simulates the function of Electronic Control Units (ECUs) in the automotive industry.

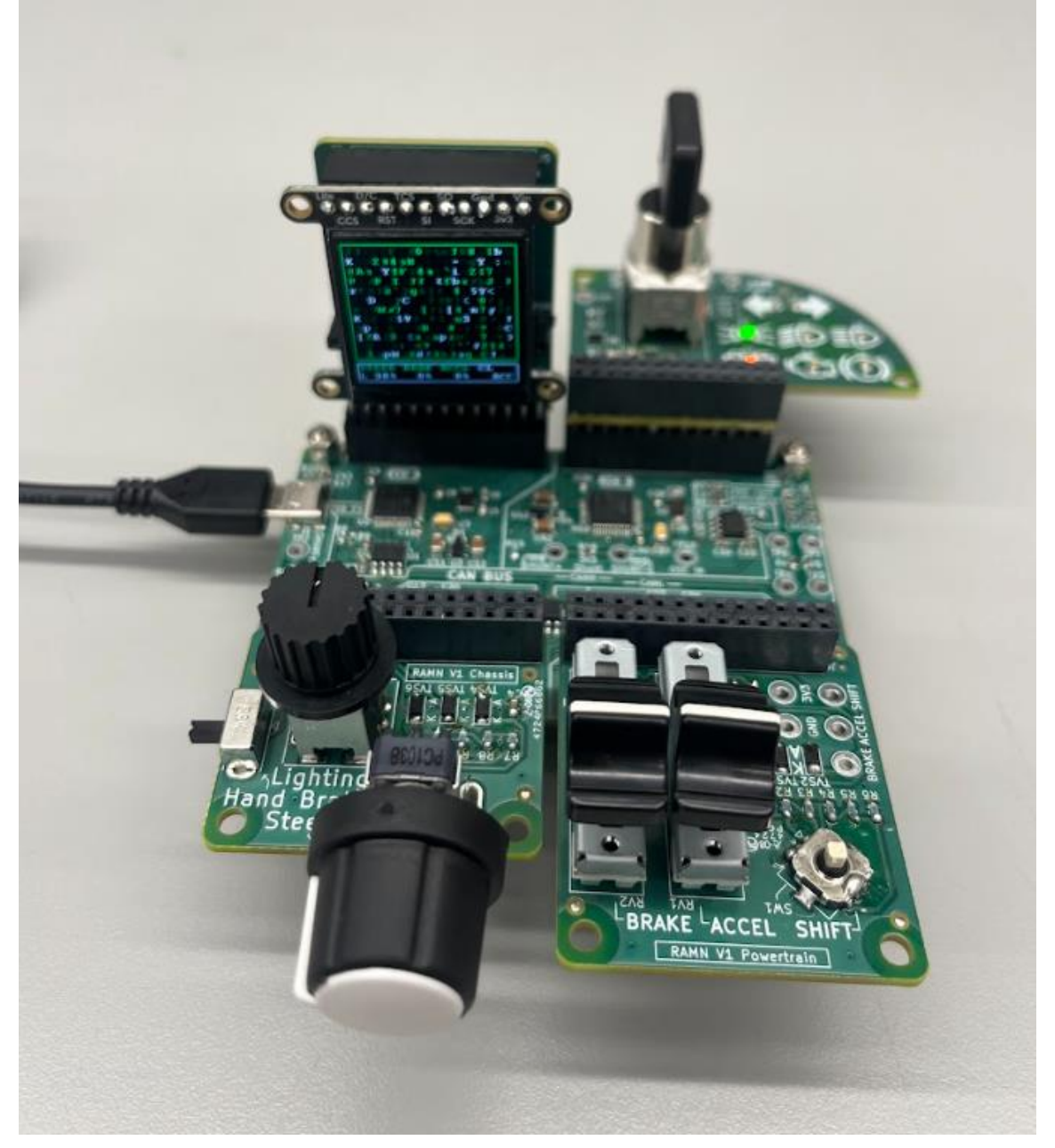


Figure 1. RAMN system.

Consists Of:

- Main board (center)
- LCD Screen Pod (top left)
- Chassis Pod (bottom left)
- Powertrain Pod (bottom right)
- Body Pod (top right)

Why?

As cars become more connected, they face the same cybersecurity risks as computers. This challenge uses RAMN to help participants uncover vulnerabilities, develop defenses, and advance the future of secure automotive systems.

Project Overview

Our Challenges:

- Entry-Level Capture the Flag Challenge
  - Use UDS commands to find the flag
- "Brute Force" Password Identifier
  - Attempt every password combination to identify the answer
- ECU Manipulation:
  - Interact at data layer instead of physical layer.

System Architecture

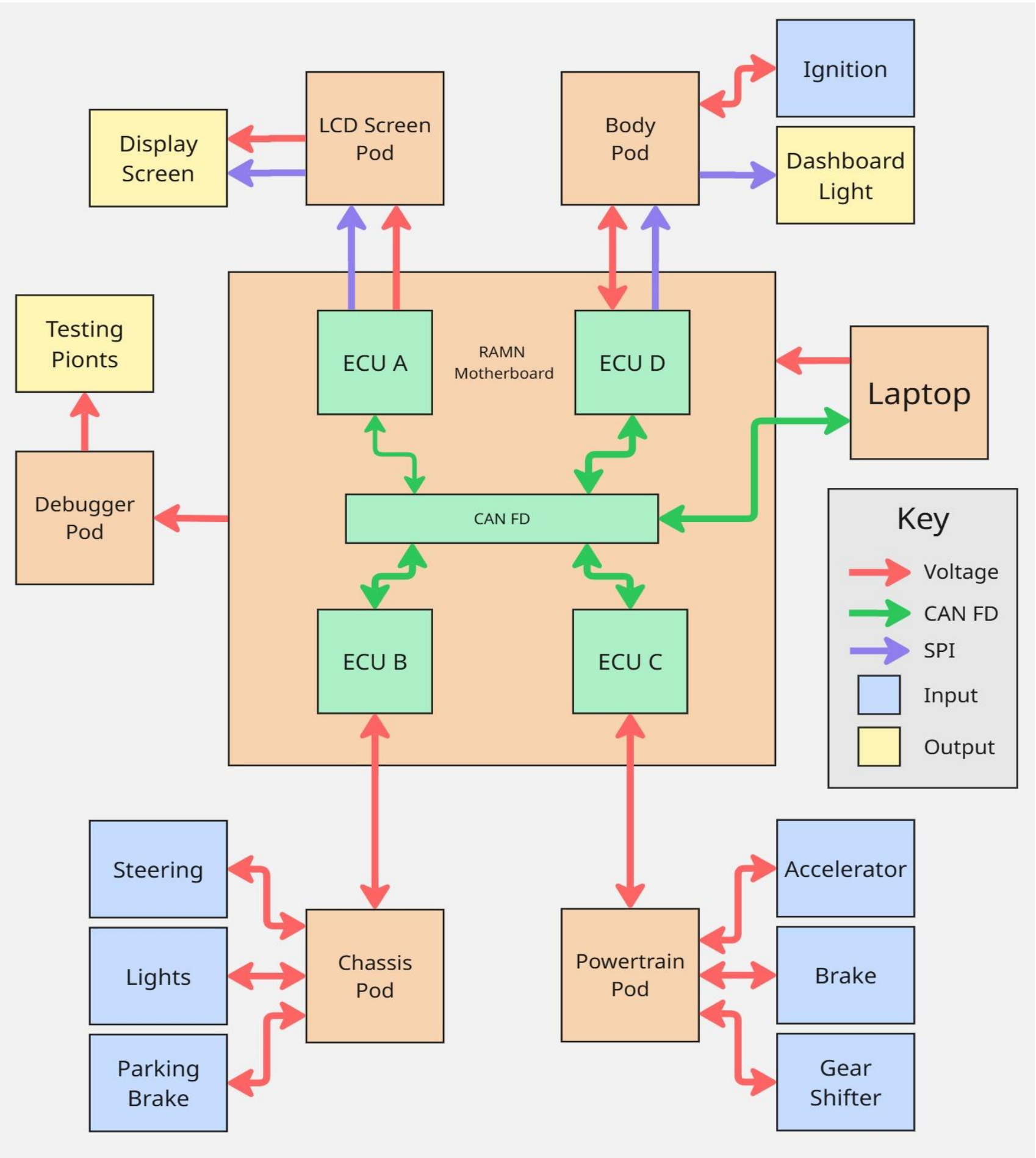
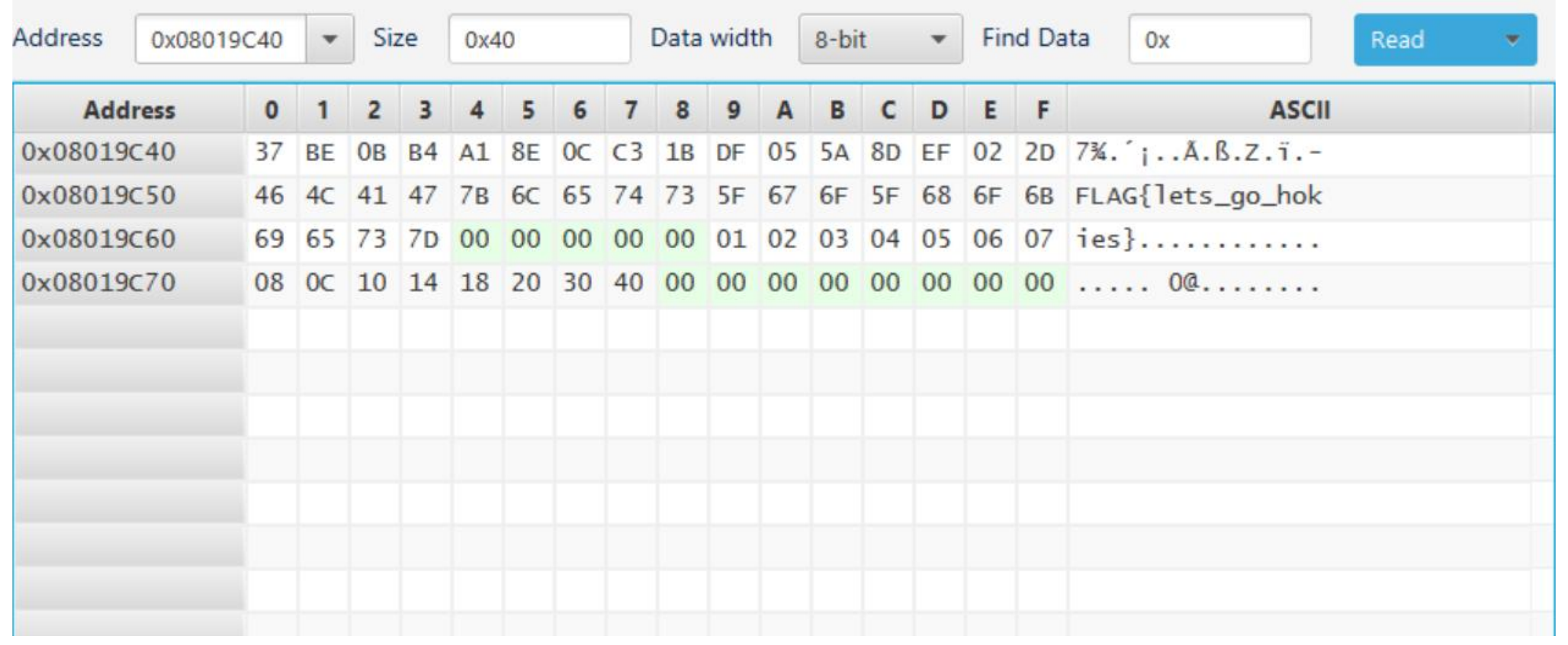


Figure 2. RAMN System architecture.

Brute Force Scripting

```
&27741 -> Wrong Password
&27742 -> Wrong Password
&27743 -> Wrong Password
&27744 -> Wrong Password
&27745 -> Wrong Password
&27746 -> Wrong Password
&27747 -> Wrong Password
&27748 -> Wrong Password
&27749 -> Wrong Password
&27750 -> Wrong Password
&27751 -> Wrong Password
&27752 -> Wrong Password
&27753 -> Wrong Password
&27754 -> Wrong Password
&27755 -> Wrong Password
&27756 -> Wrong Password
&27757 -> Wrong Password
&27758 -> Wrong Password
&27759 -> Wrong Password
&27760 -> Wrong Password
&27761 -> Wrong Password
&27762 -> flag{USB_BRUTEFORCE}
FOUND: &27762 -> flag{USB_BRUTEFORCE}
```

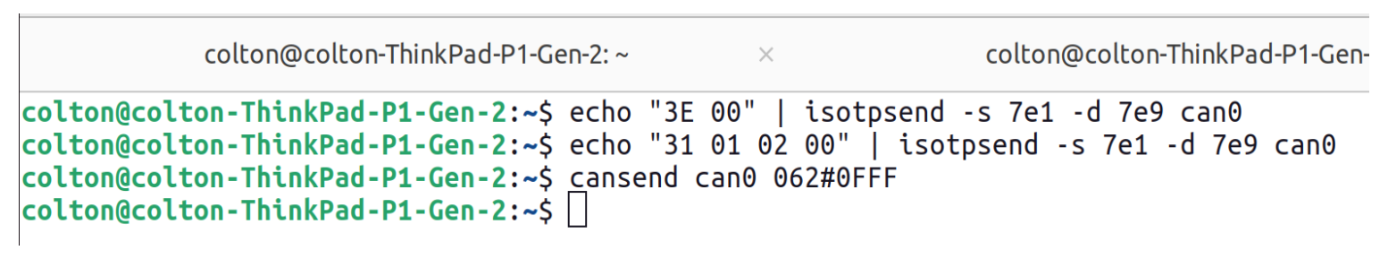
Capture The Flag Challenge



Address 0x08019C40 Size 0x40 Data width 8-bit Find Data 0x

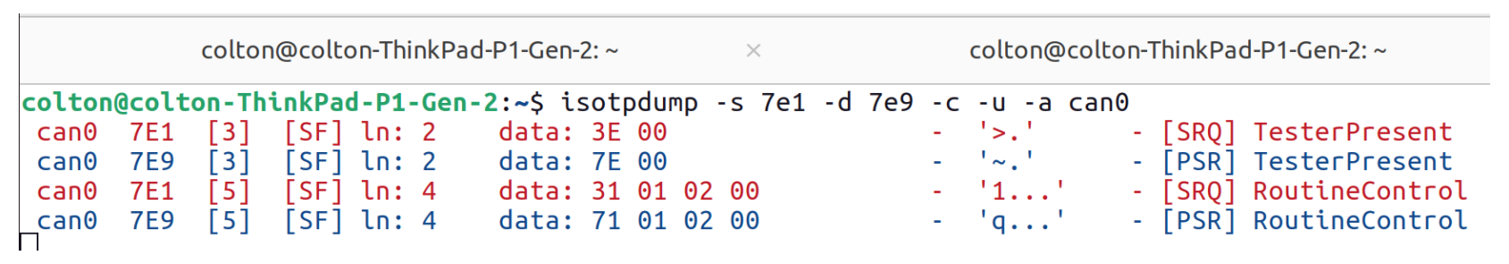
Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
0x08019C40	37	BE	0B	B4	A1	8E	0C	C3	1B	DF	05	5A	8D	EF	02	2D	7¾.´¡..Ã.ß.Z.ï.-
0x08019C50	46	4C	41	47	7B	6C	65	74	73	5F	67	6F	5F	68	6F	6B	FLAG{lets_go_hok
0x08019C60	69	65	73	7D	00	00	00	00	00	01	02	03	04	05	06	07	ies}............
0x08019C70	08	0C	10	14	18	20	30	40	00	00	00	00	00	00	00	00	..... 0@........

ECU Manipulation



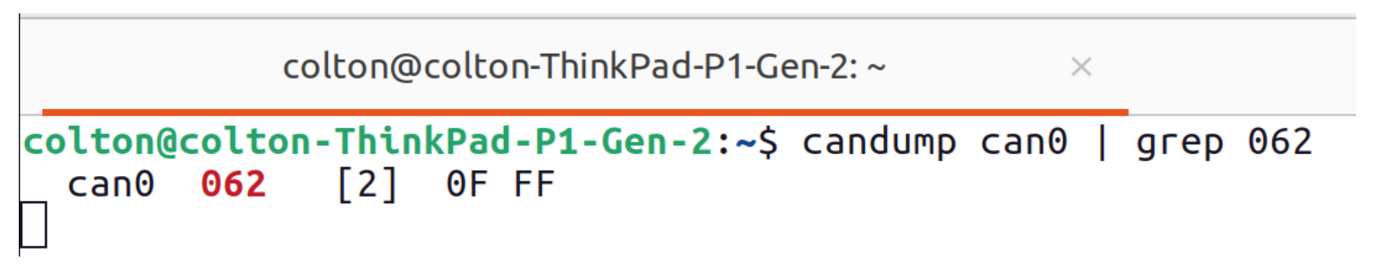
```
colton@colton-ThinkPad-P1-Gen-2: ~          colton@colton-ThinkPad-P1-Gen-
colton@colton-ThinkPad-P1-Gen-2:~$ echo "3E 00" | isotpsend -s 7e1 -d 7e9 can0
colton@colton-ThinkPad-P1-Gen-2:~$ echo "31 01 02 00" | isotpsend -s 7e1 -d 7e9 can0
colton@colton-ThinkPad-P1-Gen-2:~$ cansend can0 062#0FFF
colton@colton-ThinkPad-P1-Gen-2:~$ 
```

Figure X. Commands sent to RAMN board via CAN-UTILS after all set-up steps are complete. Set-up steps can be found in our documentation.



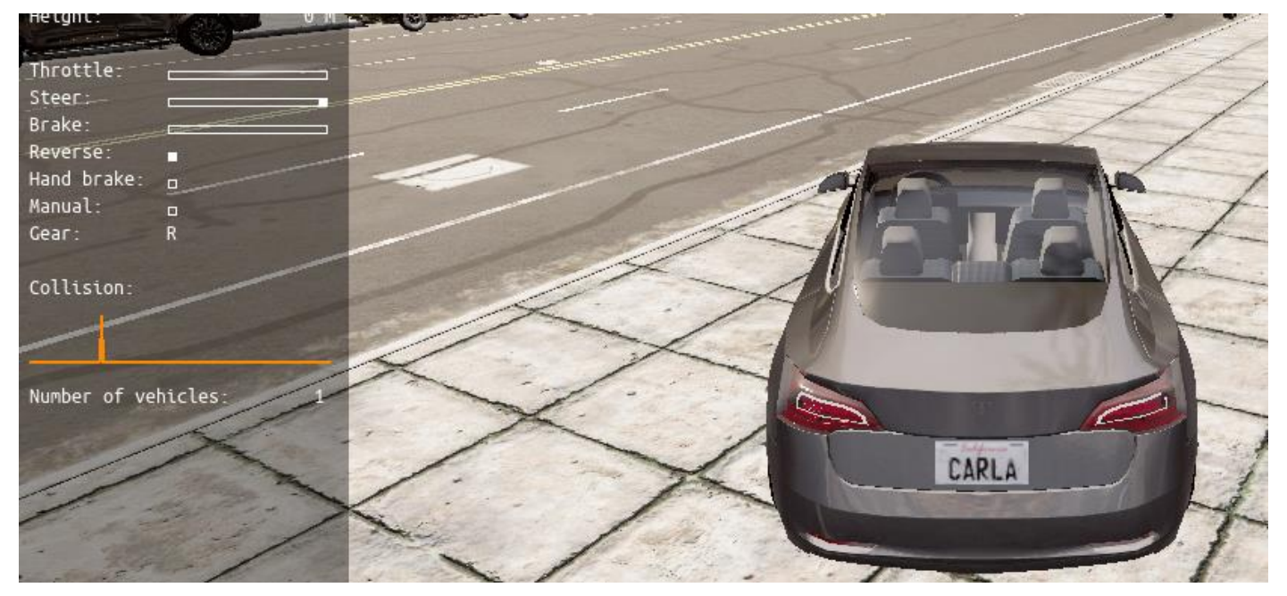
```
colton@colton-ThinkPad-P1-Gen-2: ~          colton@colton-ThinkPad-P1-Gen-2: ~
colton@colton-ThinkPad-P1-Gen-2:~$ isotpdump -s 7e1 -d 7e9 -c -u -a can0
 can0  7E1  [3]  [SF] ln: 2   data: 3E 00          -  '>.'     - [SRQ] TesterPresent
 can0  7E9  [3]  [SF] ln: 2   data: 7E 00          -  '~.'     - [PSR] TesterPresent
 can0  7E1  [5]  [SF] ln: 4   data: 31 01 02 00    -  '1...'   - [SRQ] RoutineControl
 can0  7E9  [5]  [SF] ln: 4   data: 71 01 02 00    -  'q...'   - [PSR] RoutineControl
```

Figure Y. Response messages from RAMN to sent commands in Figure X.



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

Figure Z. CAN frame changed by using cansend command in Figure X, HEX 0F FF is 100% right steering.



```
Throttle:
Steer:
Brake:
Reverse:
Hand brake:
Manual:
Gear:         R

Collision:

Number of vehicles:     1
```

Figure A. Visual output of cansend command to turn steering 100% right, observed by the white square on the steering value in CARLA.

RAMN/Challenge Documentation

A website for the RAMN already exists, but it was more resourceful for experienced users.

Our documentation:

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

SCAN ME

Conclusion

Our solution provides VTTI with three beginner level cybersecurity challenges and documentation to better help students understand automotive cybersecurity. This serves as foundation for future cybersecurity challenges.

Future Plans

- Increase cybersecurity challenge difficulty
- Design new expansion pods i.e. wireless connectivity
- Hosting a competition with our challenges
- Teach automotive cybersecurity

Acknowledgements

Special thank you to the following for supporting this work:

- Dr. Joe Adams (Project Mentor)
- Dr. Tim Talty (SME)
- Dr. Zeb Bowden (Customer)
- Camille Gay (RAMN Creator)
- Kim Medley (ECE Purchasing)
- Rusty Stewart (For Soldering Training)