Welcome to Auto-ISAC!

Monthly Virtual Community Call

September 2, 2020

Teams Meeting Protocol

Please Note…

1) The **Microsoft Teams meeting link** will provide both audio and visual presentation. In case you need to dial in for audio, please use the phone number and conference ID provided on the invite in the meeting invitation. If you are outside of the U.S, use "**Local Numbers**" link provided in the same meeting invite.
2) If you are dialing in for audio, **please press *6 to mute or unmute** your line.
3) Please keep your **mic muted** at all times except for when the host is addressing your request to ask a question or to provide feedback. Any background noise may disrupt the audio quality for other listeners.
4) If you have question or feedback, you can also use the **chat function**.
5) If you would like to speak, please use **raise hand function** on your screen. The host will be notified and will acknowledge you when ready.

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Overview ➢ Heard Around the Community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** **Urban Jonson, NMFTA, Chief Technology Officer**
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! (lisascheffenacker@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!"*

19 *Navigator Partners*

12 *Innovator Partners*

❖ Participate

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

20 *OEM Members*

❖ 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

36 *Supplier & Commercial Vehicle Members*

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

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

AUTO ISAC – 2020 WAY FORWARD

[redacted]

ROLES, RESPONSIBILITIES & METRICS | *Measuring Success*

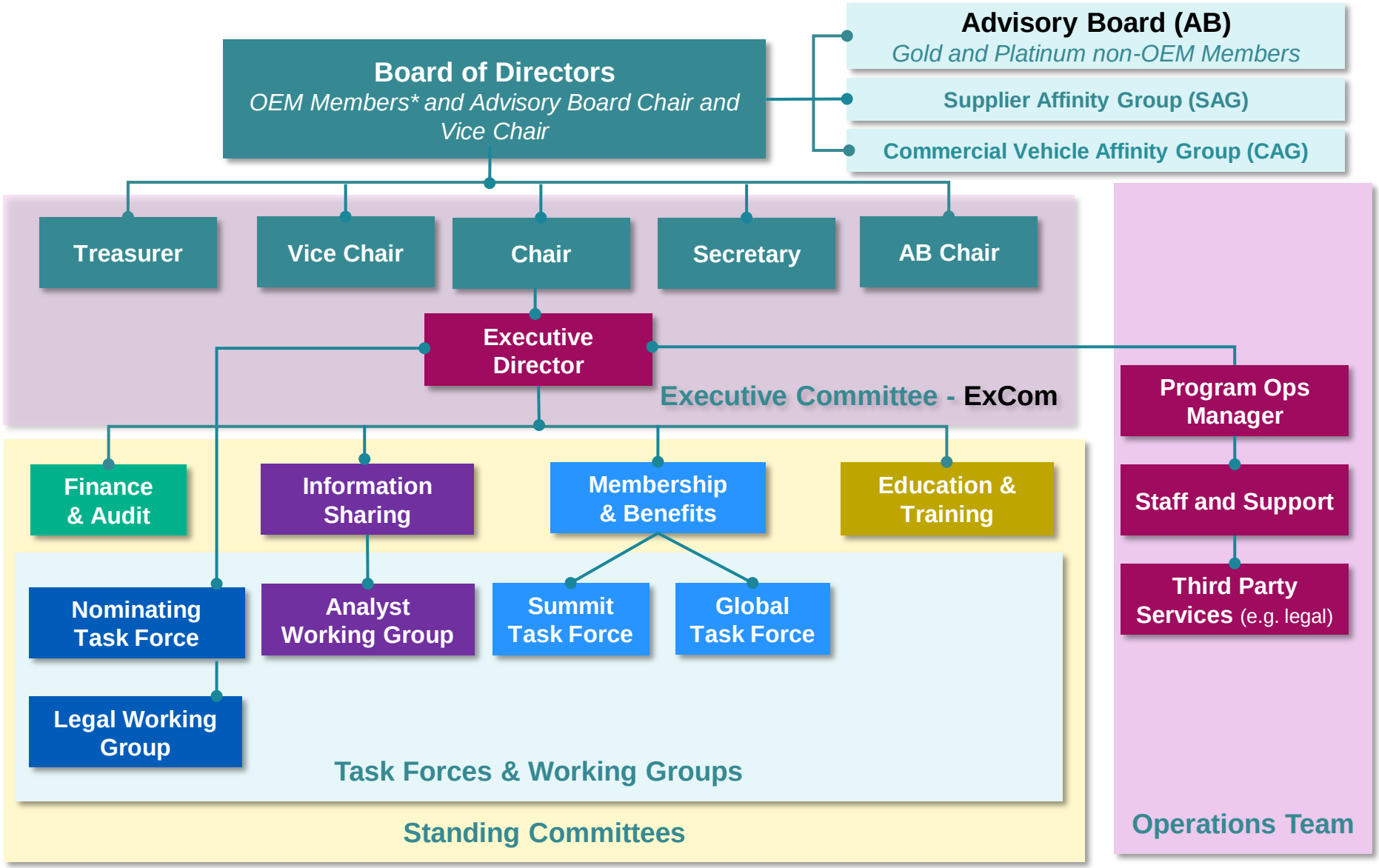
VALUE STREAMS & PERFORMANCE INDICATORS

Top Line Goal: Zero safety related cyber events in the industry

INFO SHARING & AWARENESS	EDUCATION	RELATIONSHIPS
% Participation Sharing / Platform / Attendance	% Taking Educational Offerings Maturity Surveys	% Member Satisfaction with value added relationships

Bottom Line Goal: ***Automotive Cybersecurity Resiliency Across Industry!***

Auto-ISAC Operating Model



2020 Board of Directors

Executive Committee (ExCom)

Kevin Tierney
Chair of the Board of the Directors
GM

Josh Davis
Vice Chair of the Board of the Directors
Toyota

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

2020 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Brian Murray
Vice Chair of the Advisory Board
ZF

Kevin Walker
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

Member Roster

As of September 1, 2020

Highlighted = Change

Aisin	Honda	Oshkosh Corp
Allison Transmission	Hyundai	PACCAR
Aptiv	Infineon	Panasonic
AT&T	Intel	Qualcomm
Blackberry Limited	Kia	Renesas Electronics
BMW Group	Knorr Bremse	Subaru
Bosch	Lear	Sumitomo Electric
Continental	LGE	Tokai Rika
Cummins	Magna	Toyota
Denso	MARELLI	TuSimple
Delphi Technologies	Mazda	Valeo
FCA	Mercedes-Benz	Veoneer
Ford	Mitsubishi Motors	Volkswagen
Garrett	Mitsubishi Electric	Volvo Cars
General Motors	Mobis	Volvo Group
Geotab	Navistar	Waymo
Google	Nexteer Automotive Corp	Yamaha Motors
Harman	Nissan	ZF
Hitachi	NXP	TOTAL: 56

Auto-ISAC Activities

- **Auto-ISAC Europe 2020 Meeting Members & Potential Members only –** ***September 3&4 – virtual event ccurring this week. For more information, contact Lisa Scheffenacker – lisascheffenacker@automotivisac.com***

- **Other Key Auto-ISAC Member Events -**
  - **Education & Training Series Series: Sept 16th.** Kevin presenting**:** *Building an Integrated Cybersecurity Organization*
  - **All Member's Meeting** – Sept 23rd
  - **Advisory and Board of Director Meetings** –Sept 24th

- **Auto-ISAC Summit October 14-15th – registration until OCT 30th, sponsorships on website – www.automotiveisac.com. *VIRTUAL***

AUTO-ISAC SUMMIT | OCT 14-15TH | VIRTUAL

AUTO-ISAC SUMMIT

Oct. 14-15,
2020
Virtual

2 days

400 attendees

ABOUT THE AUTO-ISAC SUMMIT:
The 2020 Auto-ISAC Summit connects global automotive industry insiders during two days of transformative conversations around cyber attack resilience and response.

Registration Open Until OCT 30th || Sponsor Prospectus

Auto-ISAC Summit | Oct 14-15th | VIRTUAL

- **REGISTER TODAY!!!** Registration open until October 30th, 6 virtual passes for price of 1 ticket.

- **Two Sponsored Speaker Slots Open-** Please reach out to sharmilakhadka@automotiveisac.com, if you have topic to present.
  - 20 minutes live speaking slot
  - Includes 6 virtual passes
  - Virtual booth included & much more (please visit our website automotiveisac.com for more info and prospectus.)

- **Sponsorship Opportunities Available-** Virtual Booth, On-Demand, Two-Sponsored Happy Hour.
  - Reach out to Sharmila Khadka if you need more information or need to schedule 30-minutes call to learn more.

The Auto-ISAC encourages the automotive industry to review their insider threat and cybersecurity awareness programs

Russian National Arrested for Conspiracy to Introduce Malware into a Nevada Company's Computer Network A Russian national made his initial appearance in federal court Monday for his role in a conspiracy to recruit an employee of a company to introduce malicious software into the company's computer network, extract data from the network, and extort ransom money from the company. Egor Igorevich Kriuchkov, 27, a citizen of Russia, was charged in a complaint with one count of conspiracy to intentionally cause damage to a protected computer. He was arrested on Aug. 22, 2020, in Los Angeles and had his initial appearance before U.S. Magistrate Judge Alexander F. MacKinnon in U.S. District Court in Los Angeles, California, who ordered Kriuchkov detained pending trial.

Tesla Insider Works with FBI to Turn the Tables on Russia's Million Dollar Attempt to Hijack the Network On August 25, the Department of Justice announced the arrest of Egor Igorevich Kriuchkov, a citizen of Russia, for conspiring to breach the network of Tesla operations in Sparks, NV and introduce malware into the+ company's network. Unpacking the criminal complaint filed by the FBI Las Vegas Field office, it is clear this isn't an ordinary attempt to infuse malware into a company's network, but rather an effort led by a well-financed and logistically nimble organization.

Tesla employee foregoes $1M payment, works with FBI to thwart cybersecurity attack

Elon Musk confirms Russian hacking plot targeted Tesla factory

For more information or questions please contact analyst@automotiveisac.com

CISA RESOURCE HIGHLIGHTS

3rd Annual National Cybersecurity Summit

- **The CISA 2020 National Cybersecurity Summit will be held virtually as a series of webinars every Wednesday beginning September 16 and ending October 7:**
  - Sept 16: Key Cyber Insights
  - Sept 23: Leading the Digital Transformation
  - Sept 30: Diversity in Cybersecurity
  - Oct 7: Defending our Democracy
- **No-cost event but pre-registration is required at https://cisacybersummit2020[.]Eventbrite[.]com/**
- **More information at https://www[.]cisa[.]gov/cybersummit2020**

Industrial Control System Joint Working Group (ICSJWG)

- **The CISA ICSJWG will be will be held virtually on Tuesday and Wednesday September 21-22, 2020**
- **The ICSJWG is a no-cost event but requires pre-registration by Friday, September 18 at**
  - **https://event[.]on24[.]com/eventRegistration/EventLobbyServlet?target=reg20.jsp&referrer=https%3A%2F%2Fwcc.on24.com%2Fwebcast%2Fgroupregistration%2F2524874&eventid=2524874&sessionid=1&key=680071B2F840164979B2E51734D61BAE&regTag=1115681&sourcepage=register**
- **More information at**
  - **https://us-cert[.]cisa[.]gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG**
  - ICSJWG.Communications[@]cisa[.]dhs[.]gov

National Insider Threat Awareness Month

- **September 2020 - National Insider Threat Awareness Month (NITAM)**
- **NITAM is sponsored by the Center for the Development of Security Excellence (CDSE) – see https://www[.]cdse[.]edu/itawareness/index.html**
- **CDSE is hosting a virtual conference on Thursday September 3, 2020 in support of NITAM. Register at https://cdse-events[.]acms[.]com/content/connect/c1/7/en/events/event/shared/6835736/event_landing.html?sco-id=6819559**
- **CISA insider threat program resources:**
  - **https://www[.]cisa[.]gov/sites/default/files/publications/fact-sheet-insider-threat-mitigation-program-092018-508.pdf**
  - **https://www[.]cisa[.]gov/insider-threat-mitigation**

TLP: WHITE – CISA Alert AA20-245A - Technical Approaches to Uncovering and Remediating Malicious Activity

- Result of collaborative research effort by the cybersecurity authorities of five (5) nations: Australia, Canada, New Zealand, the United Kingdom, and the United States
- Key takeaways include prioritization of analysis artifacts, mitigation steps, and solicitation of incident response support
- Sections include technical details and incident handling mistakes to avoid
- Available for review at:
  - https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-245a
- Available for download at:
  - https://us-cert[.]cisa[.]gov/sites/default/files/publications/AA20-245A-Joint_CSA-Technical_Approaches_to_Uncovering_Malicious_Activity_508.pdf

TLP: WHITE – CISA Current Activity - Cisco Releases Security Advisory for DVMRP Vulnerability in IOS XR Software

- Cisco has released a security advisory on a vulnerability—CVE-2020-3566—in the Distance Vector Multicast Routing Protocol (DVMRP) feature of Cisco IOS XR software.
- This vulnerability affects Cisco devices running IOS XR software that have an active interface configured under multicast routing.
- A remote attacker could exploit this vulnerability to exhaust process memory of an affected device
- This vulnerability was detected in exploits in the wild
- CISA summary at https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/08/31/cisco-releases-security-advisory-dvmrp-vulnerability-ios-xr includes the link to the Cisco advisory for this vulnerability

TLP: WHITE – CISA Technical Alert AA20-239A FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks

- Joint effort between U.S. government partners, CISA, Treasury, FBI, and USCYBERCOM
- Identified malware and indicators of compromise (IOCs) used by the North Korean government in the noted automated teller machine (ATM) cash-out scheme
- The Alert provides new details about the resumption of a North Korean global cyber-enabled bank robbery scheme targeting banks in multiple countries to initiate fraudulent international money transfers and ATM cash outs.
- An overview and a short profile of the group responsible for this activity, an in-depth technical analysis, and detection and mitigation recommendations are provided

TLP: WHITE – CISA Technical Alert AA20-239A FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks (continued)

- Alert AA20-239A "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks"
  - https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-239a
- IOCs are available in the following Malware Analysis Reports (MARs):
  - AR20-239C : MAR-10257062-1.v2 - North Korean Remote Access Tool: FASTCASH for Windows
    - https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-239c
  - AR20-239B : MAR-10301706-2.v1 - North Korean Remote Access Tool: VIVACIOUSGIFT
    - https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-239b

TLP: WHITE – CISA Technical Alert AA20-239A FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks (continued)

- Malware Analysis Reports (MARs) - continued:
  - AR20-239A : MAR-10301706-1.v1 - North Korean Remote Access Tool: ECCENTRICBANDWAGON
    - https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-239a
- North Korea cyber activity information at https://us-cert[.]cisa[.]gov/northkorea
- Additional IOC information is available from CYBERCOM at https://www[.]virustotal[.]com/en/user/CYBERCOM_Malware_Alert/

TLP: WHITE – North Korean Malicious Cyber Activity - BLINDINGCAN

- Joint effort between CISA, FBI and U.S. Government partners
- Analytical effort resulting in the Malware Analysis Report (MAR) report on the North Korean government use of the malware variant "BLINDINGCAN“
- BLINDINGCAN found to be Remote Access Trojan (RAT) malware variants used by the North Korean government.
- CISA resources for review:
  - https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/08/19/north-korean-malicious-cyber-activity
  - https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-232a
  - https://us-cert[.]cisa[.]gov/sites/default/files/publications/MAR-10295134-1.v1.WHITE_stix.xml
  - https://us-cert[.]cisa[.]gov/northkorea

TLP: WHITE – Additional Resources From CISA

- CISA Homepage - https://www[.]cisa[.]gov/
- CISA News Room - https://www[.]cisa[.]gov/cisa/newsroom
- CISA Publications Library - https://www[.]cisa[.]gov/publications-library
- CISA Cyber Resource Hub - https://www[.]cisa[.]gov/cyber-resource-hub
- CISA Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - https://www[.]us-cert[.]gov/resources/ncats/
- CISA Cybersecurity Directives - https://cyber[.]dhs[.]gov/directives/
- CISA COVID-19 Response – https://www[.]cisa[.]gov/coronavirus

For more information:
cisa.gov

Questions?
CISAServiceDesk@cisa.dhs.gov
1-888-282-0870


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

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

Slides available on our website – www.automotiveisac.com

Featured Speaker
Urban Jonson

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Urban Jonson, NMFTA

Chief Technology Officer

Urban Jonson is the Chief Technology Officer and the Program Manager of the Heavy Vehicle Cyber Security (HVCS) program for National Motor Freight Traffic Association, Inc., (NMFTA). Urban has over 30 years of experience in information technology, complex systems analysis and information technology security. NMFTA is a non-profit membership organization headquartered in Alexandria, Virginia which represents over 500 carriers that collectively operate over 200,000 power units generating over $100 billion in freight revenue. Urban is also the Transportation Subject Matter Expert for FBI's InfraGard.

Currently, Urban's main area of interest is in heavy vehicle and transportation systems cyber security, cybersecurity talent development, threat intelligence and autonomous cyber defense.

Are large fleets susceptible to advanced attacks?

Automotive-ISAC

Community Call

September 2, 2020

Based on a blog post

This presentation is based on a recent guest blog post at IOActive. A big thank you to IOActive for providing me with an opportunity to connect with their community.

https://ioactive.com/guest-blog-urban-jonson-nmfta

Agenda

- Triton Malware Overview
- Safety Controllers
- ATA/TMC RP 1218
- Persistence
- Motivation
- Collaboration
- Q & A

Triton Malware

- Attack on middle east petrochemical plant in 2017
- Highly sophisticated and targeted
- First component was a windows remote access tool for an engineering workstation
- Second component a specific zero day against Schneider Electric Triconex safety controller with firmware versions (10.0 - 10.4)
- Safety controller design to initiate automatic shutdown operations without user intervention

Triton Level of Effort

- Determine specific controllers and firmware versions at plant
- Obtain same equipment to research and find a zero day vulnerability
- Research plant's IT infrastructure for attack vector for an engineering workstation
- Compromise workstation as staging area for attack
- Actively fought to maintain foothold during blue team cleanup after discovery
- This is A LOT of effort and requires serious skills

Triton Failed

- Unplanned “accidental shutdown” revealed the presence of the malware
- A great deal about this intrusion is still murky and closely guarded, but it is considered to be one of the most potentially deadly malware attacks in history
- Theory is that attackers wanted capability, but did not intend to use it immediately
- Sometimes when you play with bombs, they go off unintentionally
- For a more successful example see Operation Olympic Games (uranium centrifuges)

Safety Controllers

- The Triconex safety controller sounds familiar
- Practically everywhere in modern automotive in the form of crash avoidance, lane departure assist and many other features
- Automotive safety systems rely on sensor data such as camera and LIDAR to make decisions on real-time braking, steering and other actions without user action
- How diverse is this market? Are there ubiquitous sensor models in our industry?

Safety Controllers

- Do we have our own version of a Triconex safety controller to worry about?
- A recent paper “Fault Detection, Isolation, Identification and Recovery (FDIIR) for automotive perception sensors” by Goelles, Schlager and Muckenhuber from Virtual Vehicle Research sheds some light
- Conclusion of the paper is that for the most part LIDAR is treated as a black box with little knowledge of firmware and interfaces

Safety Controllers

- Industry needs multiple components working cooperatively to implement active safety features
- A centralized small group of companies providing homogenous safety critical components with lack of transparency is a big security risk
- Obtaining transparency from tier suppliers is hard
- Black boxes with undocumented and poorly understood interfaces are a hacker's delight

RP1218

- Surely there are easier targets than LIDAR?
- Enter ATA / TMC RP1218
- American Trucking Associations (ATA) Technology Maintenance Council (TMC) produces recommended practices (RPs) for trucking industry
- Example RP 1226 Telematics-Tractor connector specifications
- So what is RP 1218?

RP 1218

- “Guidelines for Remote Disablement of Commercial Vehicles” - how to implement a remote shutdown and/or limp mode for a heavy truck
- Core premise of 2005 version of RP 1218 was “secret” CAN messages (Uh-oh)
- Did anyone implement this RP?
- **Good News:** After some extensive research we did not find that anyone had implemented the 2005 version RP1218
- **Bad News:** We found plenty of other ways to do it including diesel exhaust messages and derate limits among others

RVS and RVD

- We also found a robust global market for both Remote Vehicle Shutdown (RVS) and Remote Vehicle Disablement (RVD)
- **Good News:** Methods by which the various vendors achieved RVS/RVD varied significantly and were not as simple as sending a message to the engine using RP 1218
- **Bad News:** There's not a great deal of transparency. Another inscrutable black box (hacker's delight)

Persistence

- Triton's initial persistence was on an engineering workstation with a remote access tool (RAT)
- Once discovered a much broader scope of infrastructure was used to try to maintain foothold
- What is the equivalent in fleets/transportation?
  - Telematics backend systems?
  - Customer support workstations?
  - Dealership networks?
  - Telecommunications devices (think apps)?

Motivation

- How much effort do you think someone would go through to obtain the ability to affect motor transportation at scale?
- Do you think they would conduct the same level of research on infrastructure and components, and attempt to compromise these systems so that they can be hit at the most critical time?

Open Questions

- Are there any lessons from the Triton ICS attack that we can leverage in designing active safety systems for vehicles?
- Can we develop an attack tree for someone attempting a sophisticated nation-state attack against vehicle safety control systems or remote disablement vendors?
- How do we best defend against someone who would like to own our infrastructure and unleash disruption on our transportation sector?
- How do we improve our designs, resiliency, processes, and general security posture against this type of threat?

Collaboration

- Possibly Cyber-informed Engineering (CCE) can play a role, but that's very hard when it involves black-box technology with unknown interfaces
- This is a complex and difficult problem
- An updated RP 1218 is still under development and consideration
- Requires collaboration between industry experts
- Problem spans transportation modes and needs multi-model collaboration
- No easy answers so we have to do the hard work
- We have to collaborate to safeguard our infrastructure

References

Blake Sobczak, The inside story of the world's most dangerous malware. *E&E News*, March 2019

NSA/CISA Joint Report Warns on Attacks on Critical Industrial Systems. July 27, 2020.

Tara Sales, Triton ICS Malware Hits A Second Victim. *SAS 2019*, Published on *Threatpost.com,* April 2019.

Pierluigi Paganini, 'Olyimpic Games' and boomerang effect, it isn't sport but cyber war, June 2012.

Goelles, T.; Schlager, B.; Muckenhuber, S. Fault Detection, Isolation, Identification and Recovery (FDIIR) Methods for Automotive Perception Sensors Including a Detailed Literature Survey for Lidar. *Sensors,* 2020, *Volume 20, Issue 13.*

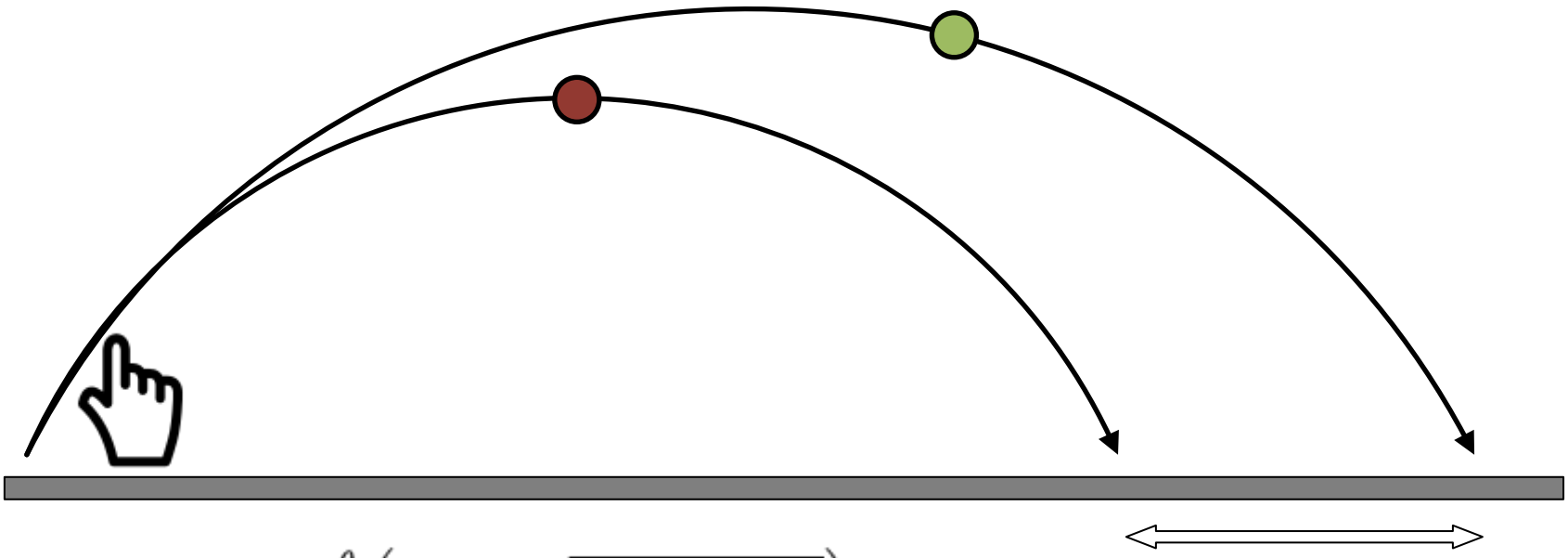
Ben Gardiner, Automotive Sensors: Emerging Trends With Security Vulnerabilities And Solutions. *MEMS Journal*, February 2017.

For more information on CCE please see the INL website. A short overview can be found here.

National Motor Freight Traffic Association, Inc., A Survey of Heavy Vehicle Cyber Security. September 2015.

Change Trajectory

… a small nudge can have a big effect



$$d = \frac{v\cos\theta}{g}\left(v\sin\theta + \sqrt{(v\sin\theta)^2 + 2gy_0}\right)$$

Thank You

A big thank you to the Automotive-ISAC for providing me with an opportunity to connect with their community.

Questions

Urban Jonson
Chief Technology Officer
National Motor Freight Traffic Association, Inc
Email: urban.jonson@nmfta.org

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 or Partnership, please contact Auto-ISAC! contact.us@automotiveisac.com

Strategic Partnership Programs

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, SANS, IOActive, GRIMM

Associations

Industry associations and others that want to support and invest in the Auto-ISAC activities.

Examples: Alliance, ACEA, ATA, JAMA, CLEPA

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: DHS, NHTSA, Colorado State, Johns Hopkins, NCI

Community

Companies interested in engaging the automotive ecosystem and supporting the community.

Examples: Summit sponsorship – key events

INNOVATOR

Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed

NAVIGATOR

Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities

COLLABORATOR

Coordination Partnership

- "See something, say something"
- May not require a formal agreement
- Information exchanges- coordination activities

BENEFACTOR

Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

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
danke
gracias
merci
obrigado
شكراً جزيلاً
ngiyabonga
謝謝
teşekkür ederim
рахмат
Баярлалаа
спасибо
faafetai lava
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
köszönöm
bedankt
bayarlalaa
grâçie
hvala
enkosi
dziękuję
sobodi
dėkuji
vinaka
спасибі
blagodaram
mersi
kia ora
barka
welalin
tack
spas
dank je
misaotra
matondo
paldies
grazzi
mahalo
tapadh leat
хвала
asante
manana
obrigada
tenki
murakoze
djiere dieuf
tau
mochchakkeram
дякую
mamnun
chokrane
akun
dankon
aciū
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
taiku
sukriya
kop khun krap
sagolun
mèsi
didi madloba
najis tuke
ありがとう
kam sah hamnida
rahmat
terima kasih
tanemirt
rahmet
grazie
arigatô
takk
dakujem
trugarez
shukriya
mercé
мерси
dhanyavadagalu
diolch
ευχαριστώ
xièxie
감사합니다
তোমাকে ধন্যবাদ

Our contact info

Faye Francy
Executive Director

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

Sharmila Khadka
Executive Organizational Secretary

20 F Street NW, Suite 700
Washington, DC 20001
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC