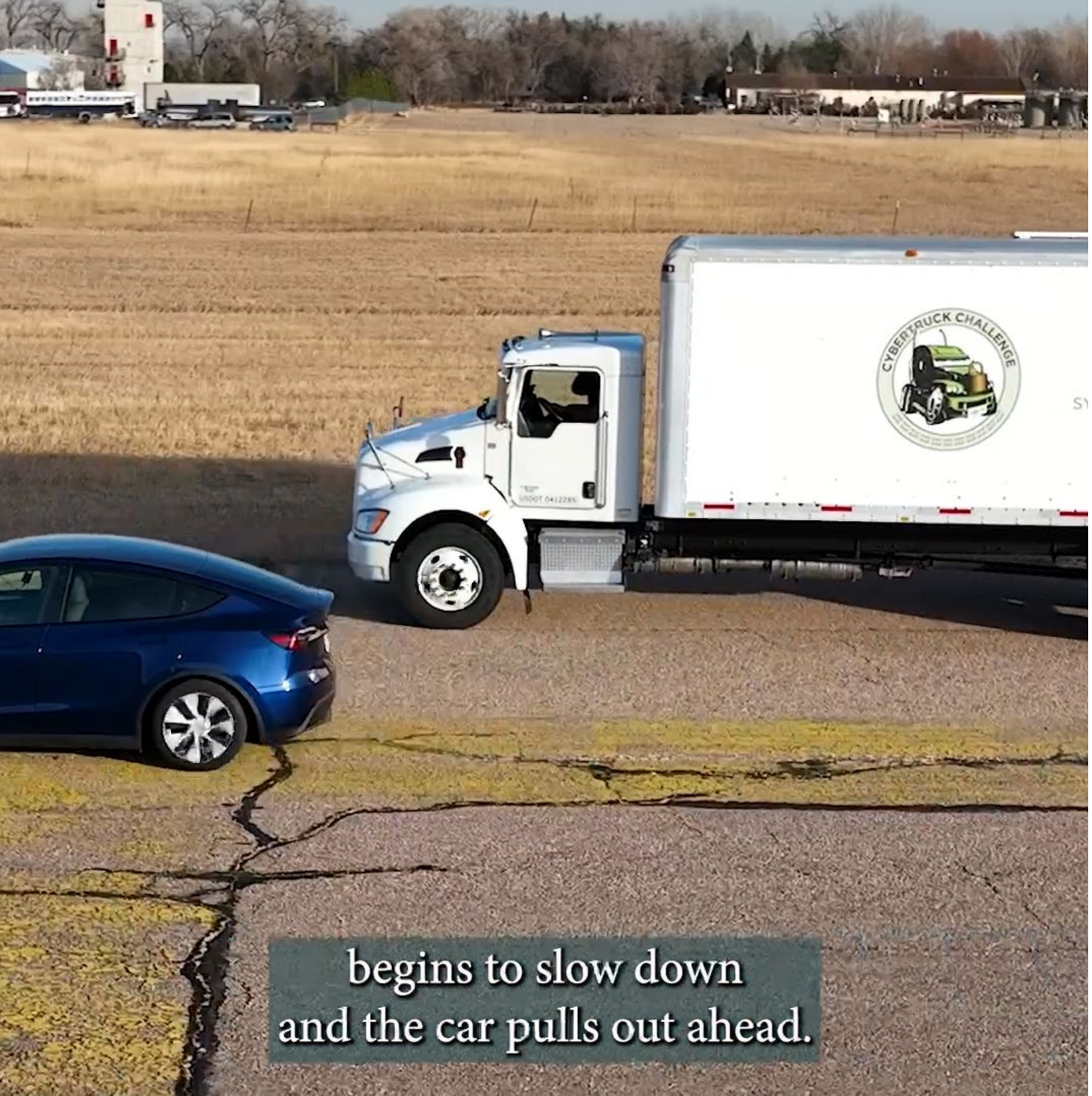
CyberBoat Challenge: Building Talent and Community

Jeremy Daily, Associate Professor of Systems Engineering
jeremy.daily@colostate.edu

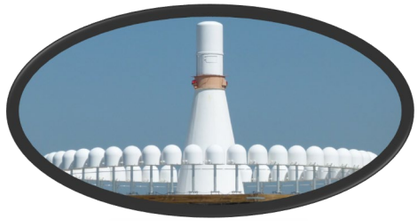
SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY



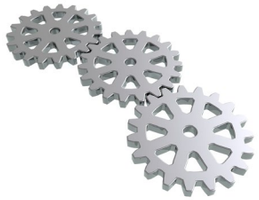
Can we do this with boats?

- Unauthorized (or unknown) Wireless to the vessel’s controller area network.

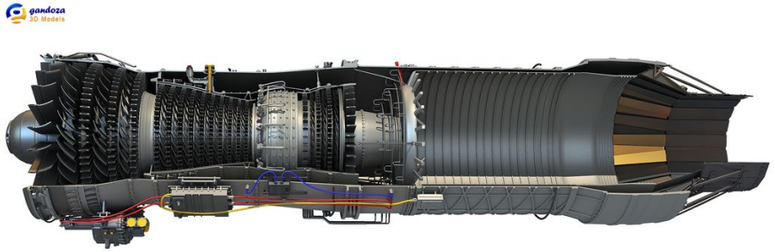
Introducing Dr. Jeremy Daily



US Air Force Flightline Electronics Maintenance



Formal Education in Mechanical Engineering



Contracted Aerospace Engineer at Wright-Patterson AFB

Faculty in the Department of Mechanical Engineering

Startup Company for Heavy Vehicle Digital Forensics

Co-Founder and Director

SYSTEMS ENGINEERING

COLORADO STATE UNIVERSITY

Department of Systems Engineering

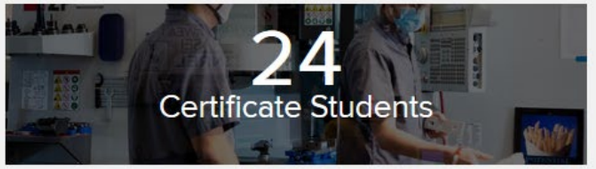
Our students and faculty implement systems-thinking to solve the world's most complex problems, ranging from aerospace systems to cybersecurity implementation.

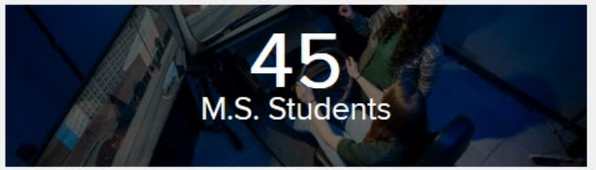
Application Information

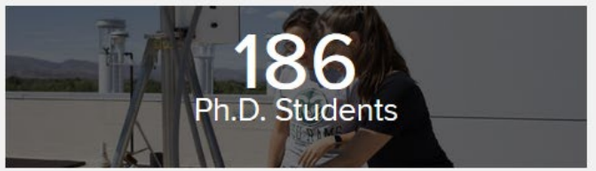
Course Offerings

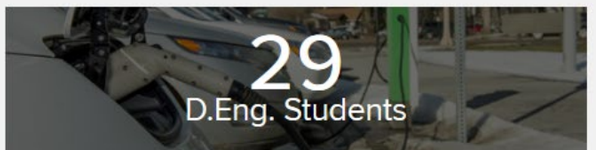
https://www.engr.colostate.edu/se

Systems Engineering by the Numbers





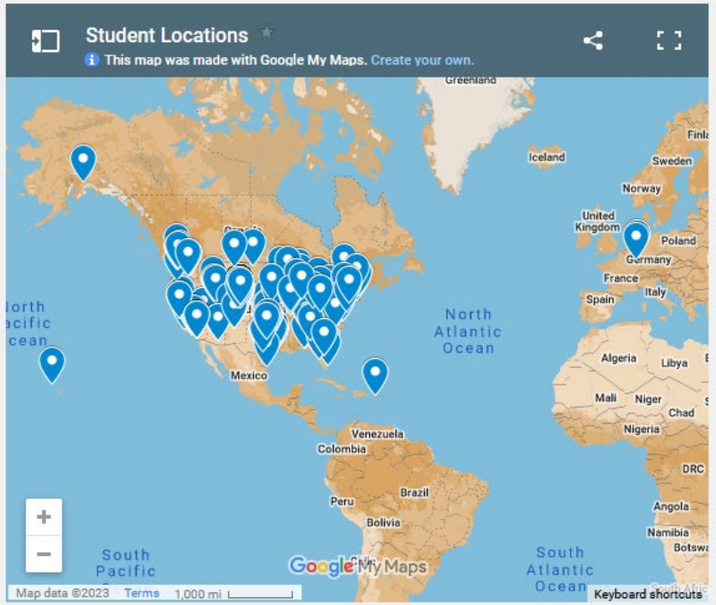




Where Our Students Are Located

Our online program allows students from all over the country and world to access our degree programs and the expertise of our professors.

Use the map to explore where our students are located while studying with us!



Agenda

- Motivation
- CyberBoat Challenge
  - What: Learn maritime cybersecurity by hacking
  - Who: Students, Security Researchers, Government, Industry
  - Where: Michigan, South Carolina
  - When: May 2022, Sep. 2024 (planned)
  - Why: Develop talent and foster community
- CyberTruck Challenge
- J1939 Cybersecurity Examples
  - ELD Hack
  - CAN Bus Denial of Service
  - Message Spoofing
  - Address Claim Attacks
  - Transport Protocol Vulnerabilities

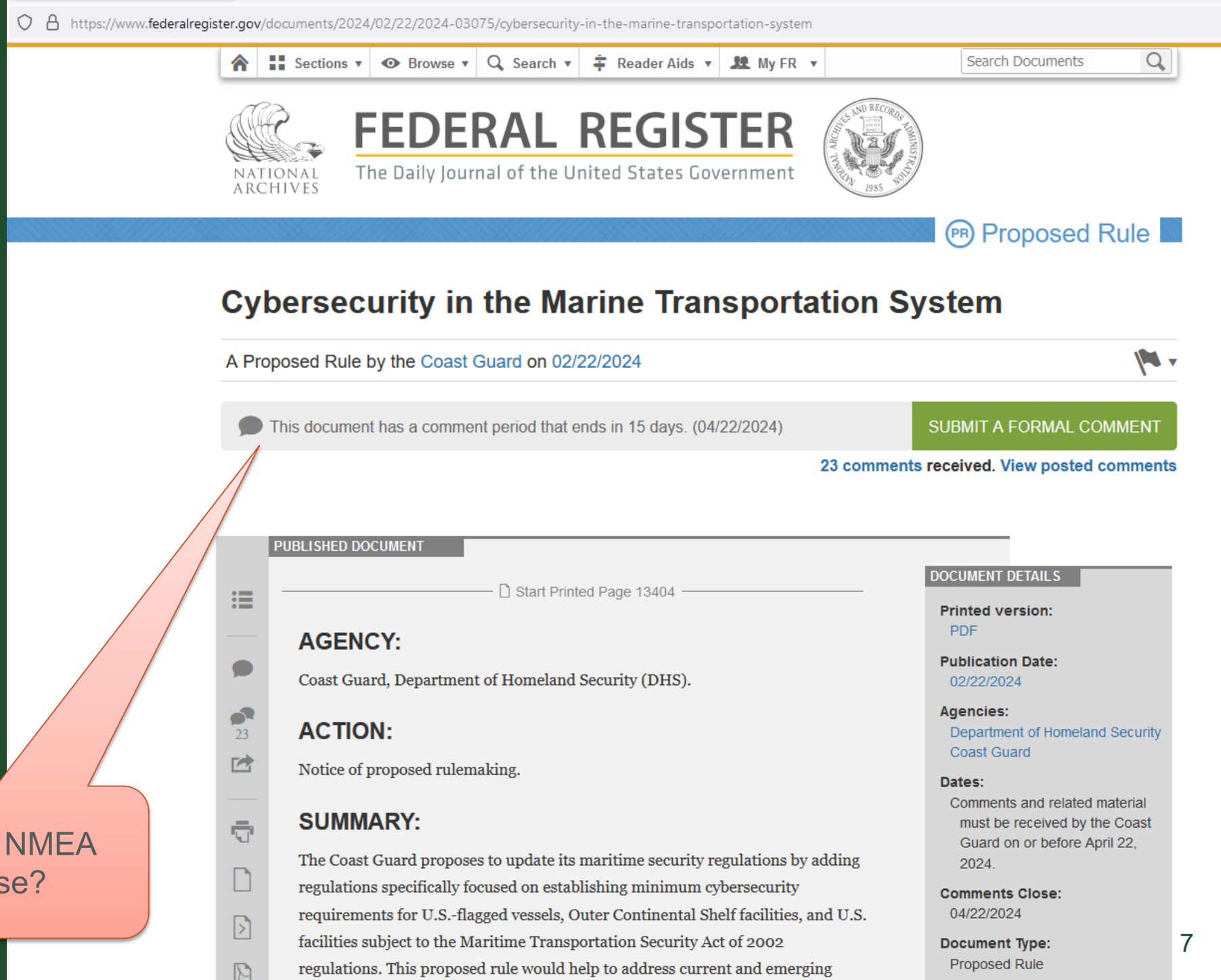
Government Pressure through Executive Order

https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Maritime Response for Cybersecurity

https://www.federalregister.gov/documents/2024/02/22/2024-03075/cybersecurity-in-the-marine-transportation-system

What is the NMEA Response?



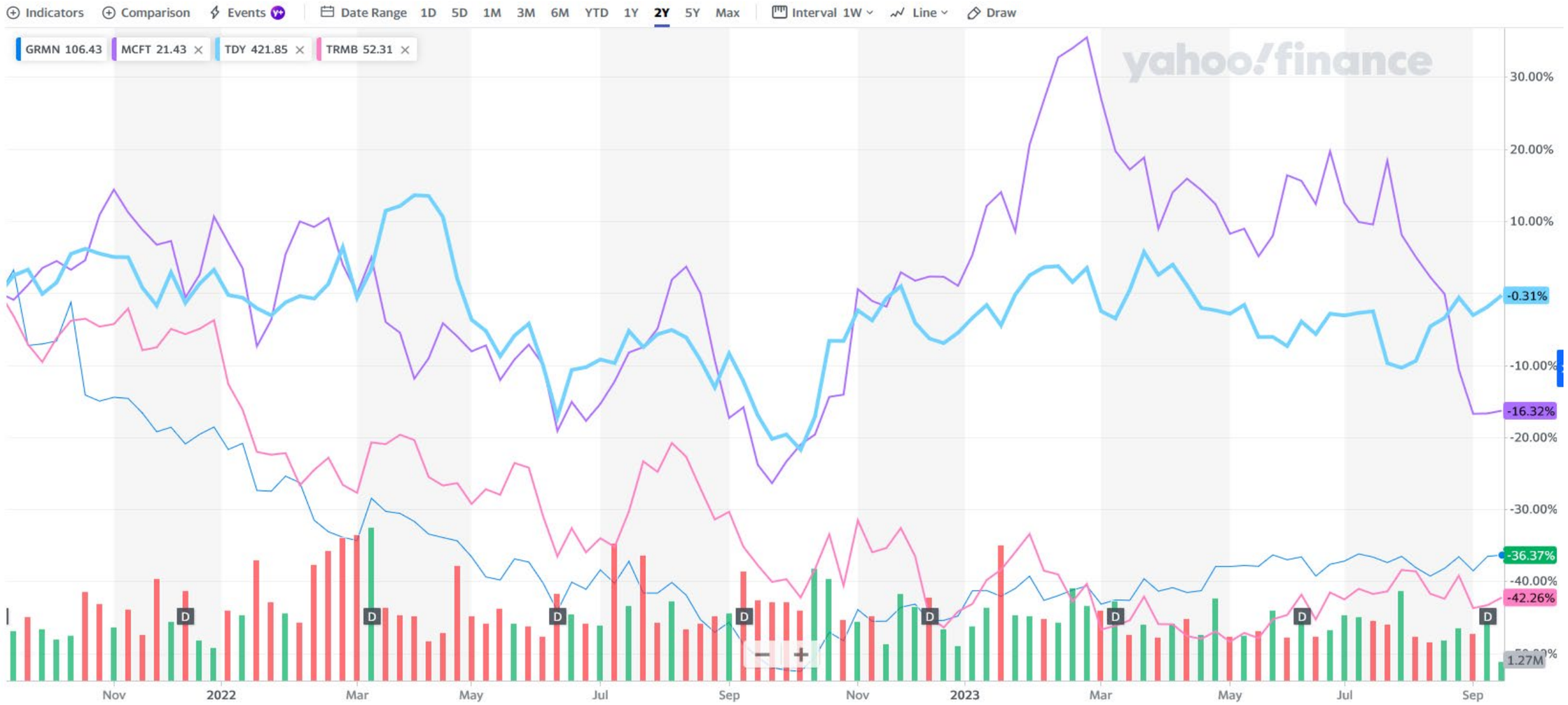
Types of Hackers

- White Hat (Ethical) Hackers
  - Examples: Researchers, penetration testers, students
  - Outcomes: Responsible disclosures, opportunities to fix products
- Grey Hat Hackers
  - Examples: Cyberpunks, Hacktivists
  - Outcomes: Loss of reputation and revenue for a company, safety recalls, privacy exposure
- Black Hat Hackers
  - Examples: Nation states, advanced persistent threats (APTs), cyber-insider, criminals
  - Outcome: theft, loss, destruction, leaked information, privacy exposure, safety concerns, war

Motivations:
- Curiosity
- Financial
- Notoriety
- Revenge
- Recreation
- Ideology
- Aggression

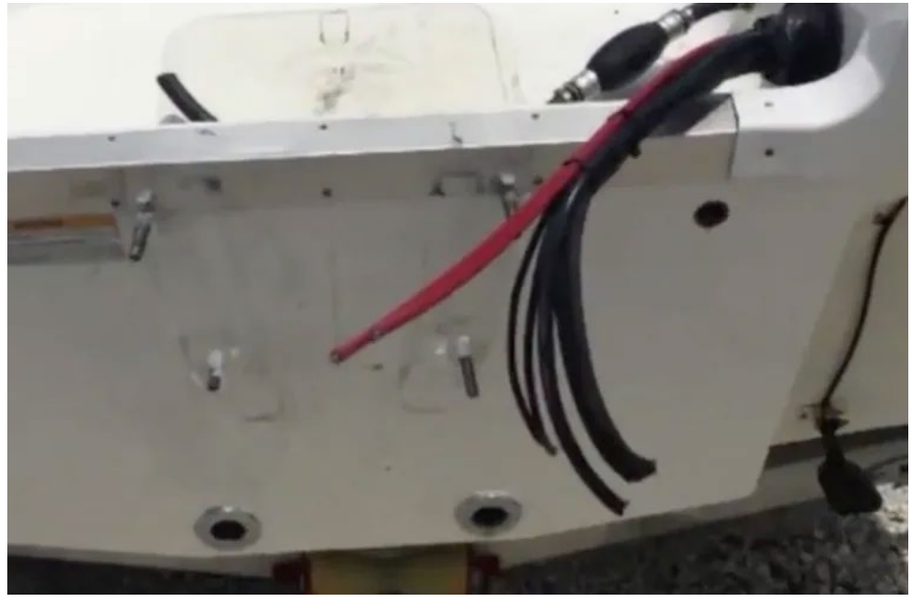
Use curious ethical hackers to protect against the others

Why Hack Boats?

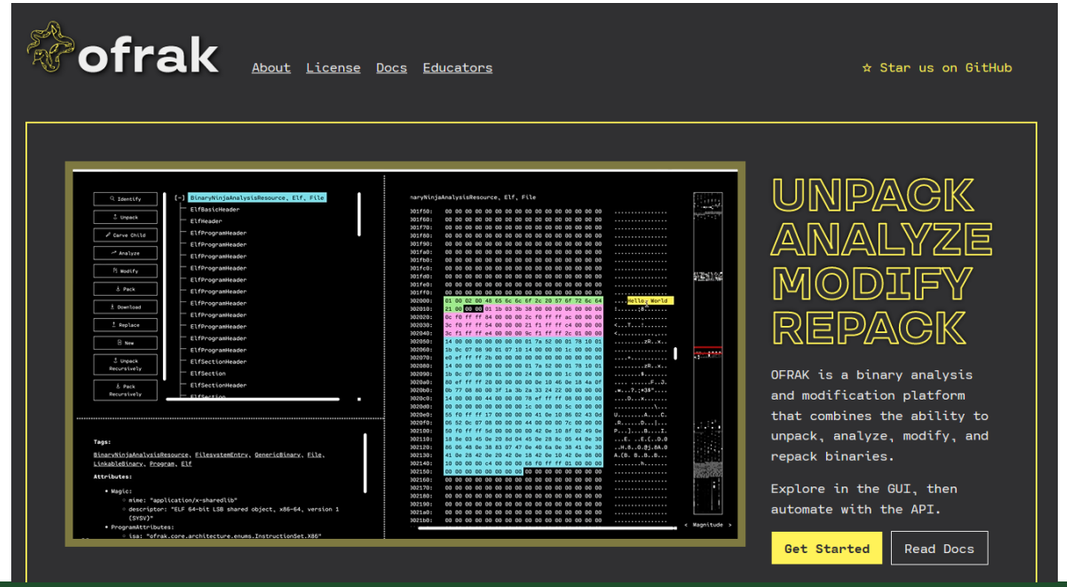


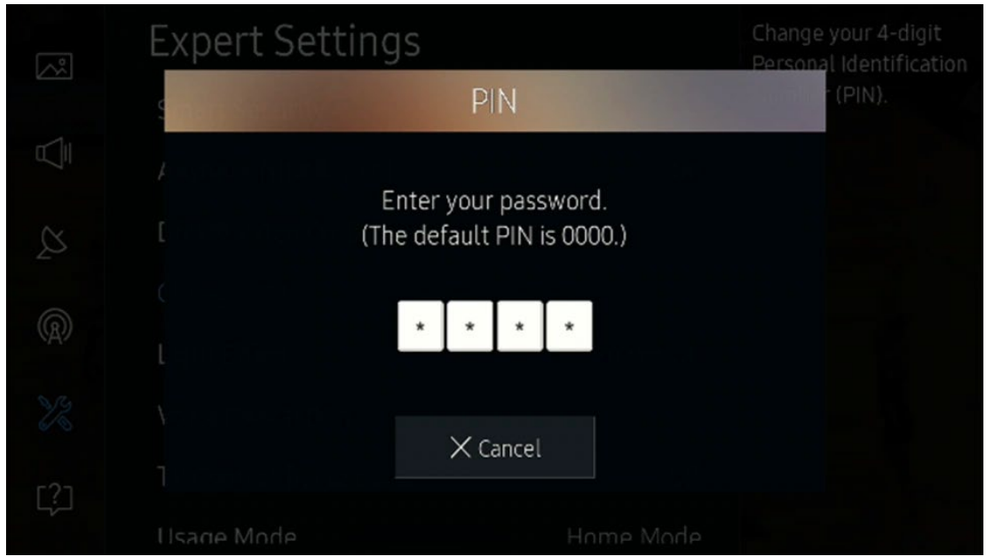
Cybersecurity and Theft

- Manufacturers add PINs or passcodes in devices to limit post-theft utility
  - Not used
  - Not changed
- Firmware modifications “defeature” PINs – industrialize theft.



https://www.tradeonlytoday.com/tech/task-force-seeks-to-stop-marine-engine-and-electronics-thefts





Chip Tuning

Prior research lowers the barrier to entry for hacking on marine systems.

https://www.alientech-tuning.com/

https://www.alientech-tuning.com/product/kess3-master-marine-pwc-obd-protocols-activation/

Home > Kess 3 Tuning Tools and Software > Kess3 Master > KESS3 Master – Marine & PWC OBD Protocols activation

KESS3 MASTER – MARINE & PWC OBD PROTOCOLS ACTIVATION

Code: KESS3MA004 ★★★★★ (3 customer reviews)

KESS3 MASTER

£1,160.00 In Stock

– 1 + Add to cart

SHARE (0)

DESCRIPTION REVIEWS (3)

DESCRIPTION

Alientech Kess3 Master Marine OBD Protocols. This activation package for the Kess 3 is for Marine and private water vehicles. Therefore, specifically, it is for marine tuning and ECU remapping applications that can be tuned through the OBD port.

The Alientech Kess3 Master Marine OBD Protocols are available as a single activation to your kess3 OBD tuning tool. As well as the option to add them to other single or multiple Kess 3 activation protocol groups. And hence building a deeper level of tuning options.

This is an OBD master Kess 3 activation package. As you are no doubt aware. Master tuning tools are usually selected by those who wish to purchase tuning files and ECU remapping files from a selection of tuning file providers. Unlike the slave tool option, you are not reliant on just one file provider. As well as tuners who wish to write their own tuning files, which of course the master version also permits.

TECHNICAL WHITE PAPER

SATCOM Terminals: Hacking by Air, Sea, and Land

Ruben Santamarta
Principal Security Consultant

White Hat Hacking Example

Abstract

Satellite Communications (SATCOM) plays a vital role in the global telecommunications system. IOActive evaluated the security posture of the most widely deployed Inmarsat, Iridium, and Thuraya SATCOM terminals.

IOActive analyzed the firmware of these devices and found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented, and/or insecure protocols.

These vulnerabilities have the potential to allow a malicious actor to intercept, manipulate, or block communications, and in some cases, to remotely take control of the physical device.

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

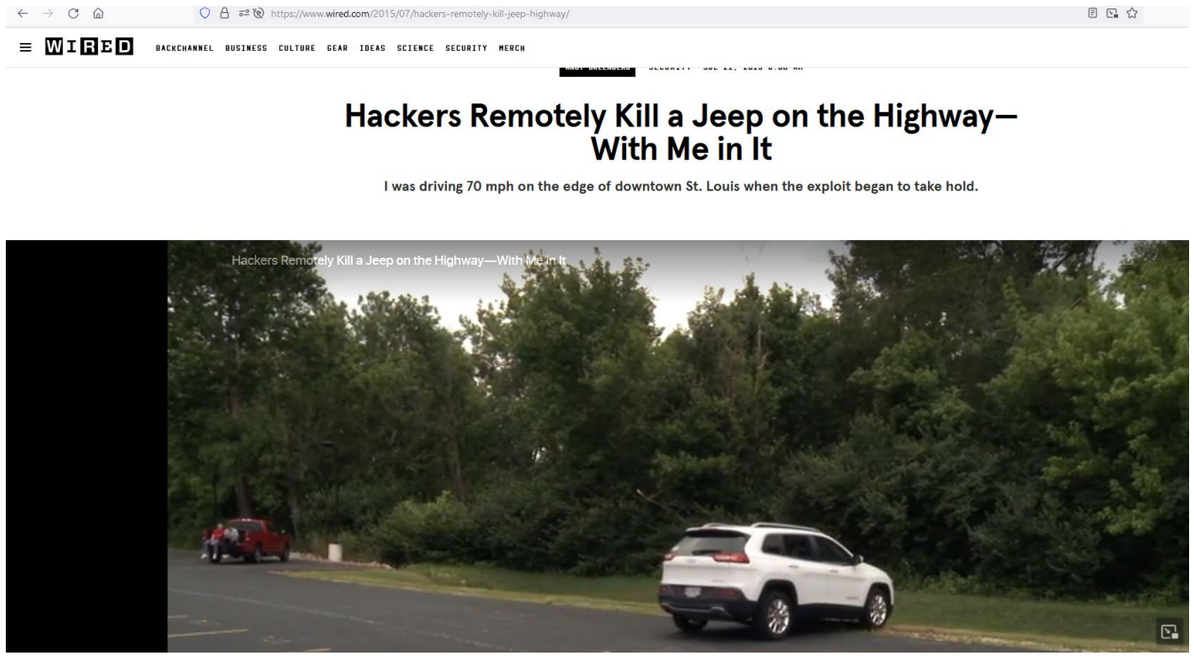
https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

Table 1: Summary of Vulnerabilities

Vendor	Product	Vulnerability Class	Service	Severity
Harris	 RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	 9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	 ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	 EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	 SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	 AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	 SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	 SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	 JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	 Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

Grey Hat Hacking

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



- https://illmatics.com/Remote%20Car%20Hacking.pdf

Hacktivism

Contents lists available at ScienceDirect

Ocean and Coastal Management

journal homepage: www.elsevier.com/locate/ocecoaman

Environmental impacts of increasing leisure boating activity in Mediterranean coastal waters

Arnau Carreño *, Josep Lloret

Oceans and Human Health Chair, Institute of Aquatic Ecology, University of Girona, C/ Maria Aurèlia Capmany 69, 17003, Girona, Catalonia, Spain

https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/cybersecurity-concerns-for-the-energy-sector-in-the-maritime-domain/

Cybersecurity Energy Transitions Geopolitics & Energy Security Maritime Security

Issue Brief | December 6, 2021

Cybersecurity concerns for the energy sector in the maritime domain

By Andy Bochman and Ian Ralby

https://www.reuters.com/markets/commodities/new-fsru-arrives-france-greenpeace-blocks-port-2023-09-18/

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Inve

Greenpeace blocks arrival of new LNG unit at French port

By **Forrest Crellin**

September 18, 2023 8:51 AM MDT · Updated a day ago

[2/2] Greenpeace environmental activists on kayaks write "gas kills" on a LNG processing terminal set to be operated by Total Energies in Le Havre port, France, September 18, 2023. Jean Nicholas Guillo / Greenpeace /Handout via REUTERS

Acquire Licensing Rights

PARIS, Sept 18 (Reuters) - A new LNG floating storage regasification unit (FSRU) arrived in western France on Monday morning, a TotalEnergies' (TTEF.PA) spokesperson said, as activist group Greenpeace tried to prevent it from entering port.

https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

NewScientist

Sign in | Enter search keywords

Technology

Ships fooled in GPS spoofing attack suggest Russian cyberweapon

By David Hambling

10 August 2017

Black Hat Hacking Examples

https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality

euronews.next BIZTECH NEWS MONEY WORK MOBILITY HEALTH HOME OPINION SI

HMS Defender: AIS spoofing is opening up a new front in the war on reality

By Tom Bateman

Published on 28/06/2021 - 15:40 • Updated 16:03

Share this article

A British warship triggered a dispute with Russia last week. But the conflict may have begun online even before alleged warning shots were fired.

An incident involving a British warship off the coast of Russian-occupied Crimea on June 24 may have begun online - with a virtual voyage that never really happened.

Worst Case Maritime Sensor Data in Decision Making

The Truth About Tonkin

Questions about the Gulf of Tonkin incidents have persisted for more than 40 years. But once-classified documents and tapes released in the past several years, combined with previously uncovered facts, make clear that high government officials distorted facts and deceived the American public about events that led to full U.S. involvement in the Vietnam War.

By Lieutenant Commander Pat Paterson, U.S. Navy

February 2008 | Naval History Magazine | Volume 22, Number 1

https://www.usni.org/magazines/naval-history-magazine/2008/february/truth-about-tonkin

We need a workforce to address maritime cybersecurity challenges.

What can we do about it?

Students connected to the NMEA2000 network on a Mastercraft X30

CyberBoat Challenge

- Inaugural Event at Michigan Tech Univ.
  - May of 2022
  - Houghton, MI (Upper Peninsula)

Misson Statement

1. Develop the next generation workforce by bringing awareness, excitement, professional involvement, and practicum-based training to the maritime cyber domain.
2. Establish a community of interest for maritime cybersecurity that transcends individual companies or departments and reaches across disciplines and organizations to make a more universal and experienced base of engineers and managers.

CyberBoat Challenge Class of 2022

Co-located Classroom and Learning Platform (Boat)

Students get unique opportunities to apply theory on the water

Schedule Highlights

Industry experts teach specialty classes

Last day is reserved for free-form assessments and student reports

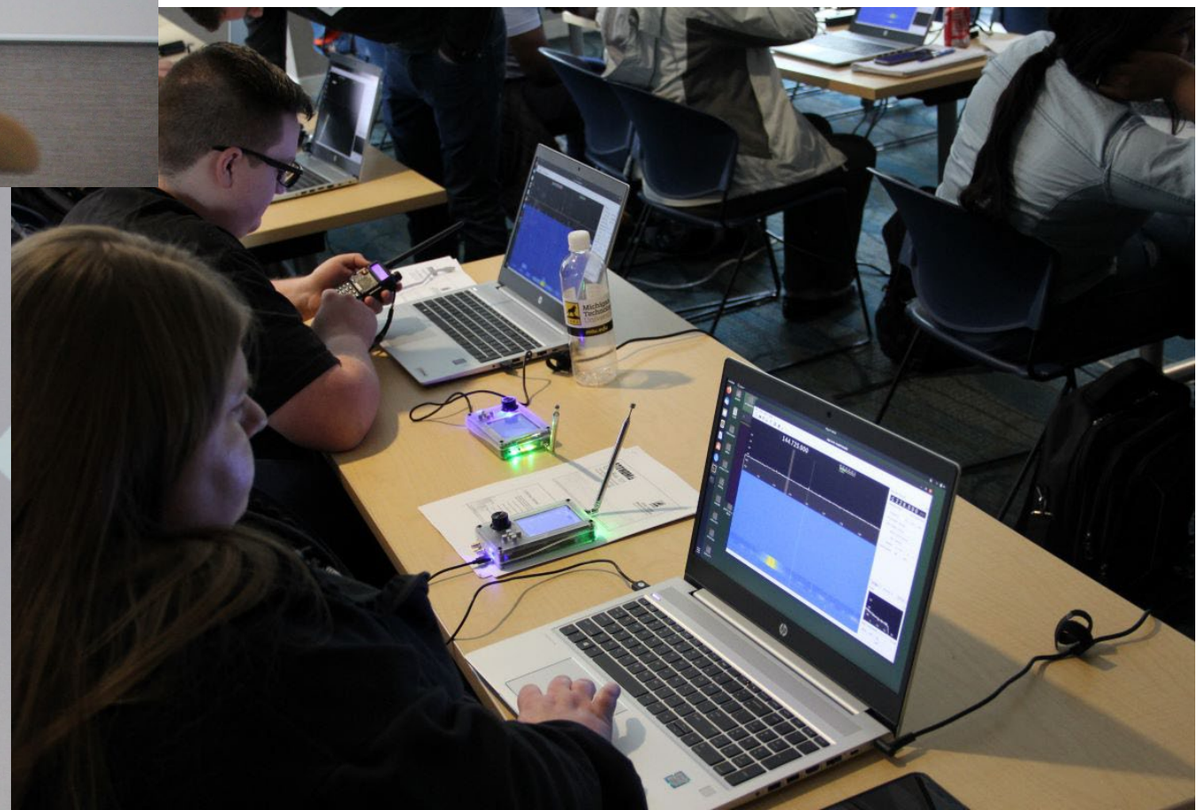
CyberBoat Challenge 2022 Schedule

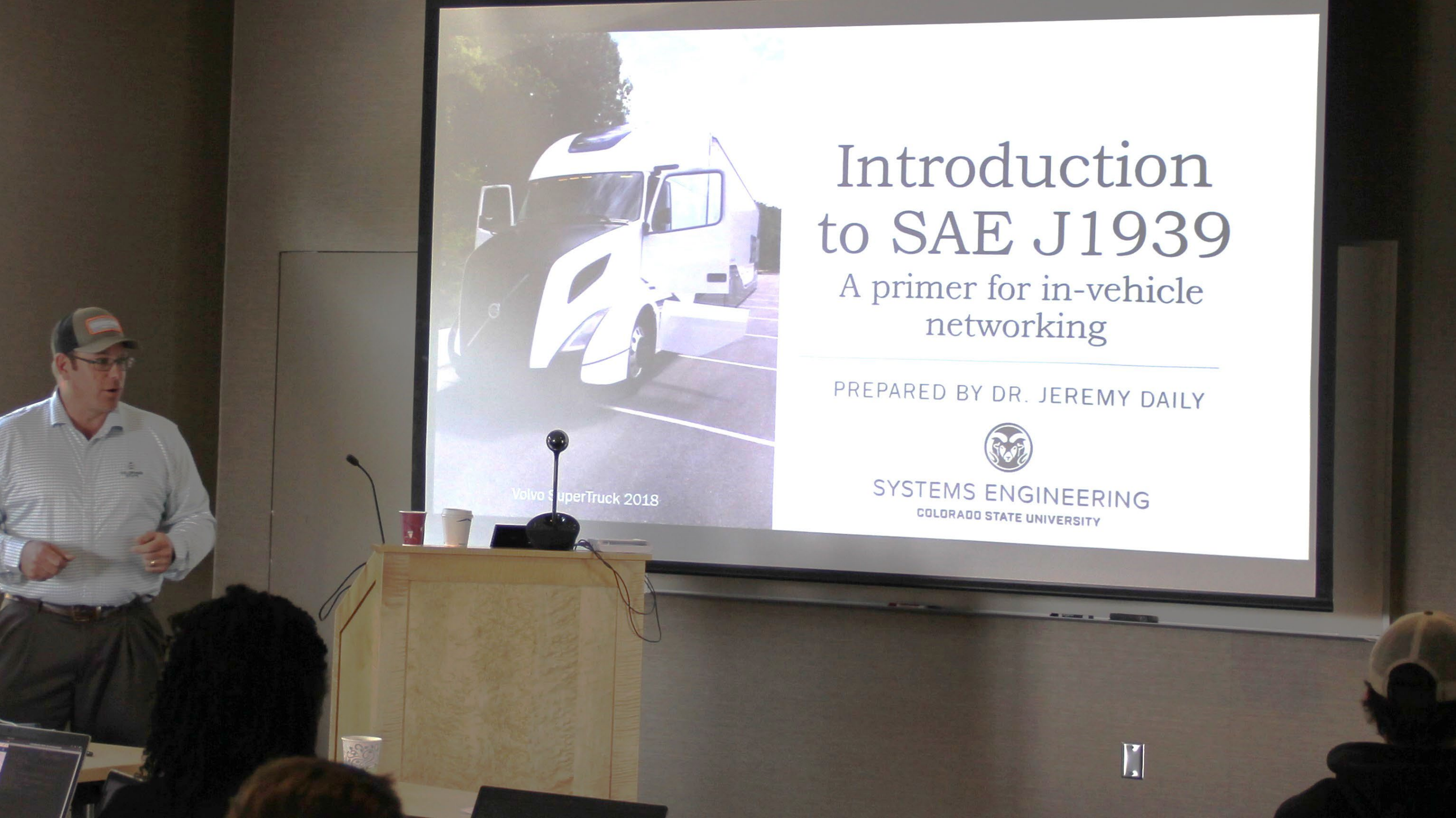
Versio

	Sunday 22May2022	Monday 23May2022	Tuesday 24May2022	Wednesday 25May2022
Before 0700	Site Closed	Site Closed		
0700-0730		Breakfast (Dorm Cafeteria)		
0730-0800				
0800-0830		Maritime ICS Protocol Exploitation (Fathom5)	Software RE (GRIMM)	**Assessment**
0830-0900				
0900-0930				
0930-1000				
1000-1030		RF Protocol Exploitation (Libertas & Fathom5)		
1030-1100				
1100-1130			Intro to J1939 (Daily)	
1130-1200				
1200-1230		Lunch (GLRC 201)		
1230-1300				
1300-1330		RF Protocol Exploitation (Libertas & Fathom5)	M-Tech staff time	**REPORTS**
1330-1400			Water Safety (USCG)	
1400-1430		Maritime Sensor Exploitation (Fathom5)	Maritime J1939 Demo (Daily)*	
1430-1500				Release
1500-1530				Site Closed
1530-1600			How to Conduct an Assessment* (AIS)	
1600-1630				
1630-1700		Maritime Testbed Assessment & CTF (Fathom5)		
1700-1730			Assessment Preperation and Planning	
1730-1800				
1800-1830	Informal Welcome Reception (Bonfire Grill)			
1830-1900				
1900-1930		Dinner (Bonfire Grill)	Dinner (GLRC 201)	
1930-2000				
2000-2030				
2030-2100				
After 2100	Site Closed			

Maritime Automatic Identification System (AIS) (in)security

Wireless Systems and Software Defined Radio (SDR)




Volvo SuperTruck 2018
Introduction to SAE J1939
A primer for in-vehicle networking
PREPARED BY DR. JEREMY DAILY
SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Grace Maritime Cyber Testbed

- Hands on with a large vessel simulator

NMEA 2000 Decoding Example

- can0 0DF50B81 42 B5 08 00 00 00 00 FF

0D – Priority (0b0000 1101 = 3)

DF50B – Water Depth PGN (0x1F50B)

81 – Dynamically Claimed Source Address

42 – Sequence ID (0x42 = 66)

B5 08 00 00 – Depth (0x8B5 = 2,229*0.01m = 22.29m = 73.13ft)

00 00 – Offset (zero)

FF – Maximum Depth Range (Not Available)

Water Depth — **PGN: 128267 hex: 1F50B**

Water depth relative to the transducer and offset of the measuring transducer. Positive offset numbers provide the distance from the transducer to the waterline. Negative offset numbers provide the distance from the transducer to the part of the keel of interest.

Single Frame:	Yes	*Priority Default:*	3	*Default Update Rate:*	1000 milliseconds	*Frequency:*	1. cycles per second
Destination:	Global	*Query Support:*	Optional	*Command Support:*	Optional	*ACK Rqmnts:*	None

Original Reference ID # 60

Field #	Field Name						
1	**Sequence ID**		*Byte Field Size:* 1 *Bit Field Size:*			*Request Parameter* Optional *Command Parameter:* Optional	
	DD056 Sequence ID			An upward counting number used to tie related information together between different PGNs . For example, the SID would be used to tie together the COG, SOG and RAIM values to a given position. 255=no valid position fix to tie it to. Range 0 to 252 for valid position fixes.			
	DF53 Integer, 8 bit unsigned	**uint8**	*Range:* 0 to 252	*Resolution:* 1 bit	Unit-less number		
2	**Water Depth, Transducer**		*Byte Field Size:* 4 *Bit Field Size:*			*Request Parameter* Optional *Command Parameter:* Optional	
	DD162 Water Depth At Transducer			Depth relative to the transducer location. Range of value specified in "Maximum Depth Range" (field 4).			
	DF09 Distance	**uint32**	*Range:* 0 to ~4.295x10E+7 m	*Resolution:* 1x10E-2 m			
3	**Offset**		*Byte Field Size:* 2 *Bit Field Size:*			*Request Parameter* Optional *Command Parameter:* Optional	
	DD161 Transducer Offset			Positive values represent distance from transducer to water line and negative values represent distance from the transducer to the keel.			
	DF46 Distance, signed, medium	**int16**	*Range:* +/- 32.764 m	*Resolution:* 1x10E-3 m			
4	**Maximum Depth Range**		*Byte Field Size:* 1 *Bit Field Size:*			*Request Parameter* Optional *Command Parameter:* Optional	
	DD350 Maximum Depth Range			Device classification of the Maximum Range over which water depth can be measured. 253 = Deeper than 2,520 meters 254 = Error 255 = Data Not Available			
	DF109 Distance, Rough Approxi	**uint8**	*Range:* 0 - 2,520 meters	*Resolution:* 10 meters			

Smart Buoy Hacking

Mentors work with students to explore cybersecurity of maritime systems

Connecting to the CAN Bus on the Boat

Students had their own connection to the NMEA2000 network.

Student Presentations

CyberBoat Challenge Sponsorship

- Michigan Tech Univ. provided housing
- Systems Engineering at Colorado State Univ. provided meals and travel
- Students provide their own travel
- We towed the boat from CO to MI
  - Yes, that's snow on the ski boat

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Sponsorship Opportunities

- The CyberBoat Challenge seeks sponsorship to conduct the event as a non-profit.
- Please consider one of the sponsorship tiers.
- Donations are tax deductible.
- Contact Jeremy at Jeremy.Daily@colostate.edu for additional details

Platinum - $25,000 or higher

- Prominent Logo
- Up to 6 organization representatives

Gold - $15,000

- Large Logo
- Up to 4 organization representatives

Silver – $10,000

- Medium Logo
- Up to 3 organization representatives

Bronze - $5,000

- Normal Logo
- Up to 2 organization representatives

Stainless Steel $1000

- 1 organization representative
- Acknowledgment

Vision

Our vision is a world class Innovation Engine for maritime transportation ecosystem cybersecurity education, research, experimentation, investment, and commercialization of products with regional and national impacts.

Key Points

- Addresses cybersecurity challenges presented by the maritime transportation ecosystem of ports, ships, shipping lines, cargo, people, inland waterways and intermodal transfers.
- Focuses on solutions presented by advances in technology to understand the independencies, vulnerabilities and risks to develop solutions.
- Catalyzes long term industry and economic growth backed by public-private collaboration and promotes investment in key cybersecurity technologies.
- Seeks to actively recruit and include partners from marginalized groups, including women and persons of color.
- Creates and encourages a culture of innovation.

Partners

University of SC Beaufort; Clemson University; South Coast Cyber Center; The Citadel; South Carolina State University; SC Research Authority; SC Ports Authority; Palmetto Tech Bridge/Naval Information Warfare Center, Atlantic; SC Council on Competitiveness; SCCyber; University of SC (Columbia); Technical College of the Lowcountry; Savannah River National Laboratory; American Bureau of Shipping; Fathom5 LLC; Alerion Capital; and Material Capital Ventures.

Background

The NSF Regional Innovation Engines program is a new initiative to fund integrated and comprehensive activities spanning use-inspired research, translation to practice, entrepreneurship and workforce development. The official name of USCB's award is "National Science Foundation South Coast Regional Innovation Engine: Cybersecurity Solutions for the Maritime Transportation Ecosystem."

The port and maritime transportation system in the U.S. represents 26% of the nation's economy. The US Coast Guard Cyber Strategy has stated: "A safe and secure maritime transportation system enhances America's competitiveness, advances trade, generates capital, grows our economy and strengthens our national security."

Initial Plans

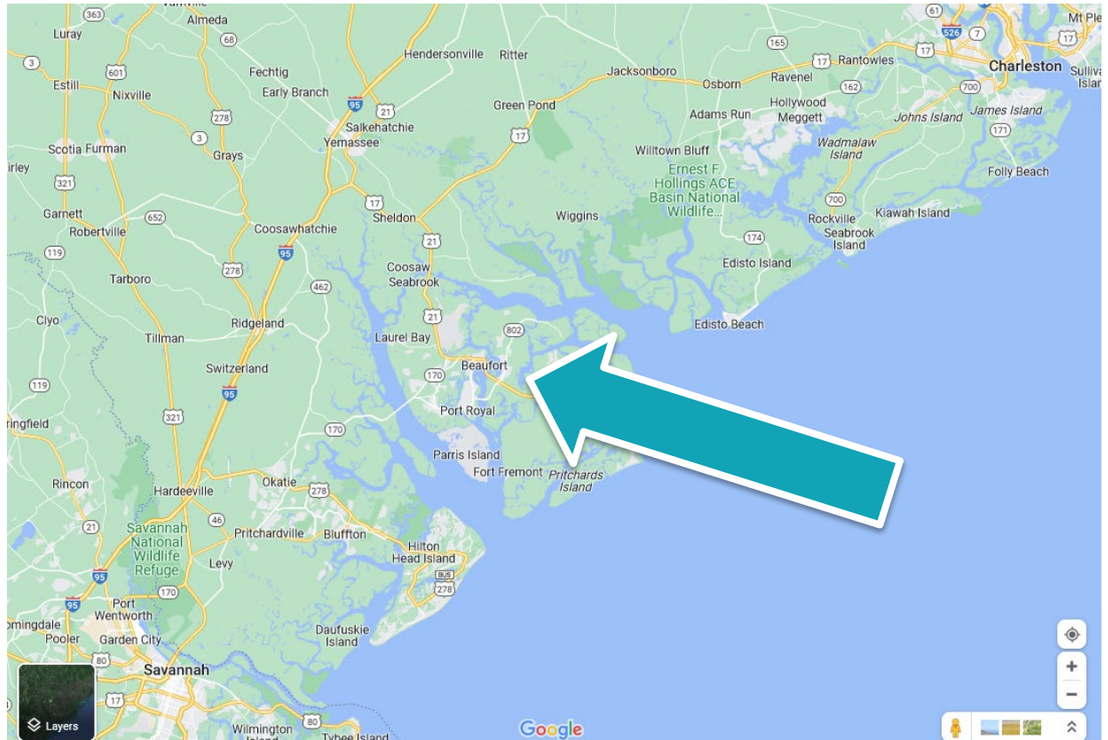
Development of a strategic plan; workshops focused on high risk areas and gaps within maritime cybersecurity with academia, government, and private sector participation; tabletop exercises; and data gathering.

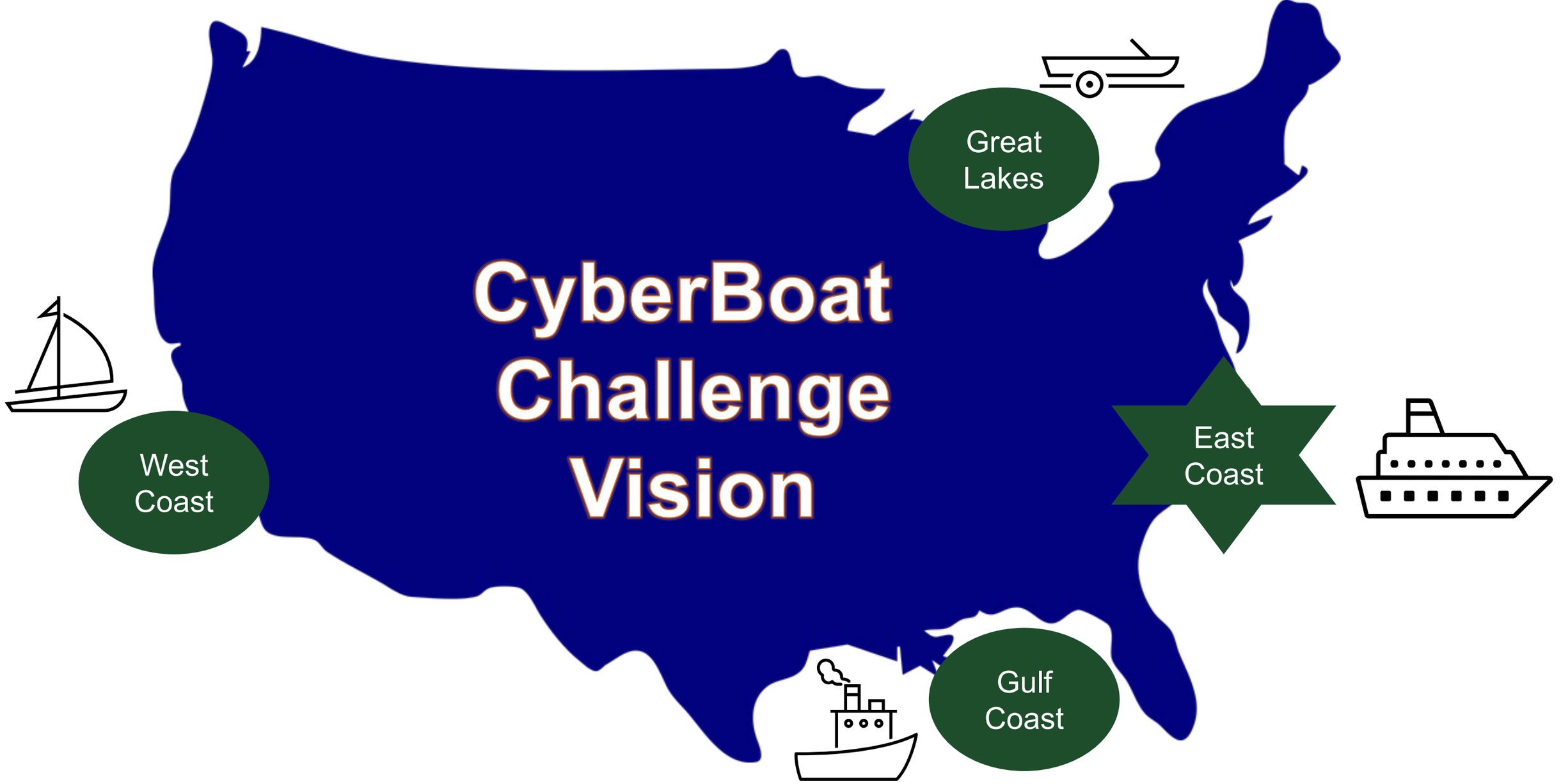
Contact

Rick Siebenaler, CEO
rasiebenaler@outlook.com
630-272-5500

Looking Forward

- University of South Carolina Beaufort will host the next CyberBoat Challenge at the South Coast Cyber Center
- CyberBoat Challenge will partner with the National Science Foundation Engine program in South Carolina
- Still need more industry support





Goal: Rotating regional events culminating with the CyberShip Challenge on a large vessel.

Save the Date:
Cyber Boat Challenge
September 25-29, 2024
Beaufort, South Carolina

www.cyberboatchallenge.net

Contacts:
Jeremy Daily, Jeremy.Daily@colostate.edu
Karl Heimer, karl.heimer@outlook.com

Host Venue for 2024 Beaufort, SC

Airports in Savannah, GA and Charleston, SC can serve Beaufort

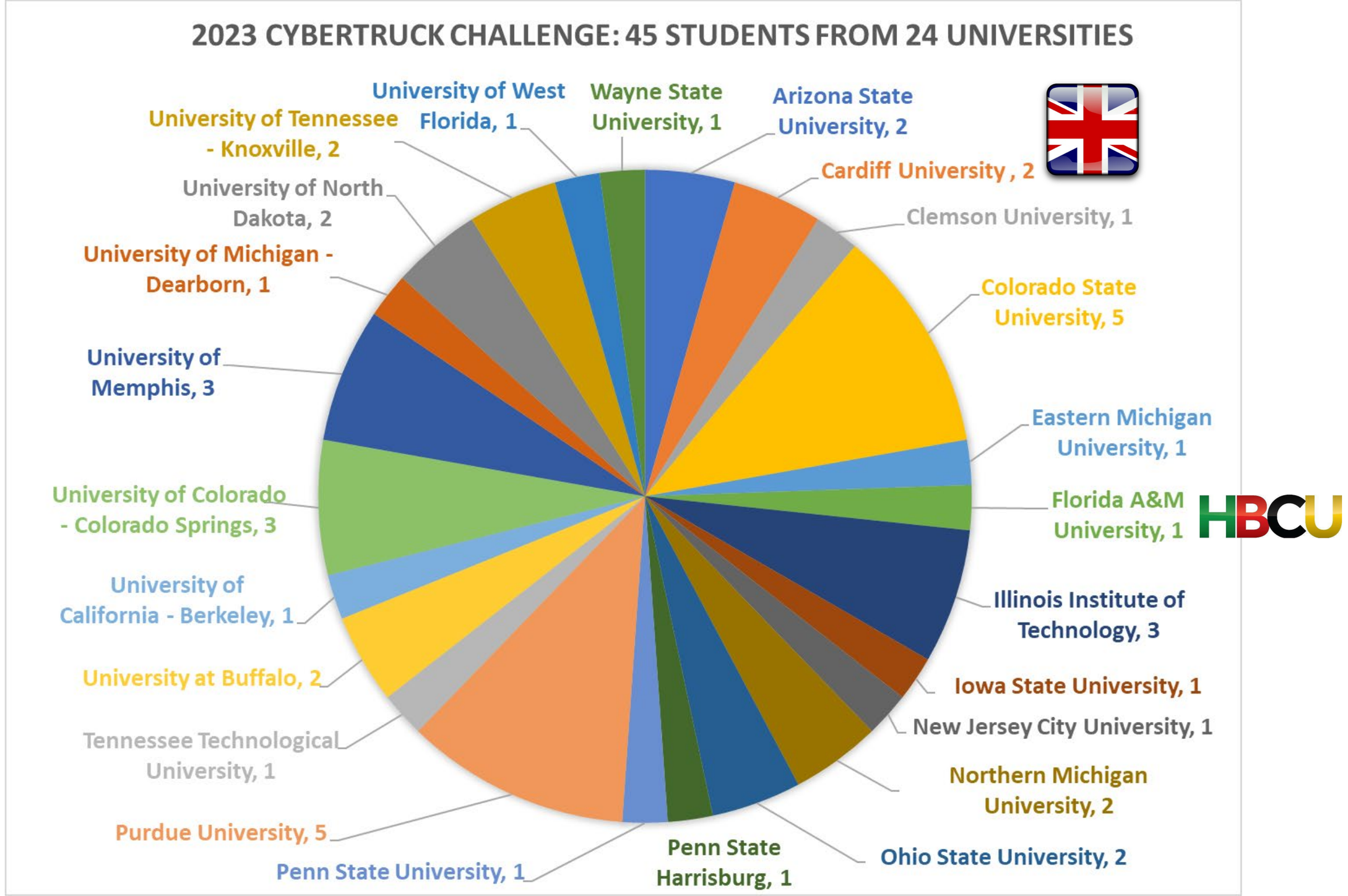
CyberBoat and CyberTruck Challenge Comparison

Sister Cyber Challenge Events demonstrate successes in other domains.

CyberTruck Challenge Class of 2023

Macomb Community College, Warren, MI

2023 CYBERTRUCK CHALLENGE: 45 STUDENTS FROM 24 UNIVERSITIES



CyberTruck Challenge 2023 Schedule

Version:20230516

	Sunday, 11 June	Monday, 12 June		Tuesday, 13 June		Wednesday, 14 June	Thursday, 15 June	Friday, 16 June	Time
		Group A	Group B	Group A	Group B				
Before 0700	Site Closed	Site Closed							Before 0700
0700-0730		Breakfast						Breakfast	0700-0730
0730-0800								Student Team Briefs (30 minutes each group)	0730-0800
0800-0830		Welcome // NDA		Wireless Systems	***Hardware Reverse Engineering***	Safety & Legal Briefing	Assessment		0800-0830
0830-0900		Vehicle Orientation				Assessment			0830-0900
0900-0930		***Software RE***	Truck Systems and J1939						0900-0930
0930-1000				Cryptography	***Binary Analysis and Modification***				0930-1000
1000-1030									1000-1030
1030-1100									1030-1100
1100-1130									1100-1130
1130-1200									1130-1200
1200-1230		Lunch						Awards	1200-1230
1230-1300						Lunch			1230-1300
1300-1330		***Binary Decompilation***	Diagnostic Systems	Lunch					1300-1330
1330-1400				***Hardware Reverse Engineering***	Wireless Systems	Assessment	Assessment	Site Closed	1330-1400
1400-1430									1400-1430
1430-1500									1430-1500
1500-1530		Truck Systems and J1939	***Software RE***						1500-1530
1530-1600									1530-1600
1600-1630									1600-1630
1630-1700					Cryptography				1630-1700
1700-1730				***Binary Analysis and Modification***					1700-1730
1730-1800		Diagnostic Systems	***Binary Decompilation***						1730-1800
1800-1830	Informal Welcome Reception (offsite)								1800-1830
1830-1900									1830-1900
1900-1930				Dinner		Dinner			1900-1930
1930-2000		Dinner		Dinner Presentation: Trucking Industry					1930-2000
2000-2030		Dinner Presentation: Dr. Bratus				Assessment	Free		2000-2030
2030-2100				Assessment Preparation					2030-2100
2100-2130	Site Closed	Free							2100-2130
2130-2200									2130-2200
After 2200		Site Closed							After 2200

Snacks will be served each afternoon. *Survey *Survey

Legend

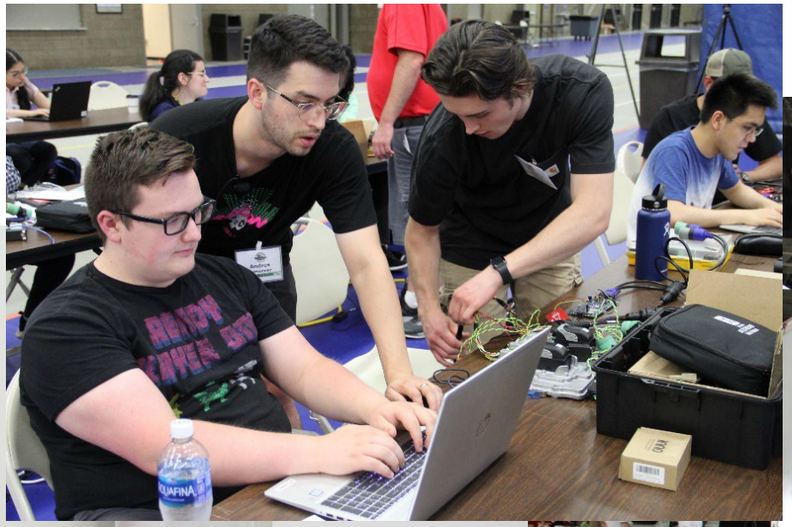
Lecture / Demo	All participants
Freightliner Side	Interactive lecture and activities
Cummins Side	Interactive lecture and activities
Meals	Meals will be catered on-site
"Hacking"	On vehicle assessments
Free	Can hack, study, rest, leave, etc.
Site Closed	No access the facility
Off Site	Limelight Grill on VanDyke Ave

Topic	Instructor, Affiliation	Verified
Welcome and Review	Karl Heimer [MEDC] & Sponsor Representatives	Yes
Wireless Systems	Daniel Salloum [Assured Information Security]	Yes
Binary Analysis and Modification	Edward Larson, Wyatt Ford [Red Balloon Security]	Yes
Binary Decompilation	Fish Wang [Arizona State University]	Yes
Software Reverse Engineering	Matt Carpenter, Erin Cornelius [GRIMM]	Yes
Truck Systems and J1939	Jeremy Daily [Colorado State University]	Yes
Hardware Reverse Engineering	Bill Hass [Self]	Yes
Cryptography	Ben Gardiner [NMFTA]	Yes
Diagnostic Systems	Sharika Kumar [Cummins, Inc]	Yes
Trucking Industry	Urban Jonson [Serjon]	Yes

Recall, the CyberBoat Challenge was 2.5 days.

Assessment Period:
Applying the hands-on lecture content

Assessment Period:
Students Explore with Mentors



Thank you to the CyberTruck Challenge® sponsors

See www.cybertruckchallenge.org for additional information.

Premier Sponsor

NMFTA
National Motor Freight Traffic Association, Inc.

Platinum Sponsors

Cummins

GEOTAB
management by measurement

Gold Sponsors

PACCAR

BOSCH

NAVISTAR®

Silver Sponsors

Allison Transmission

ORBITAL
Installation Technologies

DAIMLER

U.S. Department of Transportation
Federal Motor Carrier Safety Administration

Bronze Sponsors

Stoneridge

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Bendix

IOActive

Macomb Community College
Education • Enrichment • Economic Development
Discover. Connect. Advance.™

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Contributors

BATTELLE
It can be done

UNIVERSITY OF DETROIT MERCY
Build A Boundless Future

VOLVO

Warren Michigan, 12-16 June 2023.

The CyberBoat Challenge needs sponsorship.

J1939 Security Challenges

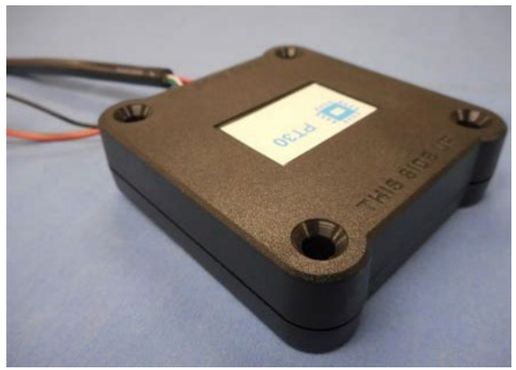
NMEA 2000 security depends on J1939 security.

Most hacks on truck have an analog in maritime.

Image credit: DALL-E

Mandatory Electronic Logging Devices (ELDs)

Security vulnerabilities affecting trucks on the road.



Mandated Technology

- The “ELD Mandate” requires truckers to connect to the engine and capture Hours of Service.
- The impact to vehicle cybersecurity was not discussed in the mandate.

DEPARTMENT OF TRANSPORTATION

Federal Motor Carrier Safety Administration

49 CFR Parts 385, 386, 390, and 395

[Docket No. FMCSA–2010–0167]

RIN 2126–AB20

Electronic Logging Devices and Hours of Service Supporting Documents

AGENCY: Federal Motor Carrier Safety Administration (FMCSA), DOT.

ACTION: Final rule.

SUMMARY: The Federal Motor Carrier Safety Administration (FMCSA) amends the Federal Motor Carrier Safety Regulations (FMCSRs) to establish: Minimum performance and design standards for hours-of-service (HOS) electronic logging devices (ELDs); requirements for the mandatory use of these devices by drivers currently required to prepare HOS records of duty status (RODS); requirements concerning HOS supporting documents; and measures to address concerns about harassment resulting from the mandatory use of ELDs. The requirements for ELDs will improve compliance with the HOS rules.

DATES: *Effective Date:* February 16, 2016.

Compliance Date: December 18, 2017.

DALL-E/Photoshop ELD shown

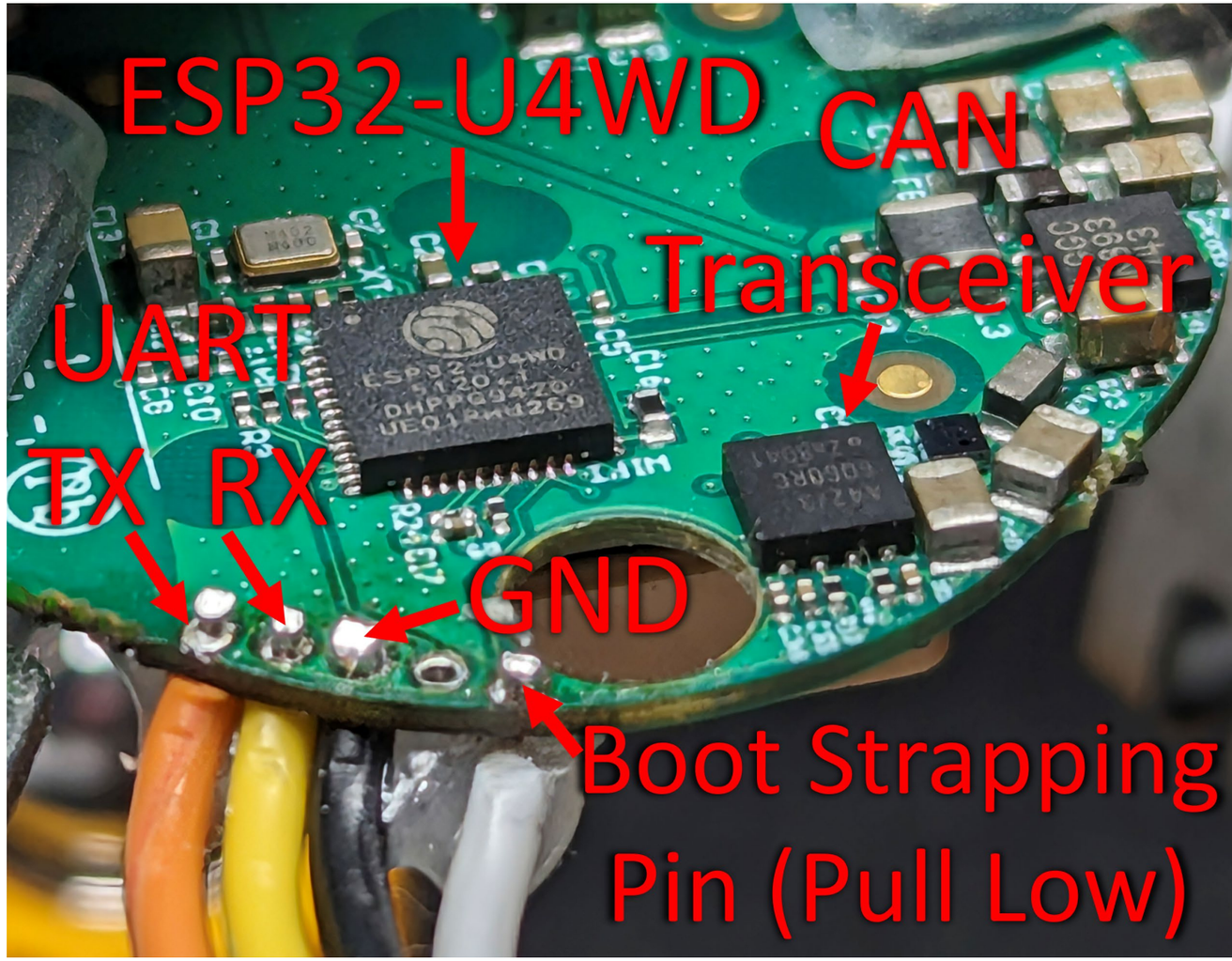
Emergent Behavior

- System Composed of Truck and ELD
  - Heavy truck: dynamic operational platform with mechanical and electronic components
  - ELD: electronic vehicle attachment mandated for data logging, regulatory compliance.
- Integration:
  - *Could* enhance operational capabilities
  - Widens attack surface / introduces new threat vectors
  - *Could* introduce potential vulnerabilities

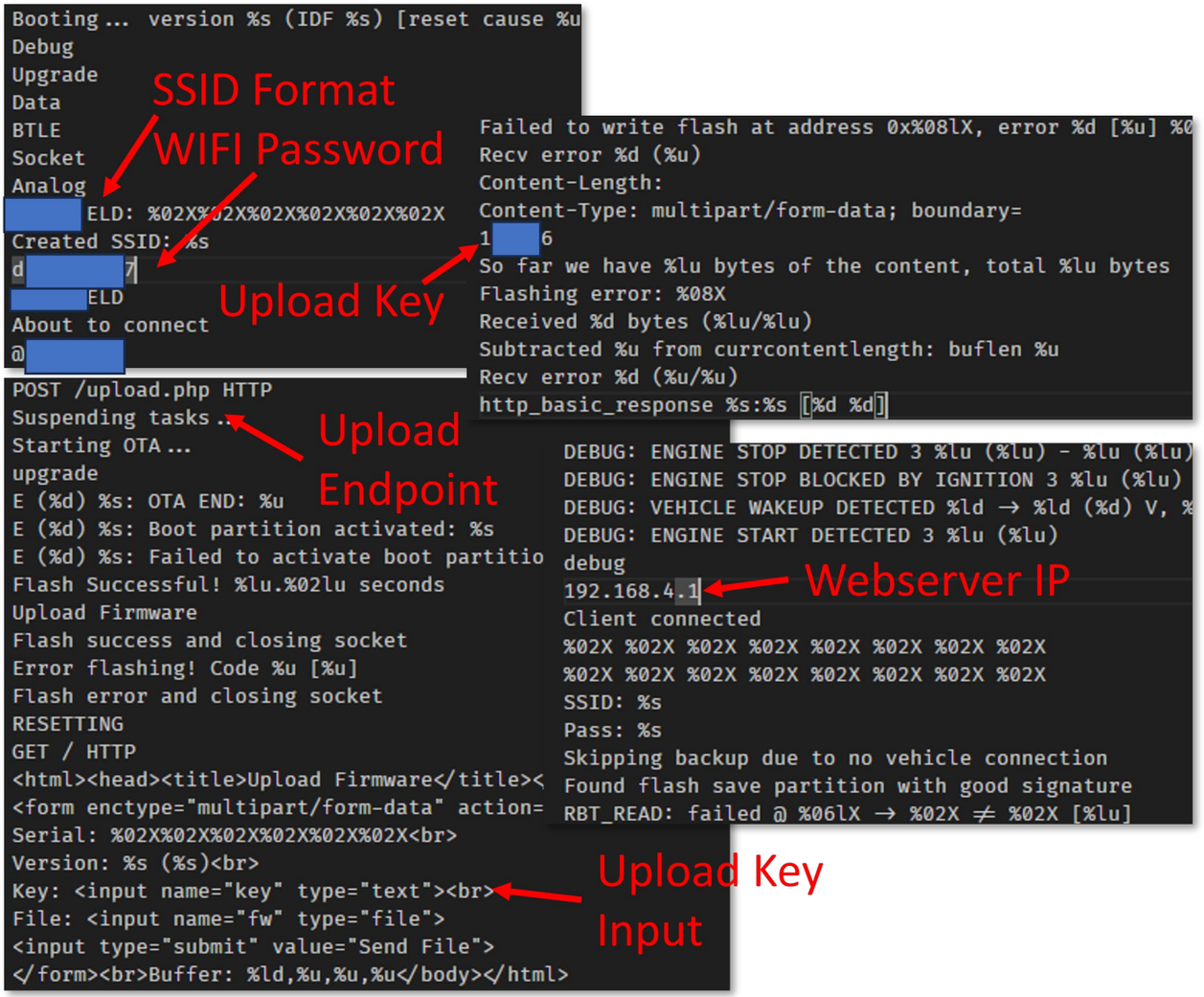
Maritime equivalent: remote bilge monitoring

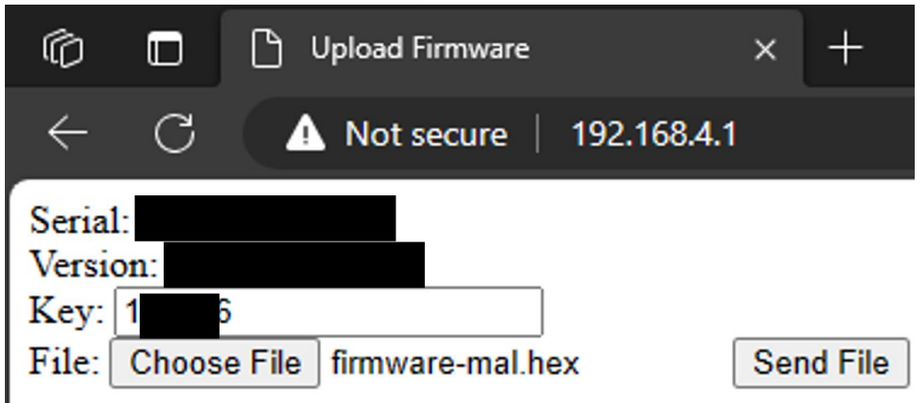
Device Analysis

- Acquired popular ELDs from popular Ecommerce site for analysis
  - All small, handheld devices
  - Connects to vehicles diagnostic port
- Quickly became apparent that multiple ELDs were clones with minimal changes
  - Same device sold by 50+ brands
  - Wireless networks not rebranded
  - Uncovered that this is commonplace in the ELD industry
- Manuals indicates:
  - Bluetooth Low Energy (BLE) and GPS connectivity
  - Companion app for data logging, monitoring, diagnostics, etc.
- Discovered password protected Wi-Fi network, not stated in manual



Technical Inspection





- Firmware Extraction & Acquisition:
  - Utilized ESPTool.py for firmware extraction via serial to USB on the ELD's programming port
  - Discovered credentials and endpoints using GNU strings command
  - Obtained newer firmware from update servers by reverse engineering mobile apps with JADX
- Employed Ghidra with ESP32 plugins for analysis
- Default Wi-Fi credentials easily accessible online
- Using default Wi-Fi credentials mapped Wi-Fi network using Nmap to identify open ports and associated services
  - Service on port 22
  - Telnet on port 23
  - HTTP server on port 80

Vulnerabilities

- Default Network Security Weaknesses:
  - Hardcoded weak password
  - Unnecessary simultaneous use of Wi-Fi & BLE
  - Simultaneous client and access point (Wormable)
- Web Server & OTA Updates:
  - Default-enabled web server, seemly unused by resellers
  - OTA update mechanism with a weak password
  - Firmware update not signed
  - Downgrade attack susceptible
- Debugging & APIs:
  - Unnecessary debug thread open on port 22
  - Unauthenticated Telnet API (port 23) and BLE exposing critical device control, including arbitrary CAN message handling and OTA updates, without security measures.
  - While API provides the ability to configure the device to a more secure state, we did not find it used by the re-seller applications we examined

```
43  ble_message = strncmp((char *)recvd_message[redacted]);
44  if (ble_message == 0) {
45    puVar7 = &command_handle_output;
46    bus = 0x6a4;
47    pcVar6 = "Dbg";
48    pcVar5 = dbg_thread;
49LAB_401162c6:
50    xTaskCreatePinnedToCore(pcVar5,pcVar6,bus,puVar7,5,0,1);
51    return (int *)0x1;
52  }
53                  [redacted] command might start a thread to stream back data */
54  ble_message = strncmp((char *)recvd_message,[redacted]);
55  cmd_parameter = baud_rate_1;
56  if (ble_message == 0) {
57    memw();
```

~ Code for other Commands ~

```
573                 /* if it doesn't equal any of the above commands then it goes to this routine
574     if (is_streaming == '\x01') {
575
576
577
578The streaming
579command, must
580be sent first
581
```

```
586       if ([redacted]) {
587                                                    );
588
589         if ([redacted]) {
590           if ([redacted]) {
591             if ([redacted]) {
592               if ([redacted]) {
593                 return recvd_message;
594               }
595               if (first_char != 6) {
```

~ Code for other CAN Bus Channels ~

```
679             debug_printf("CAN1: Requesting @%08lX %u bytes\r\n",id,length);
680             bus = 0;
681           }
682           send_can(bus,id,0,0,0,0,length,&can_data,0,0,100,&command_handle_output,0);
683           return (int *)0x64;
```

send_can sends the message to the CAN bus

Connecting to Trucks at a Truck Stop


CYBERTRUCK CHALLENGE
SYSTEMS ENGINEERING

Commercial Vehicle Electronic Logging Device Security: Unmasking the Risk of Truck-to-Truck Cyber Worms

Jake Jepson
Colorado State University
jepson2k@rams.colostate.edu

Rik Chatterjee
Colorado State University
rik.chatterjee@colostate.edu

Jeremy Daily
Colorado State University
jeremy.daily@colostate.edu

***Abstract*—In compliance with U.S. regulations, modern commercial trucks are required by law to be equipped with Electronic Logging Devices (ELDs), which have become potential cybersecurity threat vectors. Our research uncovers three critical vulnerabilities in commonly used ELDs.**

First, we demonstrate that these devices can be wirelessly controlled to send arbitrary Controller Area Network (CAN) messages, enabling unauthorized control over vehicle systems. The second vulnerability demonstrates malicious firmware can be uploaded to these ELDs, allowing attackers to manipulate data and vehicle operations arbitrarily. The final vulnerability, and perhaps the most concerning, is the potential for a self-propagating truck-to-truck worm, which takes advantage of the inherent networked nature of these devices. Such an attack could lead to widespread disruptions in commercial fleets, with severe safety and operational implications. For the purpose of demonstration, bench level testing systems were utilized. Additional testing was conducted on a 2014 Kenworth T270 Class 6 research truck with a connected vulnerable ELD.

These findings highlight an urgent need to improve the security posture in ELD systems. Following some existing best practices and adhering to known requirements can greatly improve the security of these systems. The process of discovering the vulnerabilities and exploiting them is explained in detail. Product designers, programmers, engineers, and consumers should use this information to raise awareness of these vulnerabilities and encourage the development of safer devices that connect to vehicular networks.

I. Introduction

According to the US Bureau of Transportation Statistics, the United States alone has over 14 million medium and heavy-duty trucks registered, underscoring their prevalence and importance in national infrastructure [1]. Moreover, the American Trucking Association's report highlighted these trucks moved approximately 72.6% of the nation's freight by weight in recent years, showcasing their critical role in the country's freight transportation system [2]. This statistic further emphasizes the reliance of economies on these vehicles, not only for domestic transport but also for international trade and commerce. The seamless operation of these commercial vehicles is vital for the smooth functioning of supply chains, directly impacting everything from local businesses to international markets.

A. Background on Electronic Logging Devices (ELDs)

Many heavy vehicles are required to be equipped with Electronic Logging Devices (ELDs), since they are mandated by the Federal Motor Carrier Safety Administration (FMCSA) under the ELD Final Rule [3]. This so-called ELD Mandate is a component of the Moving Ahead for Progress in the 21st Century Act (MAP-21) and it went into effect December 18, 2017. These devices are essential for recording driving hours and ensuring compliance with Hours of Service (HOS) regulations, which are designed to prevent accidents due to

Results

Coordinated Disclosure with Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security

Vendor has developed a patch to address the security issues

Best Paper Runner-Up at the VehicleSec '24 Symposium

Best Demo at the VehicleSec '24 Symposium, Feb 26, 2024

Viral News Coverage

Mandated technology without security requirements will likely lead to exploitable vulnerabilities.

Network and Distributed System Security (NDSS) Symposium 2024
26 February - 1 March 2024, San Diego, CA, USA
ISBN 1-891562-93-2
https://dx.doi.org/10.14722/vehiclesec.2024.23047
www.ndss-symposium.org

Responsible Disclosure

3.2.3 DOWNLOAD OF CODE WITHOUT INTEGRITY CHECK CWE-494

IO-1020 Micro ELD downloads source code or an executable from an adjacent location and executes the code wit sufficiently verifying the origin or integrity of the code.

CVE-2024-28878 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.6 has been calculated; the CV vector string is (AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-28878. A base score of 9.4 has been calculated; the CVSS v string is (CVSS4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

Commercial Vehicle Electronic Logging Device Security: Unmasking the Risk of Truck-to-Truck Cyber Worms (Long)

Jake Jepson, Rik Chatterjee, Jeremy Daily (Colorado State University)

ETAS Best Paper Award Runner-up!

In compliance with U.S. regulations, modern commercial trucks are required by law to be equipped with Electronic Logging Devices (ELDs), which have become potential cybersecurity threat vectors. Our research uncovers three critical vulnerabilities in commonly used ELDs.

First, we demonstrate that these devices can be wirelessly controlled to send arbitrary Controller Area Network (CAN) messages, enabling unauthorized control over vehicle systems. The second vulnerability demonstrates malicious firmware can be uploaded to these ELDs, allowing attackers to manipulate data and vehicle operations arbitrarily. The final vulnerability, and perhaps the most concerning, is the potential for a selfpropagating truck-to-truck worm, which takes advantage of the inherent networked nature of these devices. Such an attack could lead to widespread disruptions in commercial fleets, with severe safety and operational implications. For the purpose of demonstration, bench level testing systems were utilized. Additional testing was conducted on a 2014 Kenworth T270 Class 6 research truck with a connected vulnerable ELD.

These findings highlight an urgent need to improve the security posture in ELD systems. Following some existing best practices and adhering to

Researchers highlight potential cybersecurity threats to trucking industry, supply chain

19 Mar, 2024
By Josh Rhoten

SECURITY

73

Truck-to-truck worm could infect – and disrupt – entire US commercial fleet

The device that makes it possible is required in all American big rigs, and has poor security

Jessica Lyons

Fri 22 Mar 2024 // 00:03 UTC

Vulnerabilities in common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University.

In a paper presented at the 2024 Network and Distributed System Security Symposium, associate professor Jeremy Daily and systems engineering graduate students Jake Jepson and Rik Chatterjee demonstrated how ELDs can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware between vehicles.

News

'Truck-to-truck worms' introduced via ELDs could threaten major fleet disruption

Colorado State researchers call ELDs 'potential cybersecurity threat vectors'

Brinley Hineman • Friday, March 22, 2024

Truck-To-Truck Worm Could Infect Entire US Fleet (theregister.com)

Posted by **BeauHD** on Saturday March 23, 2024 @06:00AM from the poor-security dept.

23

Jessica Lyons reports via The Register:

> Vulnerabilities in common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University. In a paper presented at the 2024 Network and Distributed System Security Symposium, associate professor Jeremy Daily and systems engineering graduate students Jake Jepson and Rik Chatterjee demonstrated how ELDs can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware between vehicles. "These findings highlight an urgent need to improve the security posture in ELD systems," the trio wrote [PDF].
>
> The authors did not specify brands or models of ELDs that are vulnerable to the security flaws they highlight in the paper. But they do note there's not too much diversity of products on the market. While there are some 880 devices registered, "only a few tens of distinct ELD models" have hit the road in commercial trucks. A federal mandate requires most heavy-duty trucks to be equipped with ELDs, which track driving hours. These systems also log data on engine operation, vehicle movement and distances driven -- but they aren't required to have tested safety controls built in. And according to the researchers, they can be wirelessly manipulated by another car on the road to, for example, force a truck to pull over.
>
> The academics pointed out three vulnerabilities in ELDs. They used bench level testing systems for the demo, as well as additional testing on a moving 2014 Kenworth T270 Class 6 research truck equipped with a vulnerable ELD. [...] For one of the attacks, the boffins showed how anyone within wireless range could use the device's Wi-Fi and Bluetooth radios to send an arbitrary CAN message that could disrupt of some of the vehicle's systems. A second attack scenario, which also required the attacker to be within wireless range, involved connecting to the device and uploading malicious firmware to manipulate data and vehicle operations. Finally, in what the authors described as the "most concerning" scenario, they uploaded a truck-to-truck worm. The worm uses the compromised device's Wi-Fi capabilities to search for other vulnerable ELDs nearby. After finding the right ELDs, the worm uses default credentials to establish a connection, drops its malicious code on the next ELD, overwrites existing firmware, and then starts the process over again, scanning for additional devices. "Such an attack could lead to widespread disruptions in commercial fleets, with severe safety and operational implications," the researchers warned.

Malware targeting ELDs could allow hackers to take control of semi trucks, researchers say

This Week in Trucking

One of the top recognized fleets is looking for top notch drivers
SPONSORED CONTENT | March 18, 2024

Turkey strike causes semi crash, sends trucker to the hospital
TRUCKING NEWS | March 18, 2024

Shipping container falls off trailer, injuring two
TRUCKING NEWS | March 18, 2024

Missing trucker's big rig abandoned at Tennessee truck

FREIGHTWAVES

‘Truck-to-truck worms’ introduced via ELDs could threaten major fleet disruption

Brinley Hineman
Fri, Mar 22, 2024, 1:57 PM MDT • 2 min read

ALL INFOSEC NEWS

Truck-to-truck worm could infect – and disrupt – entire US commercial fleet

Copy link
Add to bookmarks

March 22, 2024, 12:03 a.m. | Jessica Lyons
The Register - Security www.theregister.com

The device that makes it possible is required in all American big rigs, and has poor security

Vulnerabilities in common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University....

AMERICAN BIG COLORADO COMMERCIAL DEVICE DEVICES DISRUPT FLEET INFECT LOGGING MEDIUM POOR SECURITY STATE UNIVERSITY VULNERABILITIES WORM

Visit resource

More from www.theregister.com / The Register - Security

Russia's Cozy Bear caught phishing German politicos with phony dinner invites
7 hours ago | www.theregister.com
BEAR CAMPAIGN CAUGHT COZY BEAR +10

Chinese snoops use F5, ConnectWise bugs to sell access to top US, UK networks
17 hours ago | www.theregister.com
ACCESS BEIJING BUGS CHINESE +20

3 million doors open to uninvited guests in keycard exploit
22 hours ago | www.theregister.com

Unmasking the Risk of Truck-to-

https://www.youtube.com/watch?v=SwtTzk9ys20

https://www.youtube.com/watch?v=SwtTzk9ys20

YouTube

Search

Sign in

Unmasking the Risk of Truck-to-Truck Cyber Worms

Walter Scott, Jr. College of Engineering
391 subscribers

Subscribe

9 Share Save

1K views 3 days ago #cybersecurity #hacking #coloradostate

The Cameraman Wasn't Prepared
Beach photos worth a thousand words
Sponsored · TheFunPost
Visit site

It's Been a Good Run, Drywall.
LRN2DIY
1.9M views • 2 weeks ago

This Is Why We Don't Toss Out Broken Microwaves | Remake...
Totally Handy
14M views • 1 year ago

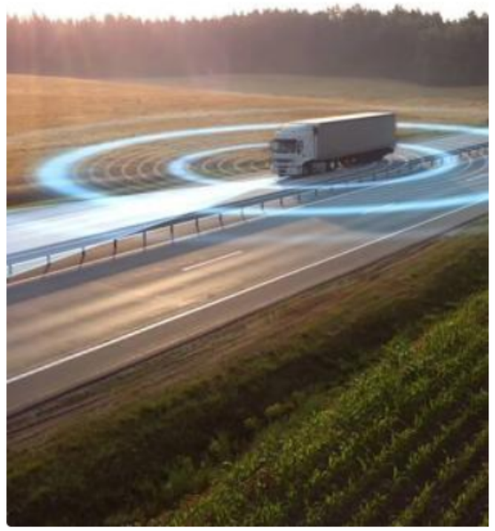
The Most MISUNDERSTOOD Feature On Your Drill
LRN2DIY
2.3M views • 1 month ago

When Did Raspberry Pi become the villain?
Jeff Geerling
1.1M views • 2 months ago

This Car Travels Farther Than You Push It
Tom Stanton
1.2M views • 7 days ago

Starship Reached Space. What Now?

Security News > 2024 > March > Truck-to-truck worm could infect - and disrupt - entire US commercial fleet



2024-03-22 00:03

While there are some 880 devices registered, "Only a few tens of distinct ELD models" have hit the road in commercial trucks.

They used bench level testing systems for the demo, as well as additional testing on a moving 2014 Kenworth T270 Class 6 research truck equipped with a vulnerable ELD. "In our evaluation of ELD units procured from various resellers, we discovered that they are distributed with factory default firmware settings that present considerable security risks," the authors noted.

The worm uses the compromised device's Wi-Fi capabilities to search for other vulnerable ELDs nearby.

After finding the right ELDs, the worm uses default credentials to establish a connection, drops its malicious code on the next ELD, overwrites existing firmware, and then starts the process over again, scanning for additional devices.

While both vehicles were in motion, in just 14 seconds the team connected to the truck's Wi-Fi, used the ELD's interface to re-flash the device, and started sending malicious messages causing the truck to slow down.

According to Jepson, the researchers disclosed the flaws to the ELD manufacturers and the US Cybersecurity and Infrastructure Security Agency before publishing the paper.

News URL

https://go.theregister.com/feed/www.theregister.com/2024/03/22/boffins_tucktotruck_worm/

#US #worm

Truck-to-truck worm could infect – and disrupt – entire US commercial fleet

Mar 21, 2024 at 09:12 PM CST

Vulnerabilities in common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University.

Home
Popular

TOPICS
Gaming
Sports
Business
Crypto
Television
Celebrity
See more

RESOURCES
About Reddit
Advertise
Help
Blog
Careers
Press

r/technology • 1 day ago
Loki-L

Truck-to-truck worm could infect – and disrupt – entire US commercial fleet

Security

theregister.com Open

487 69 Share

Related Technology

r/news
FDA approves Wegovy for lowering heart attack and stroke risk in overweight patients
2K upvotes · 350 comments

r/movies
What film would you LIKE to see a remake of?
73 upvotes · 474 comments

r/news
Navalny's mother says she has been shown his body
6.4K upvotes · 233 comments

r/videos
do you know who my dad is? [Almost Friday TV]
216 upvotes · 23 comments

The Register + Follow 7.3K Followers

Truck-to-truck worm could infect – and disrupt – entire US commercial fleet

Story by Jessica Lyons • 1d • 3 min read

Visit The Register
Flox rocks the Nix box by conquering code chaos
Russia's Cozy Bear caught phishing German politicos with...
Apple iPhone AI to be powered by Baidu in China, maybe

Truck-to-truck worm could infec
https://upstract.com/x/c3ce6cd77a9a0131

UPSTRACT

WIRE MENU

Truck-to-truck worm could infect – and disrupt

theregister.com/2024/03/22/boffins_tucktotruck_worm

Vulnerabilities in common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University. In a paper presented at the 2024 Network and Distributed System Security Symposium, associate professor Jeremy Daily and systems engineering graduate students Jake...

#JEREMYDAILY #JAKEJEPSON #RIKCHATTERJEE #ELD #PDF #880 #API #WIFISERVICE

This story appeared on theregister.com, 2024-03-22.

Truck-to-truck worm could infect, and disrupt, entire US commercial fleet

Discussion in 'Ask An Owner Operator' started by Tarh331_Dad, Thursday at 8:44 PM.

Thursday at 8:44 PM #1

Tarh331_Dad
Bobtail Member
47
54
Mar 29, 2020
0

Truck-to-truck worm could infect – and disrupt – entire US commercial fleet
https://www.theregister.com/2024/03/22/boffins_tucktotruck_worm/

Vulnerabilities in common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University.

In a paper presented at the 2024 Network and Distributed System Security Symposium, associate professor Jeremy Daily and systems engineering graduate students Jake Jepson and Rik Chatterjee demonstrated how ELDs can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware between vehicles.

"These findings highlight an urgent need to improve the security posture in ELD systems," the trio wrote...

Tarh331_Dad, Thursday at 8:44 PM #1

Flat Earth Trucker and fordconvert Thank this.

Skip to comments.

Truck-to-truck worm could infect – and disrupt – entire US commercial fleet

the register ^

Posted on **3/21/2024, 6:31:42 PM** by **algore**

Vulnerabilities in common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University.

In a paper presented at the 2024 Network and Distributed System Security Symposium, associate professor Jeremy Daily and systems engineering graduate students Jake Jepson and Rik Chatterjee demonstrated how ELDs can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware between vehicles.

"These findings highlight an urgent need to improve the security posture in ELD systems," the trio wrote [PDF].

The authors did not specify brands or models of ELDs that are vulnerable to the security flaws they highlight in the paper. But they do note there's not too much diversity of products on the market. While there are some 880 devices registered, "only a few tens of distinct ELD models" have hit the road in commercial trucks.

A federal mandate requires most heavy-duty trucks to be equipped with ELDs, which track driving hours. These systems also log data on engine operation, vehicle movement and distances driven – but they aren't required to have tested safety controls built in.

And according to the researchers, they can be wirelessly manipulated by another car on the road to, for example, force a truck to pull over.

The academics pointed out three vulnerabilities in ELDs. They used bench level testing systems for the demo, as well as additional testing on a moving 2014 Kenworth T270 Class 6 research truck equipped with a vulnerable ELD.

"In our evaluation of ELD units procured from various resellers, we discovered that they are distributed with factory default firmware settings that present considerable security risks," the authors noted.

This included an exposed API that permits over-the-air (OTA) updates. The devices also have Wi-Fi and Bluetooth enabled by default, with a "predictable" Bluetooth identifier and Wi-Fi Service Set Identifier (SSID) and weak default password. That makes it easy to connect to the device and then obtain network access to the rest of the vehicle's systems – at least for attackers within wireless range.

This can be achieved via a drive-by attack, or by hanging out at truck stops, rest stops, distribution centers, ports – basically anywhere that heavy-duty trucks tend to congregate.

The ELDs use a Controller Area Network (CAN) bus to communicate. For one of the attacks, the boffins showed how anyone within wireless range could use the device's Wi-Fi and Bluetooth radios to send an arbitrary CAN message that could disrupt of some of the vehicle's systems.

A second attack scenario, which also required the attacker to be within wireless range, involved connecting to the device and uploading malicious firmware to manipulate data and vehicle operations.

Finally, in what the authors described as the "most concerning" scenario, they uploaded a truck-to-truck worm. The worm uses the compromised device's Wi-Fi capabilities to search for other vulnerable ELDs nearby.

Here's how it knows the devices are vulnerable:

It specifically looks for devices with SSIDs starting with "VULNERABLE ELD:". Although this may sound contrived the SSID of the ELD we examined was predictable and could be used to identify the vulnerable devices.

https://www.youtube.com/watch?v=V-K2YouP5kI

Rolling Safely to Feed the Nation: The Cyber Frontline of Trucking Safety | A Conversation with C...

ITSPmagazine Podcast Network
3.9K subscribers
Subscribe

2 Share Save

14 views 4 days ago Redefining CyberSecurity Podcast | Together with executives, lines of business owners, and practitioners, we are Redefining CyberSecurity.

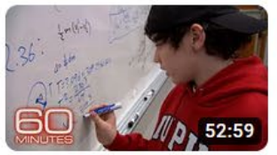
Unveiling the Art of Possible: A Glimpse into RSA Conference...
ITSPmagazine Podcast Network
6 views • 4 days ago
New

11 Of The Most Faked Foods In The World | Big Business |...
Business Insider
14M views • 6 months ago

Meet a 12-year-old hacker and cyber security expert
CBS Mornings
7.2M views • 5 years ago

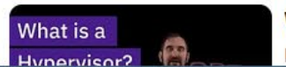
You've Never Seen A Wheelchair Like This
Mark Rober
11M views • 2 days ago
New

Only Five People Know The Secret To Making Zildjian's...
Business Insider
1M views • 3 months ago



Child prodigies and geniuses | 60 Minutes Full Episodes
60 Minutes
4.1M views • 4 months ago

How Hidden Technology Transformed Bowling
Veritasium
16M views • 2 years ago



What is a Hypervisor?
IBM Technology

Colorado State Researchers Warn Millions Of US Commercial Trucks May Have ELD Vulnerabilities

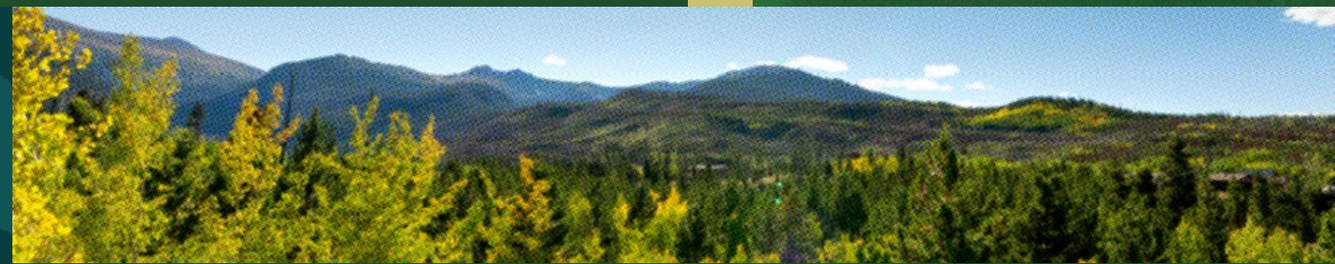
The Register (UK) (3/22) reported vulnerabilities in "common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University." In a paper presented "at the 2024 Network and Distributed System Security Symposium, associate professor Jeremy Daily and systems engineering graduate students Jake Jepson and Rik Chatterjee demonstrated how ELDs can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware between vehicles." The authors did not "specify brands or models of ELDs that are vulnerable to the security flaws they highlight in the paper." But they do "note there's not too much diversity of products on the market."

ASEE FIRST BELL WEEKEND EDITION
in affiliation with Bulletin MEDIA
Today's engineering and technology news prepared exclusively for the engineering and technology community

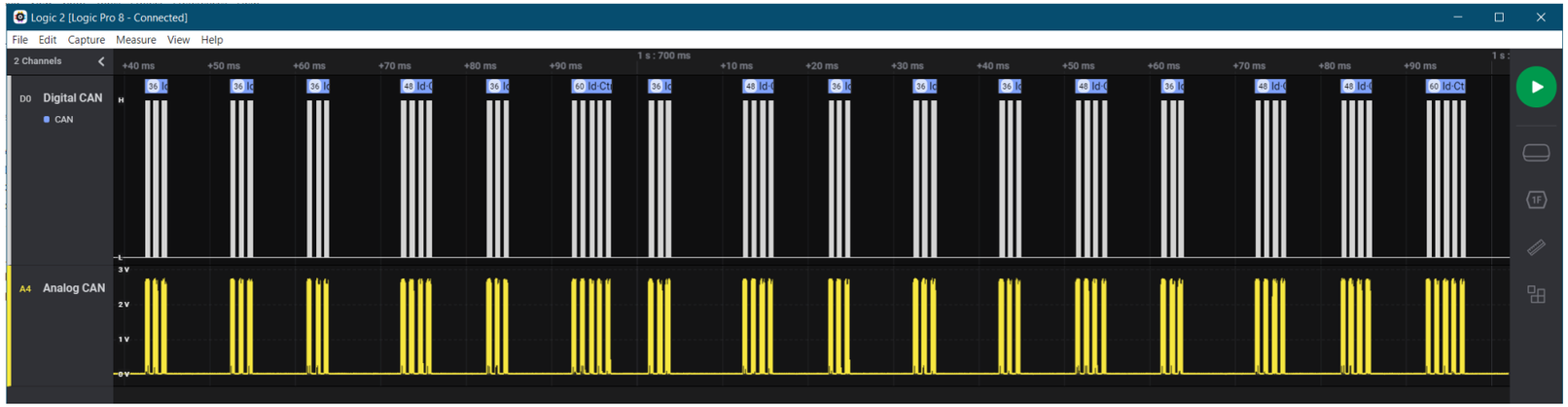
Good morning

March 30, 2024

Other J1939/NMEA2000 Vulnerabilities



Denial Of Service



Normal J1939

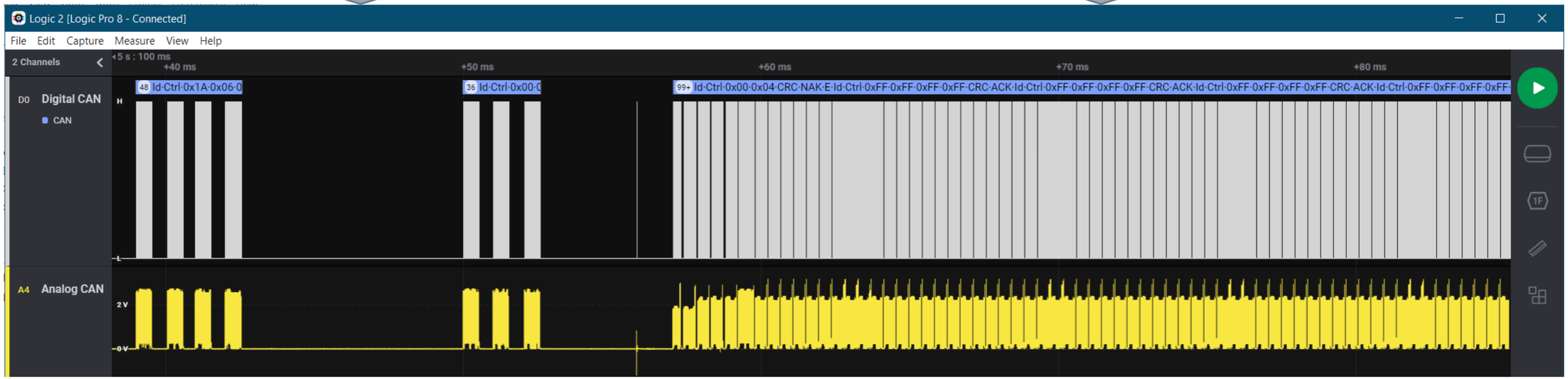
Flooded J1939

Spoofing Messages and Commands

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Normal J1939

Spoofed J1939



J1939 Address Claim

Each controller application (node) on the network should have its own source address.

Some ECUs have multiple controller applications.

- SA 0x00: Engine #1
- SA 0x0F: Engine Retarder

Address Claims happen

- On Boot
- When requested
- In response to other claims for the same address

Address Claim Parameter Group Number

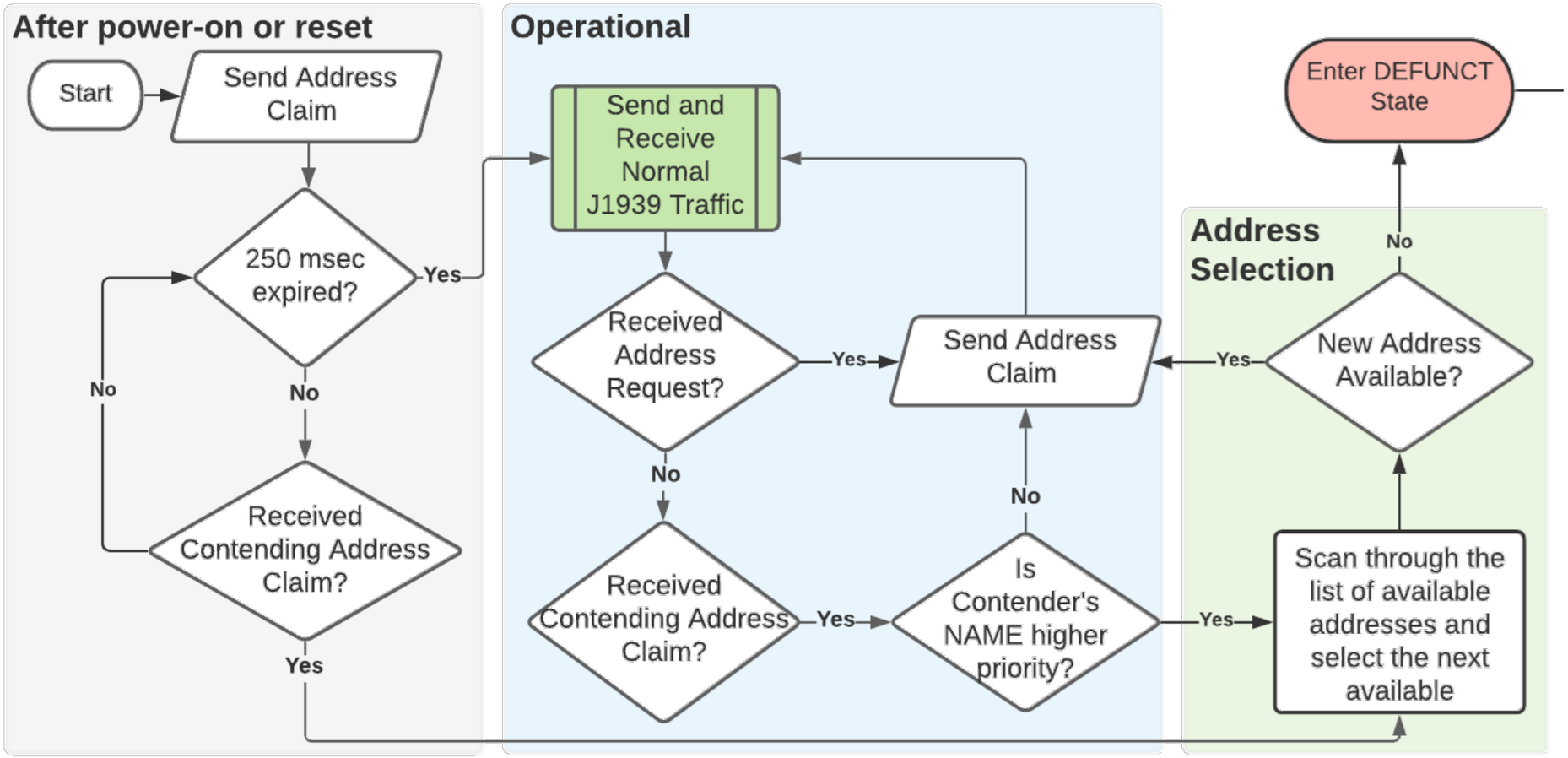
- 60928 (0xEE00)
- Mostly uses the Global destination address (0xFF)
- Source address is the address being claimed

Transmission Address Claim example:

`18EEFF03: 64 00 40 00 00 03 03 10`

- `18 – Priority 6 (default)`
- `EE – PGN 60928 = Address Claimed`
- `FF – Global Destination Address`
- `03 – Source address for Transmission #1`
- `64 00 40 00 00 03 03 10 - NAME Field`

How Address Claiming Works



See SAE J1939-81 Network Management

Address NAME Field

Arbitrary Address Capable	Industry Group	Vehicle System Instance	Vehicle System	Reserved	Function	Function Instance	ECU Instance	Manufacturer Code	Identity Number
	SAE		SAE	SAE	SAE			SAE	
1 bit	3 bits	4 bits	7 bits	1 bit	8 bits	5 bits	3 bits	11 bits	21 bits

- From SAE J1939-81, the following NAME field is 64 Bits (8 bytes) long.
- Value is translated with little endian format (Intel), so the least significant byte is first.
- Example 1: Caterpillar C15 with ADEM4 ECU

```
can1  18EEFF00   [8]  D0 6B 01 01 00 00 00 80
```

- Example 2: Detroit Diesel CPC3Evo

```
can1  18EEFF00   [8]  00 00 C0 01 00 00 00 00
```

- Additional Examples

CAN ID has:
- Priority = 6,
- Parameter Group Number = 0xEE00,
- Destination Address = 0xFF (Global),
- Claimed Source Address = 0x00 (Engine #1)

Example: Caterpillar Engine Controller

```
can1  18EEFF00   [8]  D0 6B 01 01 00 00 00 80
```

Byte 8 (0x80) = 0b1000 0000, which means:
- it is arbitrary address capable,
- the industry group is 0 (global), and
- the vehicle system instance is zero.

Byte 5 -7 (00 00 00), which means:
- the vehicle system, function, and function instance are all zero, which is consistent with an engine controller

Byte 4 (0x01), Bits 1-8 = MSB of Mfg Code
Byte 3 (0x01), Bits 8-6 = LSB of Mfg Code
- 0b0000 0001 0000 0001 = 0b1000 = 8 (dec)

Byte 3 (0x01), bits 1-5 = MSB of Identity Field
Byte 2 (0x6B) = 2nd byte of identity field
Byte 1 (0xD0) = LSB of identity field
- 0b0 0001 0110 1011 1101 0000 = 93,136 (dec)

Manufacturer ID Codes (Table B10)

The list of all Manufacturer Identifier code assignments.

Return To Documentation Tab

R	Mfr ID	Manufacturer
	0	Reserved
	1	Bendix Commercial Vehicle Systems LLC (formerly Allied Signal Inc.)
	2	Allison Transmission, Inc.
	3	Ametek, US Gauge Division
	4	Ametek-Dixson
	5	AMP Inc.
	6	Berifors Electronics AB
	7	Case Corp.
	8	Caterpillar Inc.
	9	Chrysler Corp.
	10	Cummins Inc (formerly Cummins Engine Co)
	11	Dearborn Group Inc.
	12	Deere & Company, Precision Farming
	13	Delco Electronics
	14	Detroit Diesel Corporation
	15	DICKEY-john Corporation
	16	Eaton Corp

Example: Ski Boat Navigation

```
can1  18EEFF1C [8] 02 04 45 0E 00 00 00 42
```

Byte 8 (0x42) = 0b0100 0010, which means:
- it is NOT arbitrary address capable,
- the industry group is 4 (marine), and
- the vehicle system instance is 2.

Byte 7 (0x00), the vehicle system is non-specific

Byte 6 (0x00), function is non-specific

Byte 5 (0x00), the function and ECU instance is zero, which means it's the first instance.

Byte 4 (0x0E), Bits 1-8 = MSB of Mfg Code
Byte 3 (0x45), Bits 8-6 = LSB of Mfg Code
- 0b0000 1110 0100 0101 = 0b111001 = 114 (dec)

Bytes 3-1 (0x050402) comprise the identity field

Econtrols owns Perfect Pass and Zero Off, the systems for cruise control on ski boats.

Manufacturer ID Codes (Table B10)

The list of all Manufacturer Identifier code assignments.

Return To Documentation Tab

Revised	Mfr ID	Manufacturer	Location
	112	MECALAC	Annecy le Vieux, France
	113	Stress-Tek, Inc.	Kent, WA USA
	114	EControls, Inc.	San Antonio, TX USA
	115	NACCO Materials Handling Group, Inc.	Portland, OR USA
	116	BEELINE Technologies	Brisbane, QLD Australia
	117	HUSCO International	Waukesha, WI USA
	118	Intron GmbH	Schwaebisch Hall, Germany
	119	IntegriNautics	Menlo Park, CA USA
	120	RDS Technology Ltd	Minchinhampton, Stroud UK

Address Claim Attack

Idea: Claim someone else's address with a higher priority address (All Zeros).

Keep claiming addresses as they are dynamically claimed.

If a system can't find a claimable address, then it should stop broadcasting (Denial of Service)

The following example shows how to conduct an address claim attack:

https://github.com/SystemsCyber/CyberTruckResources/blob/master/05_J1939/06%20J1939%20Address%20Claim.ipynb

- Note: This runs on Linux Socket CAN
- Try it on any J1939 network

Run these commands in Ubuntu:

```
git clone https://github.com/SystemsCyber/CyberTruckResources.git
conda activate base
jupyter notebook
```

Additional Security Vulnerabilities Specific to J1939 Networks

https://www.ndss-symposium.org/wp-content/uploads/2023/02/vehiclesec2023-23053-paper.pdf

Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks

Rik Chatterjee
Colorado State University
rik.chatterjee@colostate.edu

Subhojeet Mukherjee
Colorado State University
subhojeet.mukherjee@colostate.edu

Jeremy Daily
Colorado State University
jeremy.daily@colostate.edu

***Abstract*—Modern vehicles are equipped with embedded computers that utilize standard protocols for internal communication. The SAE J1939 protocols running on top of the Controller Area Network (CAN) protocol is the primary choice of internal communication for embedded computers in medium and heavy-duty vehicles. This paper presents five different cases in which potential shortcomings of the SAE J1939 standards are exploited to launch attacks on in-vehicle computers that constitute SAE J1939 networks.**

In the first two of these scenarios, we validate the previously proposed attack hypothesis on more comprehensive testing setups. In the later three of these scenarios, we present newer attack vectors that can be executed on bench test setups and deployed SAE J1939 networks.

For the purpose of demonstration, we use bench-level test systems with real electronic control units connected to a CAN bus. Additional testing was conducted on a 2014 Kenworth T270 Class 6 truck under both stationary and driving conditions. Test results show how protocol attacks can target specific ECUs. These attacks should be considered by engineers and programmers implementing the J1939 protocol stack in their communications subsystem.

I. Introduction

Medium and heavy-duty (MHD) vehicles are a part of the US critical infrastructure, transporting goods, supporting emergency services, and so on. Modern MHD vehicles are electronified: most mechanical operations being controlled through embedded computers referred to as Electronic Control Units (ECUs). Within the vehicle, ECUs form networks to communicate mission critical information with each other on a bus topology. For MHD vehicles, the primary choice of communication specifications within these networks is the SAE J1939 standard. SAE J1939 documents [1] are organized in layers much like the ISO/OSI [2] standards for traditional IT networking. At its lowest layers, the SAE J1939 standards utilize the Controller Area Network (CAN) specifications [3] to facilitate the in-vehicle information exchange.

CAN is used widely in automotive networking and aspects of its (in)security has be thoroughly demonstrated. For example, it has been shown, with access to remote and local entry points (vulnerable ECUs) to the CAN network, one can launch attacks on the vehicle to control or disrupt its operations. MHD vehicles also expose similar entry points [4] and, aside from CAN specific attacks, it has been shown that attacks can also be launched on the SAE J1939 protocols. Even so, the number of demonstrated attacks is still limited: Burakova et al. [5] have demonstrated a couple of attacks on the application layer specification of the SAE J1939 standards, Murvay et al. [6] have focused on weaknesses at the network management layer, and Mukherjee et al. [7] have targeted specific protocols at the data-link layer of the specifications.

While the application and network management layers are critical to the cyber-physical operations of the vehicle, important message transportation specifications are made in the data-link layer standards. As such, in this work we demonstrate newer attacks at the data-link layer of the SAE J1939 specifications that broaden the horizon of cyber threats already created by Mukherjee et al. [7]. Moreover, we validate two attacks that Mukherjee et al. demonstrated to work on laboratory test benches. For our validations we use more comprehensive testing setups, as well as a 2014 Kenworth T270 truck; the goal being to demonstrate the applicability and impact of the attacks on different platforms.

The overarching goal of this paper is to enhance the threatscape for in-vehicle networking applications in MHD vehicles. To that end, the rest of the paper is organized as follows. In section II we present a brief overview of SAE J1939, as required to clearly comprehend the contributions made in this paper. In section III we briefly cover the related work in this area. In section IV, we present a description of the testing setup used in this work. In section V, we describe the attack experimentation carried out during the course of the work. Finally, in section VI, we finish with concluding remarks and a brief introspection of the future work.

II. Background on SAE J1939

In-vehicle communication in medium and heavy-duty vehicles is mostly guided by the SAE J1939 standards. SAE J1939 messages carry operational parameters like engine speed, vehicle speed, switch status, etc. These parameters are bundled into logical groups referred to as Parameter Groups (PG). Each PG is identified by a unique number called a Parameter Group Number (PGN), which is also embedded in the message. Information in the J1939 message is carried in a J1939

Symposium on Vehicle Security and Privacy (VehicleSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-88-6
https://dx.doi.org/10.14722/vehiclesec.2023.23053
www.ndss-symposium.org

Memory Leak

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

- Request Overload → Depletion of traffic from target ECU
- Connection Exhaustion → Denial of connections to target ECU
- BAM Block → Blocking Multi-packet Broadcast Messages
- Malicious CTS → Stopping all Multi-packet communication
- Memory Leak → Reading inaccessible memory on target ECU

Colorado State University

Hypothesis

- **Specification**
  - A CTS message should contain information indicating the number of data packets that can be sent over the transport protocol
- **Attack**
  - An attack can be constructed by sending a crafted CTS message with the value of the number of packets that can be sent larger value indicated by the RTS
- **Expected Result**
  - Get back data that is not supposed to be returned in multipacket transfer

Results Showing Leaked Data

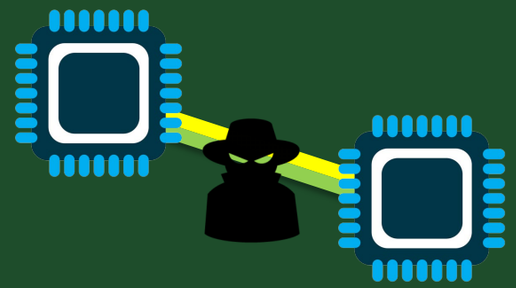

```
(1676937902.724769) can0 18EA00F9#E3FE00
(1676937902.752096) can0 18ECF900#101C0004FFE3FE00
(1676937902.778444) can0 18EC00F9#11FF06FFFFE3FE00
(1676937902.781839) can0 18EBF900#06FFFEFFFEFF01FF
(1676937902.797785) can0 18EBF900#0700000000000C00
(1676937902.811699) can0 18EBF900#08101DB003200000
(1676937902.826740) can0 18EBF900#0908F50000000000
(1676937902.841840) can0 18EBF900#0A00002A00020005
(1676937902.857193) can0 18EBF900#0B00040019000500
(1676937902.871749) can0 18EBF900#0C11000100020000
.................................................
.................................................
.................................................
(1676937906.361211) can0 18EBF900#F500000000000000
(1676937906.376190) can0 18EBF900#F600000000400000
(1676937906.391672) can0 18EBF900#F700000000000000
(1676937906.405979) can0 18EBF900#F8F4000000000000
(1676937906.421100) can0 18EBF900#F9FFFFFFF6000000
(1676937906.436086) can0 18EBF900#FA00000000000000
(1676937906.451279) can0 18EBF900#FB00000000000000
(1676937906.465952) can0 18EBF900#FC00006000000000
(1676937906.481005) can0 18EBF900#FD00000000002800
(1676937906.497411) can0 18EBF900#FE00000000000000
(1676937906.511018) can0 18EBF900#FF00800000000000
(1676937906.525783) can0 18EBF900#0000000000550000
(1676937906.540914) can0 18EBF900#01E015B380528F40
(1676937906.555834) can0 18EBF900#021FD3002DE0C044
(1676937906.570969) can0 18EBF900#03CD8052FFFFA404
(1676937906.585742) can0 18EBF900#04C058FAFFFFFFFF
```

Colorado State University

The CyberBoat Challenge ran in May 2022

The CyberTruck Challenge gives an aspirational example

J1939 Vulnerabilities exist on NMEA 2000 networks



www.cyberboatchallenge.net
www.cybertruckchallenge.org

Contact:
Jeremy Daily, Jeremy.Daily@colostate.edu

https://www.engr.colostate.edu/~jdaily/