Automotive Cybersecurity Team Home

Notice: This site is being updated as of May 2022. We look forward to updating you on all of the exciting initiatives we have, so please check back regularly! – Joby

As vehicles become increasingly connected and software-powered, COVESA (formerly GENIVI) recognizes an emerging need for a comprehensive, end-to-end security model. The COVESA Security Team looks at automotive cybersecurity holistically and delivers guidelines, research, and education that help build, deliver and manage more secure vehicles in the future.

Automotive Cybersecurity Team Charter

The Charter of the COVESA Security Team is to:

1. Assemble emerging automotive cybersecurity challenges/solutions/standards and inform stakeholders through published guidelines, briefs, webinars and event presentations
2. Equip stakeholders to understand and use methods and models for identifying and mitigating cybersecurity attacks on a vehicle
3. Deliver education that equips software developers and architects with an understanding of typical approaches for attacking a vehicle and with methods of mitigating those attacks with sound software development methods and testing
4. Advise COVESA software development activities to deliver more secure solutions for the connected vehicle.

Getting Involved / Learn More

Security Team Chair: Joby Jester joby.jester@capgemini.com

Security Team Co-Chair Lead: Jennifer Dukarski dukarski@butzel.com

Security Team Co-Chair 2nd: Brandon Barry brandon@blockharbor.io

Marketing & COVESAI: michael nunnery MikeNunnery@comcast.net

Team Meetings occur every other Thursday at 10:00am US Eastern Time

Next Meeting: May 12th, 2022, 1600 CEST, 1000 EDT, 0700 PDT.

https://us06web.zoom.us/j/87394558934?pwd=OHZ3UHJCM1Q0K1Q4M05RTWJGQU9odz09

One-Page Slide To Promote Security Team:

Current Security Team Project Initiatives & Discussions

- Data Classification
- Vehicle Spoofing
- UNECE WP 29
- Description Language
- Security Tools
- Upcoming Security Conferences & Workshop Presentations & Speaking Opportunities
- ISO 21434 Updates
- Cybersecurity Executive Order (related to White House statements on 5/12/2021)
- Privacy

Recent Activities, Reports & Deliverables

- MoRA Presentation for COVESA Sec Team
    - Planning the creation of Security Evaluation Framework based on MoRA methodologies
- Recorded cybersecurity tracks from 2020 and 2021 All Member Meetings (Virtual Conferences) please scroll below to see sessions
- 2019 All Member Meeting – (see multiple security-related topics on 5/16 and 5/17 schedule)
- 2018 All Member Meeting – (see multiple security-related topics on 4/19 schedule)
- Technical Brief: Certificate Pinning (with Cloakware/Irdeto)

- White Paper: Man in the Middle Attacks and Secured Communications
- Webinar: How to Secure the Connected Vehicle Ecosystem (Presentations by Uber and Irdeto)
- "Automotive Cybersecurity Literature Review," a report illuminating crucial research gaps
- "Automotive Industry Guidelines for Secure Over-the-Air Updates," a document for assisting automotive manufacturers and others involved in evaluating platforms for secure updates
- An Exchange zero day vulnerability.pdf (discussed on March 4, 2021 security team call)
    - SPECIAL ADVISORY: https://threatpost.com/microsoft-exchange-zero-day-attackers-spy/164438/
- Executive Order on Improving the Nations Security: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Other

Past Activities & Deliverables

- Security Requirements
- Threat Model

Upcoming Events

- COVESA All Member Meeting in Leipzig Germany April 26-28, 2022 (LIVE with some virtual workshops for Security and IVP/EV Charging)
- COVESA TU AutoTech: Detroit networking event April 8, 2022 at Bar Louie in Novi (Register at https://COVESA2022June8.eventbrite.com passcode "collaboration")

Note: Registration links for AMM in Germany is https://www.eventleaf.com/e/COVESAAMM

Past Events

- **(April 28, 2022 - Virtual during AMM in Leipzig Germany)** Register Here
- **(January 5, 2022 - LIVE in Las Vegas at Bellagio Hotel)** COVESA Networking Reception & Showcase at CES2022
- **(January 5, 2022 - LIVE in Las Vegas)** Connect2Car at CES2022
- **(November 17, 2021 - LIVE in Novi, MI)** TU Automotive Tech Week (Register at https://covesa2021.eventbrite.com passcode is "collaboration")
- **(October 5-8th, 2021 - Virtual All Member Meeting and Security Team Workshop)**
- **(June 8-10, 2021 - Virtual)** TU Automotive FOCUS: Connected Vehicle Commerce
- **(May 17-21, 2021 - Virtual)** TU Automotive FOCUS: Software Defined Vehicles
- **(May 6, 2021 - Virtual)** COVESA Virtual AMM & Cybersecurity Workshop (see content from workshop below)

Meeting Minutes

- Meeting Notes March 4 2021.pdf
- Meeting Notes January 21 2021.pdf
- Meeting Notes Jan 7 2021 .pdf

Recently Recorded Cybersecurity Talks / Workshops

COVESA Leipzig AMM - Virtual Cybersecurity Workshop Track from April 28, 2022	**VIDEO LINKS**	**SLIDES**	**SPEAKERS**
Title: GENIVI Security Team Overview: **Abstract**: COVESA's Automotive Cybersecurity team continues to lead and provide our membership and greater community with an overview of the cybersecurity team initiatives, how you and your organization can become engaged, and lastly what to look forward to in today's cybersecurity workshop track	**https://ga.wistia.com/medias/85w5bk4db6**	Welcome-Joby-COVESA_Spring_AMM_cybersecurity.pptx	Joby Jester, (COVESA Cybersecurity Team Lead /Capgemini)

Keynote Title: Trust and Security of Software in Connected Vehicles **Abstract:** Code is new fuel for a modern car. It is more dependent on code than petrol. Nowadays, a car is powered by a network of 70 to 100 electronic car units (ECUs) which constantly communicate over Control Area Network (CAN). Indeed, it takes 100 million[1] lines of code for a modern car to function, and it is expected to rise to 300 to 500 million. In contrast, a Boeing 787 Dreamliner runs on 12 million lines of code[2]. The complexity of software in a car and multi-tier supply chain have raised many challenges for quality, functionality and security testing. Moreover, WP.29 regulations by UNECE mandates frameworks essential for connected cars in the area of cyber security and software updates. asvin has designed and developed a novel solution to improve overall DevOps process integrity testing using the distributed and decentralized technologies. It consists of Distributed Software Bill of Materials (D-SBOM)[4] and secure software supply chain services. The D-SBOM service aims to pioneer creation of a list of software constituents, its storage and retrieval using the distributed ledger technology (DLT). Additionally, the objective of secure software supply chain services is to trace the track of software from its development to installation. Each event in the software lifecycle will be recorded on a distributed ledger. Both services will help in establishing an unbroken chain of ownership, software provenance, transparency, security, trust and integrity for DevOps process in automobile industry. A ledger is inherently immutable and secure. Therefore, the solution will strengthen and streamline the process of auditing and compliance adherence set by government and regulatory institutions.	**https://ga.wistia.com/medias/8zgqz1rhyx**	Rohit-Bohara Trust and Security of Software in Connected Vehicles - COVESA22.pdf	Rohit Bohara - Asvin
Title: VSS Meets NDN: Securing Vehicle Communications through Named Data Networking **Abstract:** The Vehicle Signal Specification (VSS) is a standardized vehicle data specification that allows the automotive industry to use a common naming space for communication and abstract underlying vehicle implementation details. A standardized vehicle data specification, however, has significant additional benefits: it can enhance security and efficiency in vehicle communications when coupled with Named Data Networking (NDN) that communicates using names at the network layer rather than endpoint addresses. The use of names enables cryptographically binding content to unique names to build a strong security foundation by only allowing valid content to be delivered and enables efficient content delivery (both unicast and multicast) by allowing the network to locate the nearest source of the requested content and suppress duplicate requests and data. As implemented in NDN, standardized names result in far simpler application implementations by reducing communication complexity and eliminating all address allocation and management functions such as DNS.	**https://ga.wistia.com/medias/btomh344nh**	2022-COVESA-Christos-Papadopoulos.pptx	Dr. Christos Papadopoulos - Professor, University of Memphis
Title: Keep your vehicles safe by continuously managing the software vulnerabilities **Abstract:** Both OEMs and Tier 1/2s need to control vulnerabilities and reduce the costs during development by addressing vulnerabilities as soon as possible. Tier 1s need to provide evidence of proper vulnerability management to OEMs that are required to present for regulatory compliance for type approval. Once the vehicle is on the road, the vulnerabilities need to be continuously monitored and mitigated for detected severe ones. At the end of the day, OEMs want to avoid any reputation damages and huge costs associated with a cyber incident. Gilad Bandel, veteran of automotive cybersecurity will discuss with Eden Ben Shabat, leading automotive cybersecurity analyst, how OEMs and Tier 1/s address those challenges and which course of action is recommended for effective and efficient mitigating those challenges. Field experience, lessons learned, and interesting actual cases will be used to demonstrate the proper process, options available and risks to be avoided.	**https://ga.wistia.com/medias/nxopxfc7kn**	Car Alert - COVESA AMM 2022-Gilad.pptx	Gilad Bandel (Cymotive Technologies)
Automotive Privacy Update for 2022 **Abstract:** There is more data than ever being collected by the OEMs, Tier 1s, and Application and OS providers than ever. Who is responsible for the security and safety of this data? Opt-in or opt-out? Have a seat, grab your tinfoil hats, and listen in as our Security Team Chair, Joby Jester, and resident privacy expert, Jennifer Dukarski, discuss the automotive privacy landscape of 2022 including the biggest issues, regulations, and offer suggestions towards protecting the personal and confidential information on the vehicle.	**https://ga.wistia.com/medias/psof8jla3r**	No Slides - Just Discussion	Joby Jester and Jennifer Dukarski - Butzel Long

October 7, 2021 Cybersecurity Workshop

TITLE (Cybersecurity Workshop Track from October 7, 2021 All Member Meeting)	VIDEO LINKS	SLIDES	SPEAKERS

Title: GENIVI Security Team Overview: **Abstract**: GENIVI's Automotive Cybersecurity team lead provides the audience with an overview of the GENIVI cybersecurity team initiatives, how you and your organization can become engaged, and lastly what to look forward to in today's cybersecurity workshop track			Joby Jester, (GENIVI Cybersecurity Team Lead /Capgemini)
Keynote Title: Creating cybersecurity problems through regulation **Abstract:** There have been a number of regulations in the vehicle space which have created a number of cybersecurity headaches. From the original ODB port to the recent ELD mandate for trucks more and more connectivity is being mandated with little regard for cybersecurity. Where are we now? What is coming next? What should we be looking for to help avoid the problems coming our way?		Creating Cybersecurity Problems Through Regulation.pdf	Urban K. Jonson, (National Motor Freight Traffic Association, Inc)
Title: Fall 2021 Regulatory and Compliance Update **Abstract:** Cybersecurity and privacy concerns have dominated the news cycle in recent months. We've seen everything from the White House and Congress responding to ransomware payment issues to home EV chargers replete with security vulnerabilities. Join the Butzel team to hear the latest changes including regulations, requirements for critical infrastructure, Executive Orders, guidance, and draft bills. We will discuss the issues you need to be prepared for to promote a culture of compliance while meeting new incident reporting obligations and ransom payment guidance.		FALL 2021 REGULATORY AND COMPLIANCE UPDATE.pdf	Claudia Rast & Jennifer Dukarski (Butzel Long)
Title: Counterfeit Modules, Right to Repair, and Cybersecurity Plans, Challenges and Opportunities **Abstract:** Current state of the art allows secure boot of a small subset of modules on the vehicle bus while allowing diagnostic access with very few restrictions. We will explore ways to build a stronger foundation for security, safety, and reliability while sharing the right data and allowing the right R2R!		Counterfeit Modules, Right to Repair, and Cybersecurity Plans.pdf	Chad Childers (Privafy)
Title: Making Sense of Security Testing for ISO/SAE 21434 **Abstract:** Fuzz Testing? Pen Testing? Vulnerability Scanning? Functional Testing? Verification Testing? Whether you're an automaker or supplier, you'll inevitably need to get comfortable with security testing as ISO/SAE 21434 permeates the automotive supply chain. In this talk, we'll walk through each type of testing to discuss what it is, why it's done, and when/how to do it. Finally, we'll end this talk with a few recommendations for ways you can get ahead of the curve and start thinking about automating cybersecurity testing for ISO/SAE 21434		Making Sense of Security Testing for ISO-SAE 21434 and UNR 155.pdf	Brandon Barry, (Block Harbor Cybersecurity)
Title: Cybersecurity Challenges and Implications in C-ITS **Abstract:** ITS ecosystems are the dominant solution to networks' saturation as they provide several benefits. They contribute to congestion reduction, limitation of emissions and air pollution, avoidance of unexpected incidents on the road, and transportation efficiency. However, deploying interconnected Intelligent Transport Systems creates several challenges, mainly in terms of safety and cybersecurity. During this session, the current situation will be presented and discussed, focusing on challenges and issues that need to be studied to address the growing needs of the ICT infrastructure.		CONNECTED AND AUTOMATED VEHICLES.pdf	Gilad Bandel (Arilou Automotive Cybersecurity)
Cybersecurity Staffing Challenges/Wrap-Up **Abstract:** The GENIVI Security Team Lead, Joby Jester wraps up the talks for today and provides additional industry insight and upcoming automotive cybersecurity event opportunities		Security Track Closing.pdf	Joby Jester (GENIVI Cybersecurity Team /Capgemini)

Title (GENIVI Security Team Workshop May 6, 2021)		
GENIVI Security Team Overview **Speaker:** Joby Jester, Solutions Architect at Irdeto and GENIVI Security Team Lead **Abstract:** Welcome everyone, About the GENIVI Automotive Cybersecurity Team, How to get involved and engage with the team, and lastly what the agenda for the day will be	Recorded Session	GENIVI Security Team 1pg.pptx

On Transforming Automotive Cybersecurity: Bridging gaps, Opportunities, and Diversity **Speaker:** Ikjot Saini, Academic Director ASRG And Assistant Professor Academic Network **Abstract:** With the increasing demand for connectivity and the rapidly evolving Autotech sector, cybersecurity concerns have raised exponentially. The global automotive cybersecurity job markets are in a talent crunch and need reskilling, upskilling, and cross-disciplinary competencies to manage the risks in this emerging cyberspace. SHIELD automotive cybersecurity center of excellence at the University of Windsor is dedicated to the development of industry-ready solutions to meet the rapidly changing technology and threats. SHIELD also focuses on training to lower the barrier to entry and create an industry-ready talent pipeline. To enable knowledge transfer and collaborations among research labs at the academic institutions, globally, ASRG is building an academic network for the researchers and graduate students to provide the support network of auto security scholars. One of the important aspects which are often overlooked is diversity at the workplace. In this emerging field, where both automotive and cybersecurity have records of significantly low representation of women, diversity is a major challenge. In 2021, women hold 25% of the cybersecurity jobs globally (source) which has doubled in a decade. While in automotive, the percentage has increased only by 1% from 2014 to 2018(from 7 to 8), with no women on the executive teams of over half of the top 20 companies. The statistics indicate the grim state of the diversity in automotive cybersecurity in the future. This can only be changed by actively and collectively working on diversity and inclusion.	Recorded Session	No slides for this session
The Implications of Biometric Data in the Vehicle **Speaker:** Jennifer Dukarski, Emerging Technology, IP and Media Litigation at Butzel Long **Abstract:** Biometric data includes physical or behavioral human characteristics that can be used to digitally identify a person to grant access to systems, devices or data. In terms of biotechnology in the car, researchers proclaim “give me 10 biometric sensors in the car and I’ll revolutionize healthcare.” But collecting this data comes with a price: enhanced security and privacy protections and regulations. This discussion will look at how global and local legal and regulatory frameworks impact the design, collection, and use of this potential treasure trove of data. This topic will: • Define the scope of biometric data and the regulatory frameworks that apply in the US and internationally • Address regulatory directives for security and privacy with the collection, storage, and use of biometric data	Recorded Session	Biometric Data Presentation Dukarski.pptx
Navigating the Current Threat Environment **Fireside:** Claudia Rast, Department Chair Cybersecurity at Butzel Long, and Scott Bailey Partner at N1 Discovery **Abstract:** It’s hard to overemphasize the importance of maintaining robust privacy and data security measures. Not only are hackers becoming more sophisticated in their offensive weaponry—even harnessing AI to launch their attacks—but with 1 in 4 Americans continuing to work from home through 2021, threat actors have a broad and largely unprotected threat landscape to harvest. In addition, with fewer employees present at any given time in their traditional office environments, physical security is also important. Recent trends include hacking insurance companies to discover those insureds that have sufficient cyber coverage to afford high ransom demands. We will discuss these and other evolving cybersecurity threats that are present today and that we expect in the coming year and will describe the tools and best practices currently available to augment defenses.	Recorded Session	Rast_&_Bailey_Cybersecurity_Roadmap.PPTX

OpenXSAM **Speakers:** Dirk Leopold, Regional Director at itemis AG, Brandon Barry CEO at Block Harbor Cybersecurity **Abstract:** Wouldn't it be nice if you could export cybersecurity data from your TARA tool and import it into your requirement management platform or verification environment? One of the biggest challenges in automotive security is building cohesion between tools to speed up cybersecurity engineering. https://openxsam.io seeks to achieve this by building an open format to exchange security information for vehicles. In this talk, Itemis will give you an introduction to openXSAM and how it's used by their TARA platform. Then, Block Harbor will talk about how they envision their integration of openXSAM into their automotive verification environment. You'll walk away from this talk with new ideas on how you can create a seamless integration between your tools to make your vehicle cybersecurity engineering more efficient and more effective.	Recorded Video	brandonbarry-dirkleopold_openXSAM.pptx
Break with the ASRG introduction Video	ASRG Video	
V2X / Cloud Managed Services Security Trends: **Speakers:** Brandon Barry, Joby Jester **Abstract:** Explore the trends of Automotive Cybersecurity brought to you by ASRG Leadership and the GENIVI Security Team. Chat about the near and far challenges for AV, EV, Mobility, and beyond! Tune in, sit back, and have a chat with us!	Recorded Session	AutomotiveSecurityTrends.pptx

Network Micro-Segmentation Cloaking Technology for Autonomous Vehicles **Speaker:** Will Hill, Security Technologist at CuDes, and Greg Shields, Director at NetFoundry **Abstract:** In this talk, we discuss a zero-trust cybersecurity solution that prevents remote access to any software app by hiding the internet connection to this app. Because a hidden-, cloaked-, dark-connection is used, the attack hackers cannot find what does not exist. A user can also implement micro-segmentation such that one software app can only talk to one other software app. The software app can be in the cloud or one app of many apps running on any device with an application processor. Simply put, any app which calls to the internet will be completely hidden from remote access. This is all orchestrated from the cloud as a 100% software solution and no hardware is involved whatsoever. It is free to prototype, right now, via the open-source community.	Recorded Session	NetworkMicroSegmentation_Day3_Slides
Automotive Security Hacking & Protection Practice **Pre-Recorded:** Vincent Zhang - Senior Security Architect at Tencent **Abstract:** Since the globally recognized “Tesla Model S remote hacking” public research in 2016, Tencent Security Keen Lab has conducted more than 30 connected vehicle security research projects with industry-leading OEMs. This presentation will illuminate common automotive security threats and attack chains based on our rich research experience, as well as mitigation & protection best practices.	AutomaticSecurityHacking&ProtectionPractice	No slides for this session
Automotive Ethernet Specific Cybersecurity Protection Solutions with IDS/IPS) **Speaker:** Gilad Bandel, VP Product & Marketing at Arliou Automotive Cybersecurity **Abstract:** The automotive industry is swiftly moving towards automotive Ethernet as the new in-vehicle network core. This technology comes with many new features and benefits, but it also comes with numerous legacy risks from the traditional IT Ethernet landscape, as well as from new, error-prone software that is developed. Automotive Ethernet risks need to be mitigated, with security and protection incorporated into new devices. This lecture will detail solutions to address and mitigate those threats and focus on IDS/IPS required functionality.	Recorded Session	No slides for this session

Previous GENIVI Virtual Cybersecurity Talks

Titles from Oct 28th Cybersecurity Workshop during AMM	Video Links / Session Playback	Slides
GENIVI Cybersecurity Industry Focus	Recorded Session	pptx
Cybersecurity Industry Focus by Strategy Analytics	Recorded Session, Record Session (pt 2)	pptx
An Alternative Universe without Collaboration	Recorded Session	pptx
Data Privacy for Automotive	Recorded Session	
ISO 21434 / UNECE WP.29 Update w/OEM Partners	Recorded Session	
Increased Complexity of Cybersecurity Controls Due to Consolidation of Connected Modules	Recorded Session	
Perception vs. Reality: How Lack of Collaboration Leads to False Perceptions By Media And Academia	Recorded Session	
Vehicle Forensics - Digital Evidence from infotainment Systems	Recorded Session	pdf

Recent space activity

michael nunnery
COVESA In-Vehicle Payment (SIG) updated Jun 28, 2023 view change

Paul Boyes
VSS to AOSP translation - WBS updated Feb 21, 2023 view change

Karin Hanson
Android Automotive SIG home updated May 19, 2022 view change

michael nunnery
Automotive Cybersecurity Team Home updated May 11, 2022 view change

Paul Boyes
Android Automotive OS Problems and Opportunities updated Apr 27, 2022 view change

Space contributors

- michael nunnery (738 days ago)
- Joby Jester (1039 days ago)
- Vincent Zhang (1165 days ago)
- Nicholas Contino (1489 days ago)
- Gunnar Andersson (1520 days ago)
- ...