Welcome to Auto-ISAC!

Monthly Virtual Community Call

February 2, 2022

This Session will be recorded.

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

DHS Traffic Light Protocol (TLP) Chart

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

From: https://www.us-cert.gov/tlp

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** ▪ **Victor Murray, *Manager, Cyber-Physical Systems Security, SWRI***
11:45	**Around the Room** ➢ Sharing Around the Virtual Room
11:55	**Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: **TLP:GREEN -** May be shared within the Auto-ISAC Community and "off the record"

How to Connect: For further info, questions or to add other POCs to the invite, please contact us! (sharmilakhadka@automotiveisac.com)

Engaging in the Auto-ISAC Community

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *"Cybersecurity is everyone's responsibility!"*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

22 *OEM Members*

21 *Navigator Partners*

❖ Share – *"If you see something, say something!"*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

42 *Supplier & Commercial Vehicle Members*

15 *Innovator Partners*

Membership represents **99%** *of cars and trucks on the road in North America*

Coordination with **26** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

2022 - 2023 Board of Directors

Executive Committee (ExCom)

Josh Davis
Chair *of the*
Board of the Directors
Toyota

Kevin Tierney
Vice Chair *of the*
Board of the Directors
GM

Jenny Gilger
Secretary *of the*
Board of the Directors
Honda

Tim Geiger
Treasurer *of the*
Board of the Directors
Ford

Todd Lawless
Chair *of the*
Advisory Board
Continental

2022-2023 Advisory Board (AB) Leadership

Todd Lawless
Chair *of the*
Advisory Board
Continental

Bob Kaster
Vice Chair *of the*
Advisory Board
Bosch

Allen Houck
Chair *of the SAG*
NXP

Larry Hilkene
Chair *of the CAG*
Cummins

Member Roster

as of February 2022

64 Members, 2 in Progress

Aisin	Hyundai	Oshkosh Corp
Allison Transmission	Infineon	PACCAR
Aptiv	Intel	Panasonic
Argo AI, LLC	John Deere Electronic	Polaris
AT&T	Kia	Qualcomm
Blackberry Limited	Knorr Bremse	Renesas Electronics
AVL	Lear	Stellantis
BMW Group	LGE	Subaru
BorgWarner	Luminar	Sumitomo Electric
Bosch (Escrypt-Affiliate)	Magna	Tokai Rika
Continental (Argus-Affiliate)	MARELLI	Toyota
Cummins	Mazda	TuSimple
Denso	Mercedes-Benz	Valeo
Faurecia	Meritor	Veoneer
Ford	Mitsubishi Motors	Volkswagen
Garrett	Mitsubishi Electric	Volvo Cars
General Motors (Cruise-Affiliate)	Mobis	Volvo Group
Geotab	Motional	Waymo
Google	Navistar	Yamaha Motors
Harman	Nexteer Automotive Corp	ZF
Hitachi	Nissan	
Honda	NXP	

Upcoming Events

- **Community Call:**
  - **Wednesday, March 2 - Speaker: Tamara Shoemaker**, Auto-ISAC **Title: *Become A CyberPatriot Youth Mentor: Validate your Leadership Skils*** **Time:** *11 – 12:00 p.m.* **TLP:WHITE**

- **Announcements:**
  - **Call for Community Call Speakers:** Might you want to speak on the topics related to Automotive and Cybersecurity? Please send your ideas to Sharmila Khadka.

Auto-ISAC Intelligence

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Intelligence

- Know what we track daily by subscribing to the DRIVEN
  - Send feedback, contributions or questions to analyst@automotiveisac.com
- Expect the Auto-ISAC 2021 Annual Report and Threat Assessment this quarter.
- Intelligence Notes
  - Cybersecurity teams should continue to monitor Russia-Ukraine developments until at least the end of February, when Russian military drills are expected to end (Reuters).
    - The key threat is Russia-Ukraine tensions could yield cyberattacks that spill outside the region and cause impacts to environments worldwide. If attacks occur, they are likely to be perpetrated by agitators or Russian government-deniable proxies (CISA, NCSC).
  - Given the current threat environment, review some of the significant vulnerabilities or vulnerable products that were reported in the past year (the list is not all-inclusive):
    - Log4Shell, BadAlloc, Microsoft Exchange, Pulse Secure, Kaseya, Codecov, Trojan Source
    - CISA Known Exploited Vulnerabilities Catalog

CISA RESOURCE HIGHLIGHTS

TLP: WHITE – CISA Industrial Control Systems Working Group (ICSJWG) Upcoming Events

- **Webinar – Wednesday February 16, 2022 – Internet of Things Embedded Security Guidance**
- **ICSJWG Spring 2022 – Virtual Event – Tuesday and Wednesday April 26-27, 2022**
- **Save-the-date and registration links at:**
  - https://www[.]cisa[.]gov/uscert/ics/icsjwg-meetings-and-webinars
  - https://www[.]cisa[.]gov/uscert/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG
- **Contact ICSJWG at ICSJWG.Communications@cisa.dhs.gov**

TLP: WHITE – Forty (40) Known Exploited Vulnerabilities added in JAN 2022

- **The following CISA Current Activities highlight added KEVs:**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/01/28/cisa-adds-eight-known-exploited-vulnerabilities-catalog
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/01/21/cisa-adds-four-known-exploited-vulnerabilities-catalog
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/01/18/cisa-adds-13-known-exploited-vulnerabilities-catalog
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/01/10/cisa-adds-15-known-exploited-vulnerabilities-catalog
- **KEV Catalog:**
  - https://www[.]cisa[.]gov/known-exploited-vulnerabilities-catalog

TLP: WHITE – CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats

- **Published in response to malicious cyber incidents in Ukraine**
- **Provides a checklist and CISA resources with measures to address intrusion prevention, detection, and response**
- **See:**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/01/18/cisa-urges-organizations-implement-immediate-cybersecurity
  - https://www[.]cisa[.]gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf

TLP: WHITE – Additional Resources From CISA

- CISA Homepage - https://www[.]cisa[.]gov/
- CISA NCAS – https://us-cert[.]cisa[.]gov/
- CISA News Room - https://www[.]cisa[.]gov/cisa/newsroom
- CISA Blog - https://www[.]cisa[.]gov/blog-list
- CISA Publications Library - https://www[.]cisa[.]gov/publications-library
- CISA Cyber Resource Hub - https://www[.]cisa[.]gov/cyber-resource-hub
- CISA Cybersecurity Directives - https://cyber[.]dhs[.]gov/directives/
- CISA COVID-19 Response – https://www[.]cisa[.]gov/coronavirus
- CISA Webinar Series on YouTube: https://www[.]youtube[.]com/playlist?list=PL-BF3N9rHBLJN3HUIZnTnyZHex9gPk_Yy

For more information:

cisa.gov

Questions?

CISAServiceDesk@cisa.dhs.gov

1-888-282-0870

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Auto-ISAC Community Meeting

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

30+
Featured Speakers to date

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 ***Best Practice Guides available on website***

2000+
Community Participants

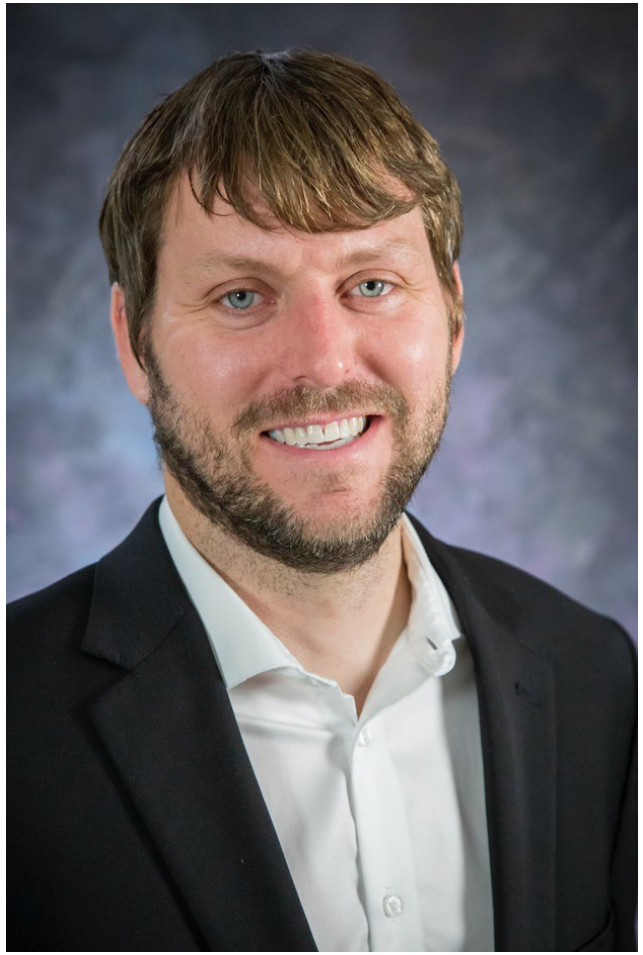
Featured Speaker

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Victor Murray- SwRI

Manager- Cyber-Physical Systems



Victor Murray is Manager of the Cyber-Physical Systems Security Section at Southwest Research Institute (SwRI).

He is a Certified Information Systems Security Professional (CISSP) whose background includes performing risks assessments, penetration tests, and developing secure systems.

Victor Murray, CISSP[1]
Courtney Westrick[2], Jonathan Wolford[1], and Ryan Elder[1]
[1]Southwest Research Institute, San Antonio, TX
[2]Ground Vehicle Systems Center (GVSC), Warren, MI

Research Into Defending Automobiles Via Intrusion Detection Systems (IDS)

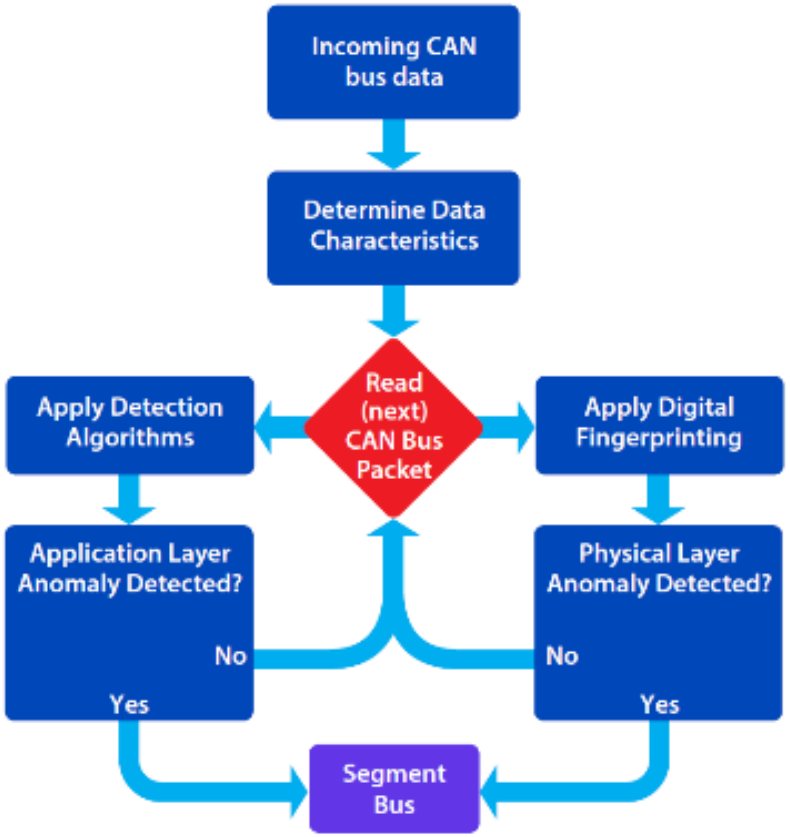
GVSC funded most work detailed in this presentation.

Agenda

- **Why Are We Talking About This?**
  - CAN Bus has no security features
  - Remote technologies have increased this risk of exploitable vulnerabilities
- **How can security be improved?**
  - Intrusion Detection Systems
  - Encryption, Hashing
  - Bus Segmentation, Gateways
  - Automotive Ethernet
- Discuss our Solution
  - How Does it Work?
    - Digital Fingerprinting
    - Detection Algorithm
    - Bus Segmentation
  - Benefits
- Success Metrics
  - Methodology
  - Results
- What's Next for IDS Research?
- Presentation History and Publications
- Questions

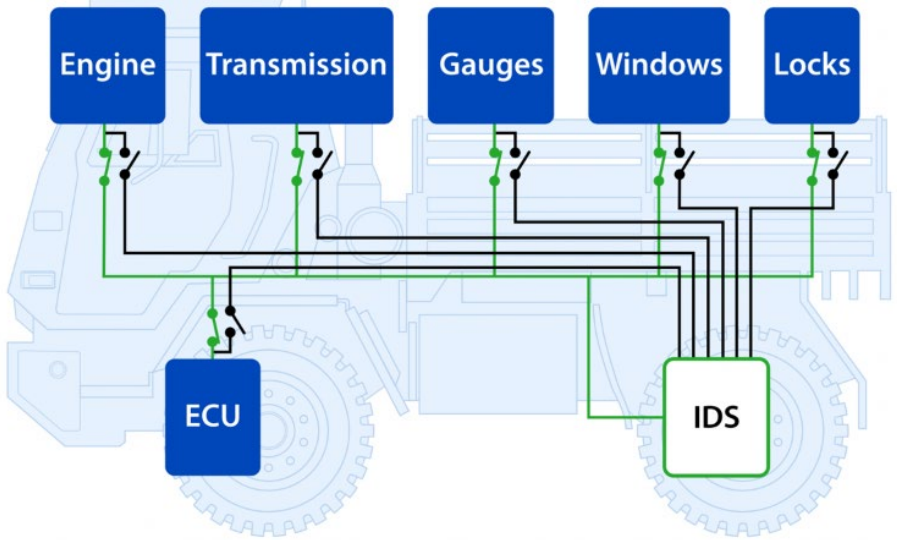
Intrusion Defense System (IDS)

- Digital Fingerprinting
  - Detects anomalies at the physical layer
- Detection Algorithms
  - Signature-based: Uses characteristics of *previously identified malicious packets to uncover anomalies*
  - Anomaly-based: Examines *behavioral characteristics of traffic*
- Bus Segmentation
  - Isolates node where an attack is detected
  - Routes traffic through the IDS and filters out anomalies
  - Retransmits filtered data to keep node operational

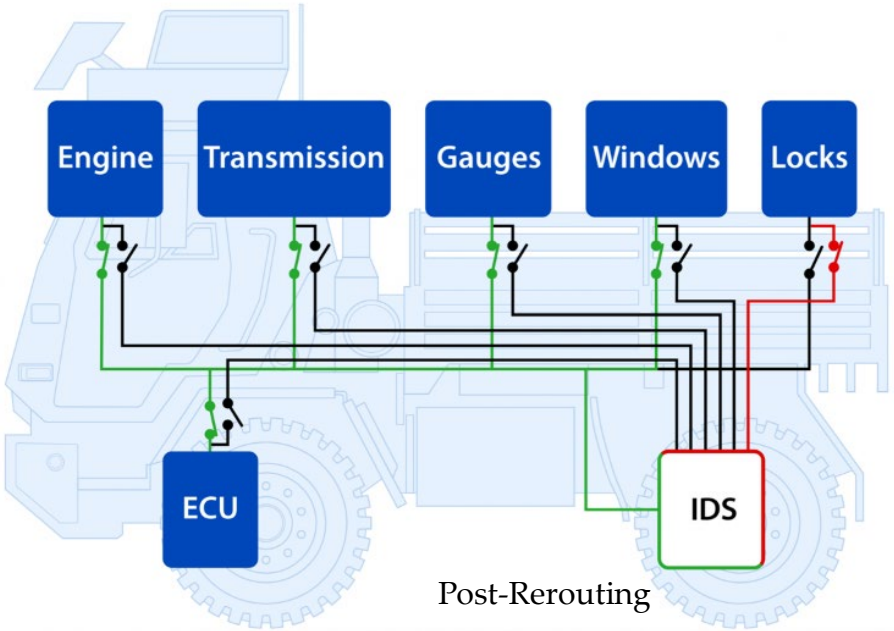


Bus Segmentation Overview

- Used to separate ECUs with remote connectivity
  - Telematics and entertainment units are isolated from critical systems such as the drive train
- Utilize gateway to connect and route traffic between the segments of the bus



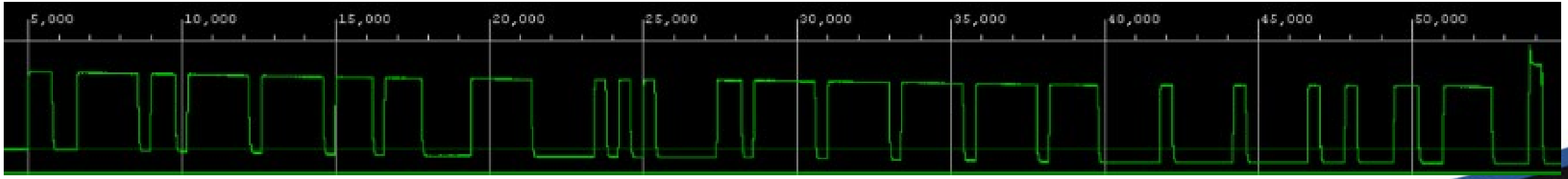
Pre-Rerouting



Post-Rerouting

Digital Fingerprinting Overview

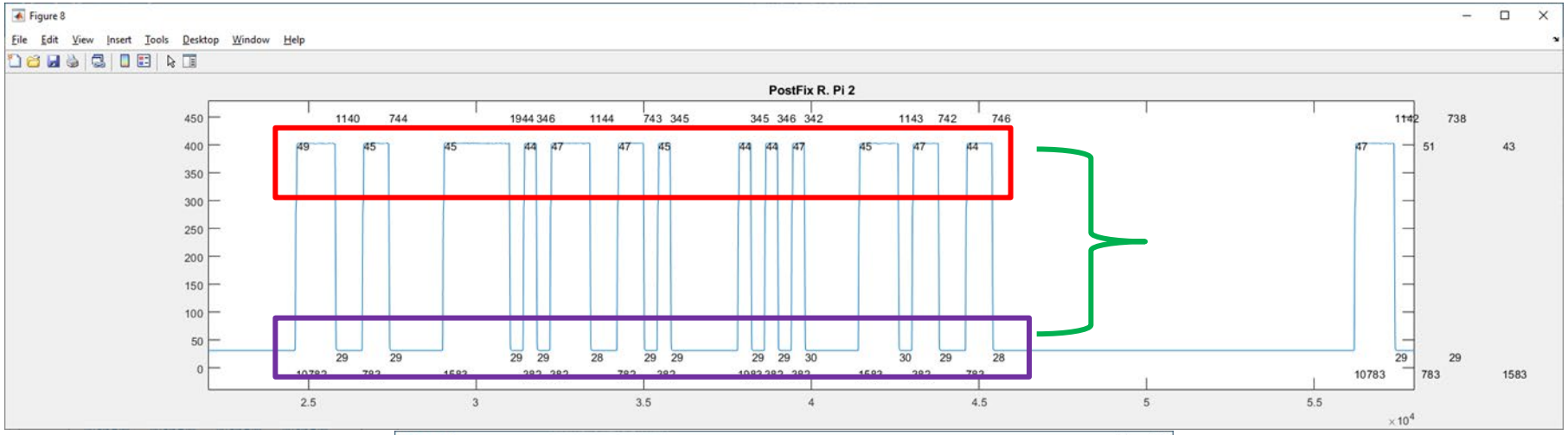
- Analyzes physical layer characteristics of CAN messages
  - Focuses on low-level voltage characteristics of each CAN frame
- Uses characteristics to "fingerprint" each node transmitting messages
- Enables IDS to accurately identify messages sent from unauthorized nodes
- Helps detect compromised nodes that overwrite values, replay packets, and mimic timing
  - Application-layer detection is weak in these areas

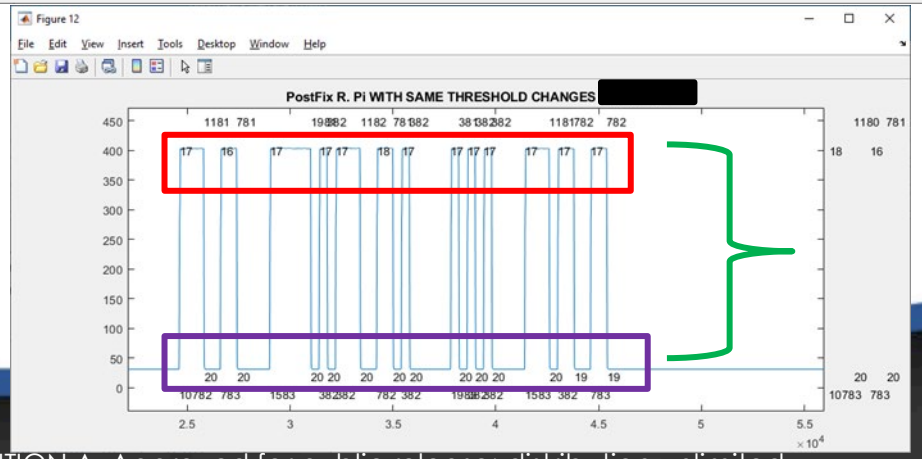


Example. CAN Frame Signal

IDS Fingerprinting: Example

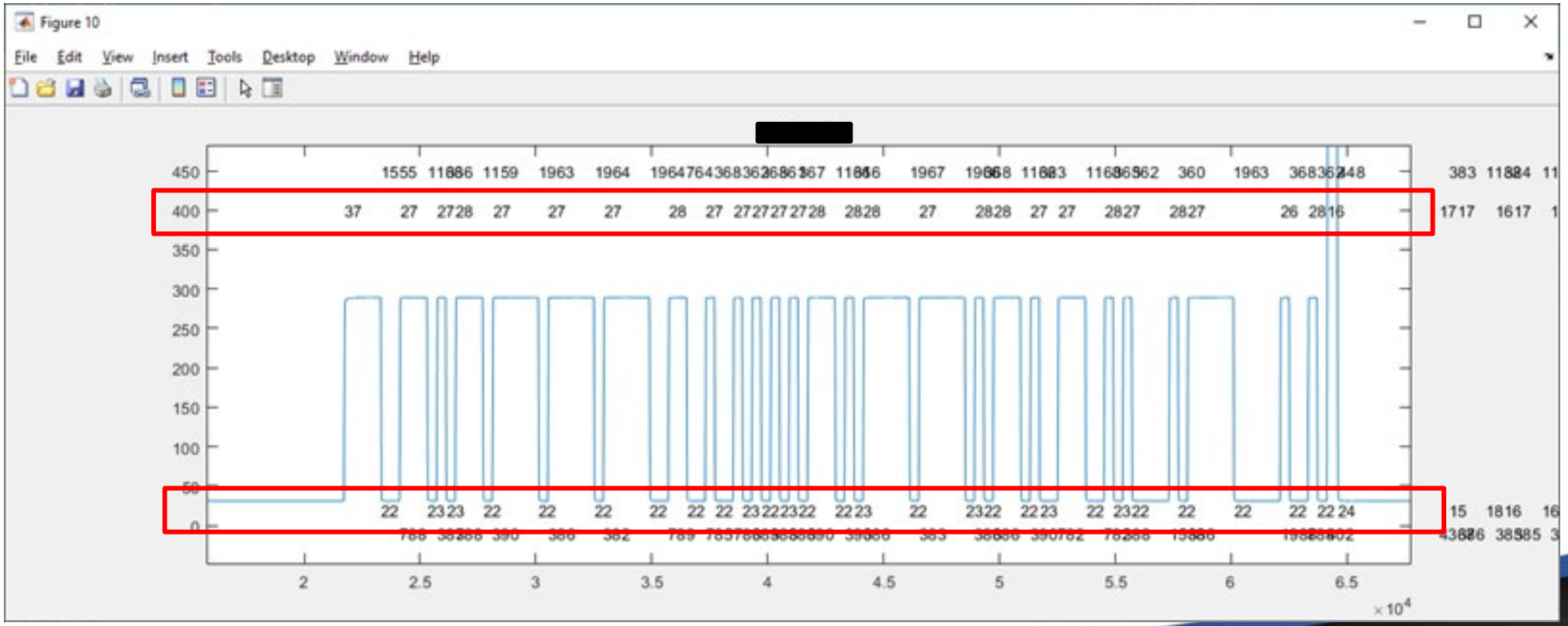
- Two images of single and separate CAN messages (from raspberry pi)
  - Very consistent rise times of each message! (red box)
  - Very consistent fall times of each message! (purple box)
  - CAN messages are different from each other! (green bracket)





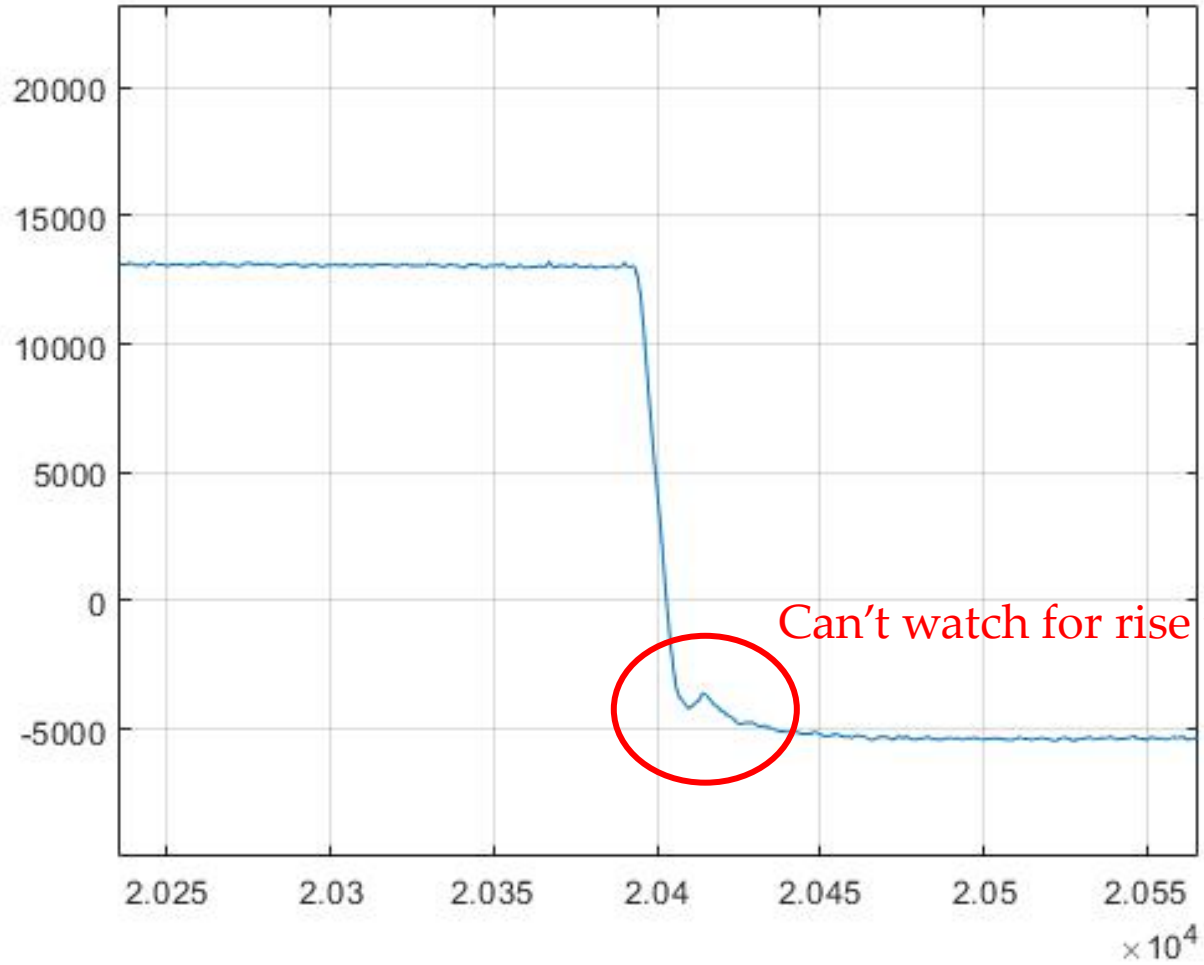
Commercial Vehicle Example

Count rates for rise/fall times outlined highlighted. They are very consistent!



CAN Bus Noise

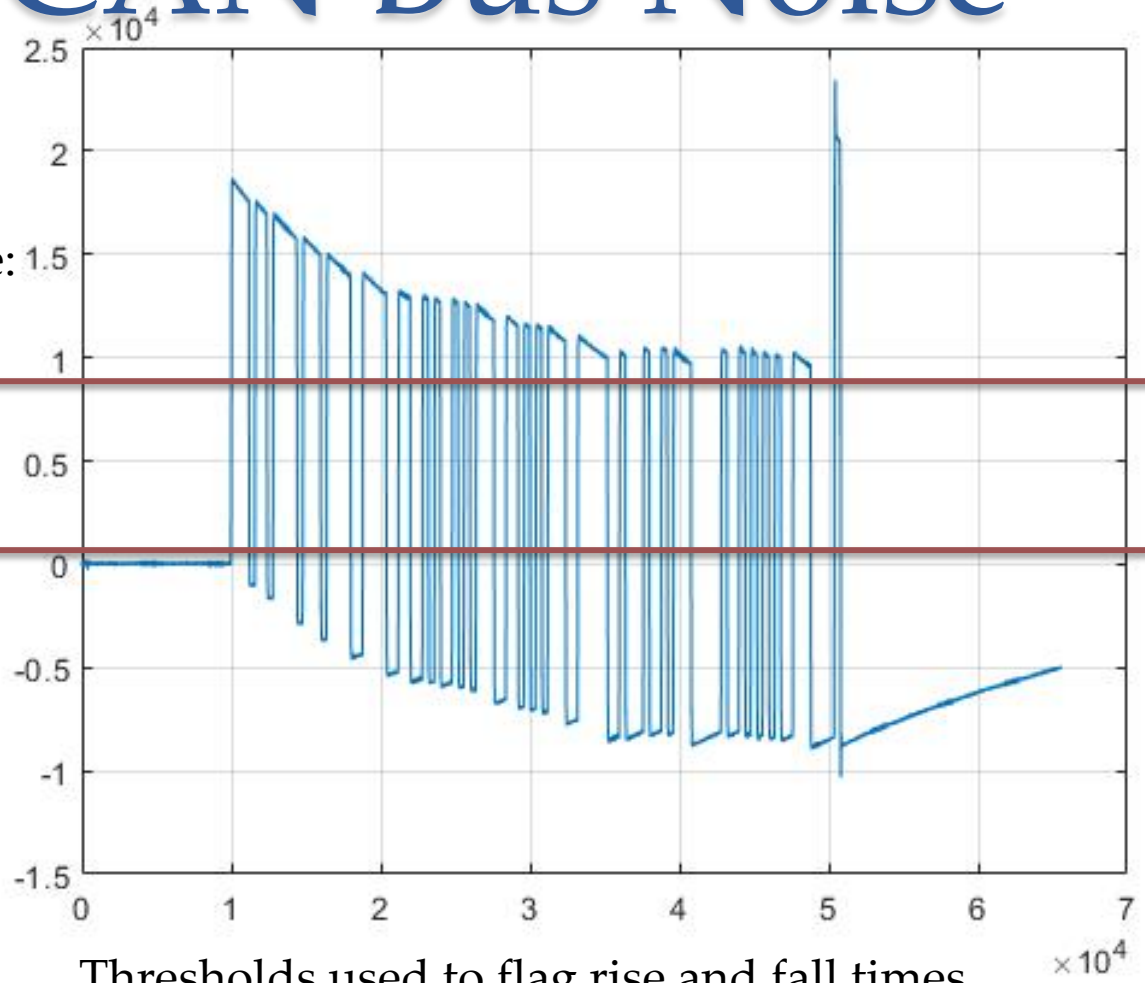
Interesting signal case:



Can't watch for rise to trigger stop.

CAN Bus Noise

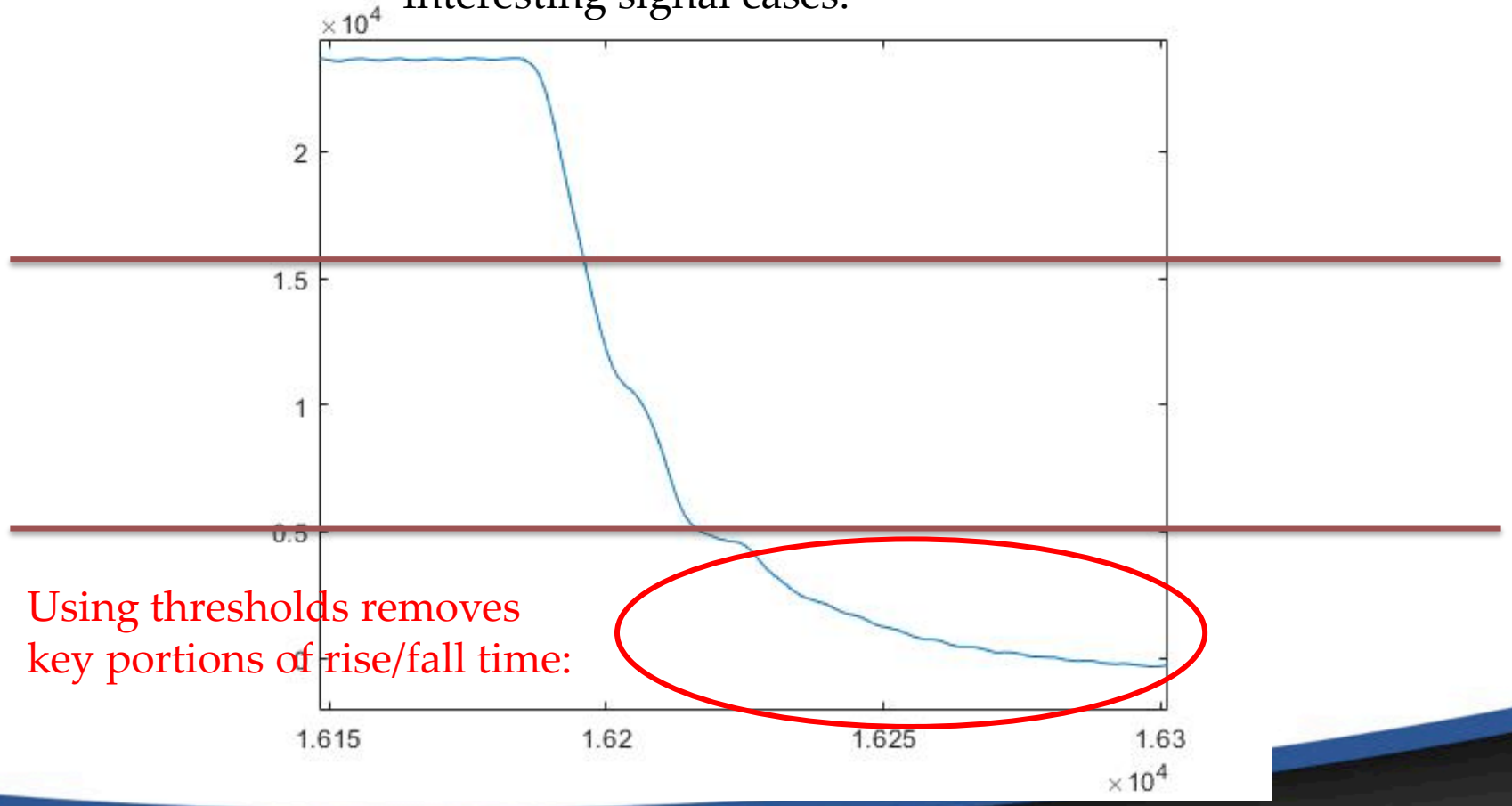
Sample CAN frame:



Thresholds used to flag rise and fall times.
Example: 1.37V low, 3.66V high

CAN Bus Noise

Interesting signal cases:



Using thresholds removes key portions of rise/fall time:

Benefits of the IDS

- Quickly removes malicious messages from the bus
- Avoids introducing a single point of failure onto the vehicle
- Transparent to the vehicle during normal operation
- Fingerprinting adds additional layer of protection
- Full source code and rights are provided

Methodology: Tested Scenarios

Digital Fingerprinting

- **Normal**: Normal operation of the vehicle
- **Masquerade**: One node sends messages that are normally transmitted by another node

Application Layer

- **Normal**: Normal operation of the vehicle
- **Arbitrary Injection**: Arbitrary packets injected onto CAN bus
- **Bus Flood**: High rate of packets intended to overwrite legitimate traffic
- **Throttling**: Manipulates the speed at which packets are broadcast
- **Whitelist**: Packets that don't follow the format of the DBC file
- **Diagnostic**: Normal diagnostic messages

Methodology: Target Thresholds

True Positive
Injected attack packet ***correctly*** flagged as attack

True Negative
Non-attack packet **correctly** not flagged as attack

Result Type	Target Rate
True Positive Rate	>95%
False Positive Rate	<5%
True Negative Rate	>95%
False Negative Rate	<5%

False Positive
Non-attack packet ***incorrectly*** flagged as attack

False Negative
Injected attack packet ***incorrectly*** not flagged as attack

Digital Fingerprinting Results

Test	TP Rate	TN Rate	FP Rate	FN Rate
Normal	Not Applicable	99.76%	0.24%	0.00%
Masquerade Attack	95.70%	99.77%	0.23%	4.30%

- Attack detection rates can be further improved through detection threshold adjustments

Results succeeded metrics and show IDS can identify messages sent from other nodes with very low False Positive rates

Detection Algorithms Results

Test	TP Rate	TN Rate	FP Rate	FN Rate
Normal	Not Applicable	99.67%	0.33%	NA
Arbitrary Injection	91.80%	99.86%	0.14%	8.20%
Bus Flood	98.31%	99.46%	0.64%	1.69%
Throttling	96.80%	99.90%	0.10%	3.20%
Whitelist	100%	99.86%	0.14%	0.00%

Application layer detection has excellent results with very low False Positives

Fingerprinting CAN Transceiver Statistical Model Sample

- Nodes 1A and 1B
  - Two of same device from one manufacturer
  - Two of same device from another manufacturer
- Each devices has consistent measurements and are *easily discernible from another device*
  - Similar hardware from the same manufacturer has significant overlap

Node	Arb ID	Rise Time (Clock Cycles)		Fall Time (Clock Cycles)	
		Mean	Std Dev	Mean	Std Dev
1A	700	10.00	0.08	11.13	0.34
	7EF	10.01	0.13	11.12	0.32
	7F0	10.01	0.08	11.12	0.32
	7FE	10.01	0.09	11.12	0.32
	7FF	10.00	0.05	11.13	0.33
1B	12A	10.31	0.46	11.04	0.20
	135	10.19	0.40	11.00	0.04
	137	10.18	0.38	11.00	0.05
	139	10.19	0.39	11.00	0.06
	160	10.18	0.39	11.00	0.00
2A	410	5.15	0.35	9.41	0.49
	415	5.19	0.39	9.46	0.50
	420	5.15	0.36	9.42	0.50
	425	5.14	0.34	9.40	0.49
	433	5.13	0.33	9.40	0.49
2B	440	5.11	0.55	10.34	0.89
	443	5.07	0.25	10.30	0.87
	444	5.10	0.30	10.27	0.88
	450	5.10	0.30	10.25	0.90
	460	5.09	0.29	10.28	0.90

Fingerprinting Vehicle Statistical Model Sample

- Arbitration IDs from vehicle are grouped by similar measurements
- Vehicle measurements are discernable from other CAN transceivers

Arb ID	Rise Time (Clock Cycles)		Fall Time (Clock Cycles)	
	Mean	Std Dev	Mean	Std Dev
172	22.61	0.71	19.26	0.58
174	22.84	0.54	19.19	0.50
176	22.89	0.48	19.23	0.54
1A1	19.72	0.46	19.24	0.43
1A2	19.20	0.40	20.20	0.40
1B0	18.58	0.61	19.62	0.48
224	16.57	0.52	19.13	0.34
226	16.50	0.53	19.18	0.38
228	16.48	0.57	19.16	0.37
514	12.00	0.03	22.01	0.14
52A	12.00	0.03	22.00	0.11
530	12.00	0.03	22.01	0.12

Arbitration IDs with similar measurements are transmitted from same transceiver within vehicle

Current Work - Automotive Ethernet

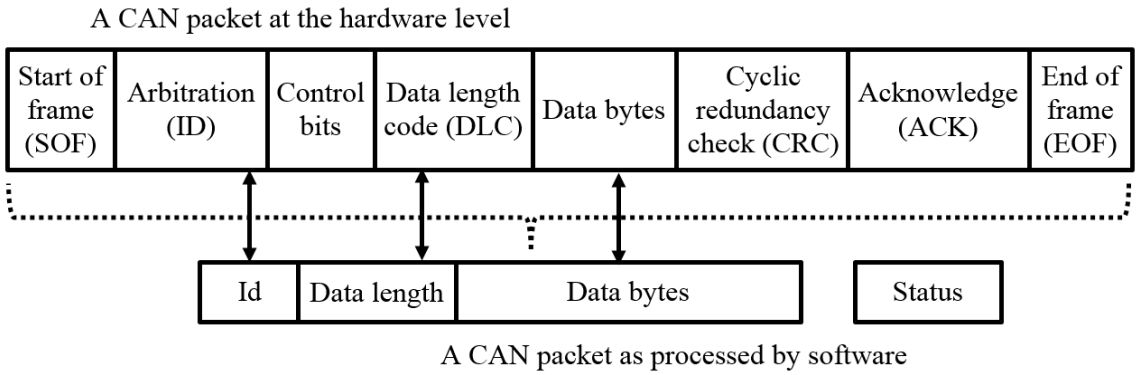
- IDS can read in, characterize, and monitor Automotive Ethernet data
- Specifically looking at the MAC address, IP address, Port, and payload data for each Automotive Ethernet packet

	MAC (Ethernet)	IP	PORT
Source Device: →	('02:00:00:00:02:00',	'10.0.2.0',	'49216')
Destination Device: →	('01:00:5e:00:01:f0',	'239.0.1.240',	'51915')
Communication Protocol: →	UDP		

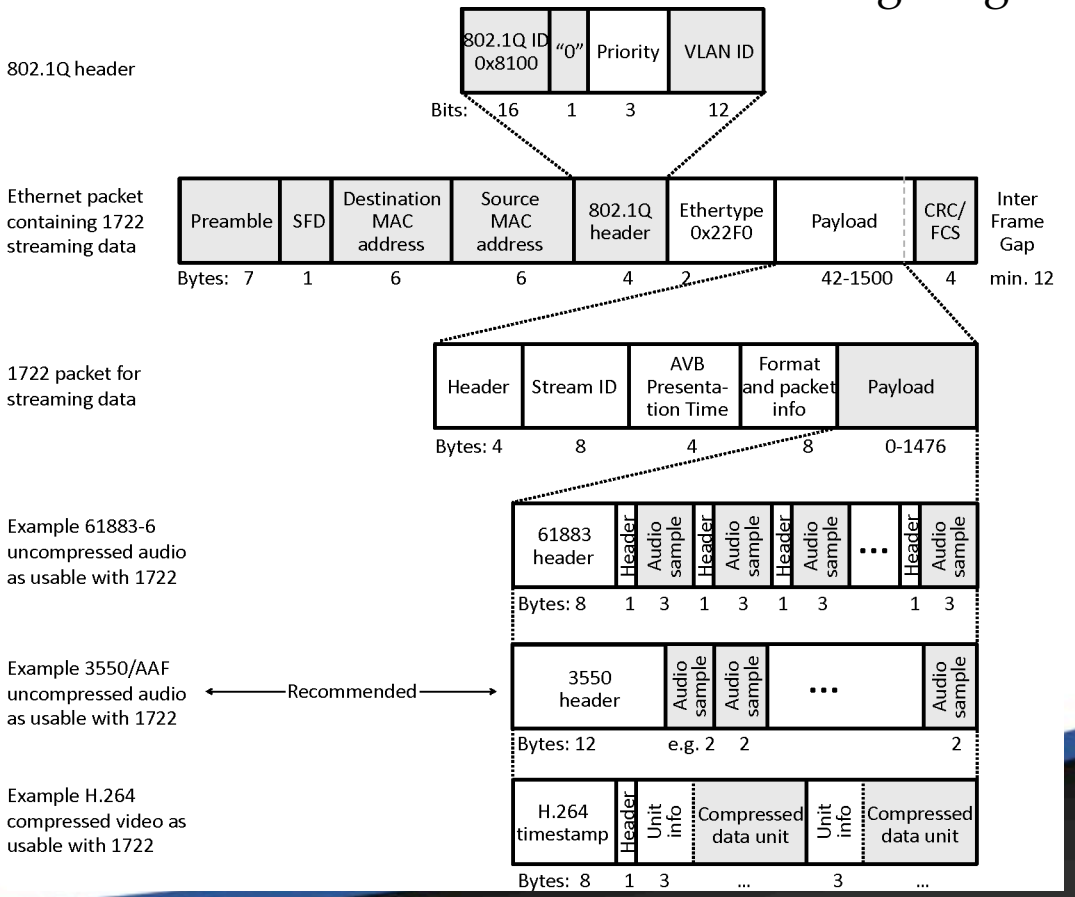
- New challenges involved with adding Automotive Ethernet
  - Requires a new strategy of grouping communications (using src/dst pairs over just Arb. ID)
  - Packets contain more data, higher packet rate (for sample size of 1)

CAN Vs. Automotive Ethernet

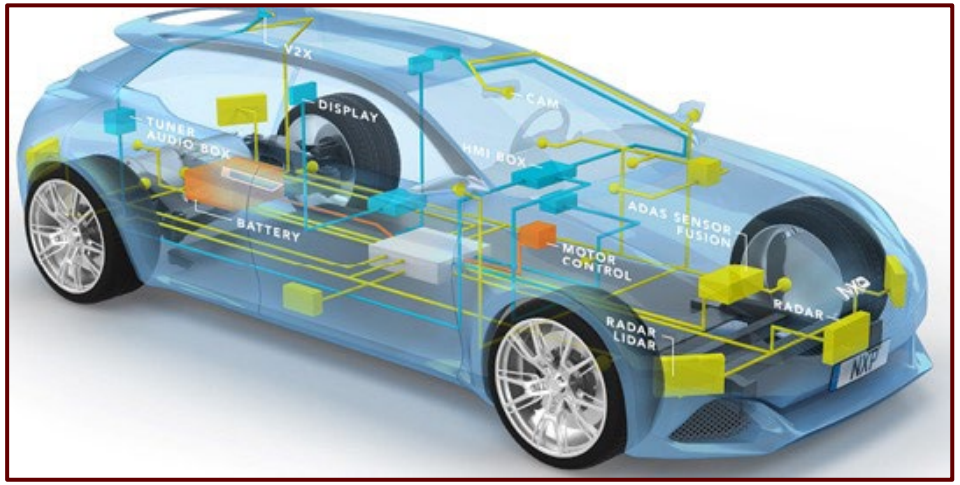
Source: tekeye.uk



Source: cambridge.org



Future Work



- Prepare IDS for deployment by:
  - Reducing false positives
  - Thorough testing on multiple vehicles under various conditions:
    - Environment
    - Temperature
    - Duration
  - Adapting to provide full vehicle coverage

History

- IDS initially funded by SwRI, but most work presented was funded by GVSC (excluding automotive ethernet). The technical POC for GVSC is listed on next slide.
- Similar presentation given to GVSETS (http://www.ndia-mich.org/events/gvsets)
- Links to published papers
  - http://gvsets.ndia-mich.org/documents/VEAC/2020/Cyber_0940_Cyberattack%20Detection%20and%20Bus%20Segmentation%20In%20Ground%20Vehicles_Paper.pdf
  - https://ndia-mich.org/images/events/gvsets/2021/Papers/vea/Cyber%20220PM%20Cyberattack%20Defense%20through%20Digital%20Fingerprinting%20Detection%20Algrorithms%20and%20Bus%20Segmentation%20in%20Ground%20Vehicles.pdf
    - Award for Best Cyber Paper GVSETS.

Questions?

Victor Murray, CISSP
Manager, R&D
Southwest Research Institute
victor.murray@swri.org

Courtney Westrick
Cybersecurity Specialist
Ground Vehicle Systems Center
courtney.m.westrick.civ@mail.mil

References

- http://www.flexautomotive.net/EMCFLEXBLOG/image.axd?picture=/EMCLAB/PNG/CAN%20Bus_Sample_Applications.png
- https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en
- https://www.youtube.com/watch?v=ysAam9Zmdv0
- https://www.gmv.com/export/sites/gmv/images/Sectores/Automocion/automocion_2EN.png
- http://www.simmasoftware.com/j1939-presentation.pdf
- https://style.nxp.com/assets/images/en/photography/gateway-key-topic-card.jpg
- https://img.deusm.com/networkcomputing/2014/12/1318162/connected-car-image-1.png

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

How to Get Involved: Membership

If you are an OEM, supplier or commercial vehicle, Carrier or Fleet, please join the Auto-ISAC!

- *Real-time Intelligence Sharing*
- *Intelligence Summaries*
- *Regular intelligence meetings*
- *Crisis Notifications*
- *Member Contact Directory*
- *Development of Best Practice Guides*
- *Exchanges and Workshops*
- *Tabletop exercises*
- *Webinars and Presentations*
- *Annual Auto-ISAC Summit Event*

To learn more about Auto-ISAC Membership, please contact andreaschunn@automotiveisac.com.
For Partnership, please contact sharmilakhadka@automotiveisac.com.

Auto-ISAC Partnership Programs

Strategic Partnership

- **For-profit** companies such as "Solutions Providers" that sell connected vehicle cybersecurity products & services.
- **Examples:** *Hacker ONE, Upstream, IOActive, Karamba, Grimm*

1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
2. Formal agreements: **NDA, SPA, SoW, CoC** required.
3. **In-kind contributions** allowed. Currently no fee.
4. **Does not** overtly sell or promote product or service.
5. Commits to **support the Auto-ISAC's mission.**
6. Engages with the automotive ecosystem, **supporting & educating Auto-ISAC Members and its Community.**
7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
9. Engagement **must provide Member awareness, education, training, and information sharing**
10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
11. Supports our mission through **educational webinars and sharing of information.**

Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
- Includes ***Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non- Profit, Technical Experts, Auto-ISAC Sponsors.***
- **Examples:** *Autos Innovate, ATA, ACEA, JAMA, MEMA,CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.*

1. **No formal agreement** required.
2. **No approval** required.
3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
4. Participate in **Auto-ISAC Monthly Community Calls.**
5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
6. Added to **Auto-ISAC DRIVEN** list to receive our **daily cyber automotive newsletter.**
7. Part of the Network with **Automotive Community and the extended automotive ecosystem.**
8. Invitation to **attend and support** our yearly Summit.

Current Partnerships

Many organizations engaging

Thanks for your Support to our Many Partners

Community Partners

INNOVATOR
Strategic Partnership (15)

ArmorText
Celerium
Cybellum
Ernst and Young
FEV
GRIMM
HackerOne
Karamba Security
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trillium Secure
Upstream

NAVIGATOR
Support Partnership

AAA
ACEA
ACM
American Trucking Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR
Coordination Partnership

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence Center (NCRIC)
NTIA - DoCommerce
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsch College

BENEFACTOR
Sponsorship Partnership

2021 Summit Sponsors-
Celerium
Cyware
Denso
NDIAS
IOActive
Claroty
Deloitte
Finite State
Tanium
Recorded Future
PaloAlto Networks
Upstream
Securonix
Zimperium
Micron
Block Harbor
SecurityScorecard
Booz Allen
CybelAngel
ATT
Ford
Cybellum

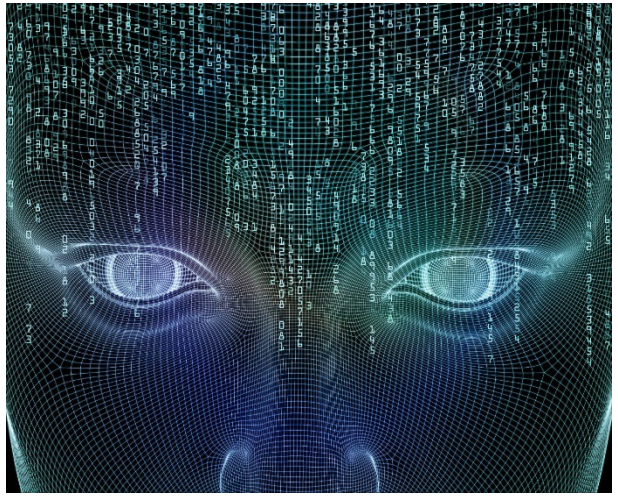
2020 Summit Sponsors-
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

AUTO-ISAC
Automotive Information Sharing and Analysis Center

TLP:WHITE

Auto-ISAC Benefits

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



Building Resiliency Across the Auto Industry

Thank You!


THANK
YOU
WELALIN
JUSPAXAR
OBRIGADO
MATONDO
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
MULTUMESC
GRAZIE
MERCI
MOCHCHAKKERAM
GRAZIE
CHOKRANE
MATUR NUWUN
MATONDO
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
RAIBH MAITH AGAT
SPASIBO
MAAKE
OBRIGADO
SPASIBO
SALAMAT
KIITOS
MOCHCHAKKERAM
MERCI
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
MERCI
RAIBH MAITH AGAT
OBRIGADO
MOCHCHAKKERAM
ASANTE
UA TSAUG RAU KOJ
MOCHCHAKKERAM
KIITOS
OBRIGADO
DANK JE
VINAKA
NIRRINGRAZZJAK
MAMANA
MULTUMESC
ARIGATO
KIITOS
DANKON
MOCHCHAKKERAM
NIRRINGRAZZJAK
MOCHCHAKKERAM
OBRIGADO
SPASIBO

Our Contact Info

Faye Francy
Executive Director

20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Information Technology Executive Coordinator

20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC