SANS

Automotive Cybersecurity
Summit 2018

@SANSInstitute #SANSAutoSummit

Agenda

All Summit Sessions will be held in the Chicago River Ballroom (unless noted).

All approved presentations will be available online following the Summit at
https://www.sans.org/summit-archives/cyber-defense

Sunday, May 6

7:00-8:00 pm

Bonus Session –
Lifting the Sheets on Automotive Embedded Control

A car hacking lab requires more blood and sweat than spinning up a few VMWare images, so we decided to build our own. Come join us as we talk about the surprises and pitfalls we found hiding inside of a real car as we surgically removed its electronic systems from its mechanics. See first-hand the specialized embedded devices and interconnected systems that are widely used inside vehicles that are on the road today. Learn about the mix of old and new technologies, the manufacturer's challenge to balance competing needs, and also some key observations we made about simple network redesign techniques that can reduce security risks. You'll get to see, up close, GRIMM's unique 3PO Car Hacking Lab demo and you might even get a chance to play.

Tim Brom*, Security Researcher, GRIMM*

Monday, May 7

7:00-8:30 am

Registration & Coffee (LOCATION: PRE-FUNCTION BALLROOM AREA)

8:30-9:15 am

Security, Safety, and Self-Driving Cars

Self-driving cars are hackable computers that move fast, weigh a ton and can run into things. From a security standpoint, it would be most prudent to keep them as far away from the Internet as possible. Unfortunately they not only rely on up-to-date information from the cloud, like detailed maps or infrastructure information; true "self-driving cars" will also require the ability to be teleoperated, at least for quite some time after their market introduction. One way or another, Internet connectivity for these devices is inevitable. This makes them a prime target for high-security applications.

We will examine what requirements for connectivity exist today and will probably exist in the future, and how access to self-driving vehicles can be limited to the barest minimum; possible scenarios for hacked self-driving cars and their impact; how functional safety is handled in the automotive industry, and what possibilities this entails for automotive security.

Bjöern Giesler*, Head of L4 Autonomous Driving Functions bei ZF Group*

Monday, May 7

9:15-10:00 am

Security Considerations for Connected Autonomous Vehicles

The automotive landscape has drastically changed with respect to cybersecurity over the last few years, and autonomous vehicles will need to address the challenges presented by current and future autonomous vehicle technologies such as infotainment units, telematics, and sensors. As vehicles become more and more connected, they also become more and more open to the possibility of cyber threats. To this point, researchers have developed methods to exploit vulnerabilities involving multiple vehicle sensors. The applicability of these vulnerabilities is not limited to the local vehicle sensors, but also to their telematics technologies that connect them via Vehicle-to-everything (V2X). As these technologies become more commonplace, researchers will undoubtedly continue to find vulnerabilities in the vehicles of tomorrow, and these vulnerabilities must be analyzed for appropriate fixes, when applicable, or countermeasures. This presentation discusses the cybersecurity concerns of autonomous vehicle technologies, and describes how a defense-in-depth approach is crucial to securing connected autonomous vehicles.

***Abe Garza**, Research Engineer – Embedded Systems Security Group, Southwest Research Institute*

10:00-10:20 am

Networking Break (LOCATION: PRE-FUNCTION BALLROOM AREA)

10:20-11:05 am

ISO/SAE 21434 WIP: Overview of Work to Create the First Standard for Automotive Cybersecurity

The Society of Automotive Engineers (SAE) and the International Standard Organization (ISO) are working together to create a standard for automotive cybersecurity that will be jointly released by each organization. Will discuss: agreement between SAE & ISO; structure of ISO/SAE teams; participating companies, universities, etc., benefits of Standard for automotive cybersecurity, summary of planned content of standard, and timeline for activity. Known connections with other existing and in-process standards, best practices, policies and guidelines.

***Angela Barber**, Senior Advisor, Product Cybersecurity for Mitsubishi Motors R & D of Americas; SAE member of Joint Working Group for ISO/SAE 21434*

11:05-11:50 am

Fortifying the Security Assurance Process Using Software Composition Analysis

As modern automobiles become increasingly connected, the need for proactive cybersecurity practices grows stronger. The impact of exploitable vulnerabilities in a vehicle may completely compromise its functional safety and put passengers at serious risk. One major source of these vulnerabilities is the use of open-source software, so software composition analysis (SCA) becomes an essential cybersecurity assurance step in the software development process. SCA tools identify vulnerabilities associated with open-source software components using the National Vulnerability Database managed by NIST. Three tools were evaluated based on a sample software project and manual post-processing of the results. Issues discovered during evaluation included: false identification of scanned components, incorrect version number, incomplete coverage, and other extraneous data. Due to these issues, it is not readily apparent which tool best meets our needs. Therefore, we developed an assessment approach to rate the effectiveness of each tool. Attendees can expect to learn the value and basic concept of available SCA tools, along with our assessment approach. Although the names of the tools will be anonymized, the metrics used in our assessment approach will aid attendees in performing their own evaluation of SCA tools.

***Jason Gay**, Cybersecurity Engineer, Magna Electronics*

Monday, May 7

11:50 am – 12:35 pm

Automotive Critical Controls: A Mapping of CIS Critical Controls to Automotive Cybersecurity

The Center for Internet Security (CIS) Critical Controls provides a short list of recommended “must do, do first” cyber defense actions to thwart today’s most pervasive and dangerous global enterprise Internet attacks. Organizations and publications including the U.S. National Institute of Standards and Technology (NIST), European Telecommunications Standards Institute (ETSI), and topically the U.S. National Highway Traffic Safety Administration’s (NHTSA’s) “Cybersecurity Best Practices for Modern Vehicles” each reference and endorse the CIS Critical Controls. As a bridge between framework and implementation, advocates and users appreciate the tangible, applicable examples prevalent in Critical Control case studies. In practice, application of some of the twenty Critical Controls to automotive cybersecurity efforts is straightforward, with readily available enterprise implementations for reference. However, automotive nuances regarding lifespan, connectivity, processing resources, and safety often necessitate alternative views and reference implementations when applying many of said Critical Controls. This presentation provides a mapping of contemporary automotive cybersecurity mechanisms to the twenty CIS Critical Controls. It supports this mapping with an elaboration of traditional Internet versus automotive similarities and differences, while presenting examples of automotive implementations of each Critical Control. The presentation also aids topical application via added focus on Critical Control implementations with significant automotive versus enterprise differentiation. Following this presentation, audience members will gain a list of automotive cybersecurity mechanisms, each being an application of a case study example of one or more Critical Controls. Audience members may then use the resultant mapping for assistance in proactively prioritizing “must do, do first” automotive cybersecurity protections as outlined by the Center of Internet Security and endorsed by NIST, ETSI, and NHTSA among others.

Dave Bares*, Cybersecurity Senior Engineer, Lear Corporation*

12:35-1:45 pm

Lunch

1:45-2:30 pm

Assuring and Insuring Automotive Cyber Risk

Thatcham Research are UK-based experts in automotive security, safety and repair, funded by the UK motor insurance industry to research these areas and provide insight to allow insurers to control costs and understand underwriting risk, as well as providing consumer advice and awareness. Thatcham’s work in the security sector over the last 25 years has been a major contributor to the reduction in vehicle theft. 620,000 vehicles were stolen in the UK in 1992. Currently, the UK experiences only 90,000 annual thefts. This has been achieved by understanding the threat landscape through collaboration with law enforcement, and physically assessing every new vehicle and feeding the results into the insurance group rating system in order to motivate manufacturers to continuously develop their vehicles to address the evolving threat. Thatcham works closely with the OEMs to assist in their development cycle and provides guidance on current and future elements of the assessment profile. With the emerging threat of automotive cybercrime, Thatcham is enhancing our knowledge and capability in this area, including collaborating with cyber and automotive industry partners to develop a framework for the assessment of the cyber risk of vehicles, to inform the insurance industry and provide information to consumers. This project will draw on Thatcham’s experience in the design and implementation of vehicle security assessment systems, to ensure that the processes are as effective at tackling cyber crime as they have been for controlling traditional vehicle security threats.

Richard Billyeald*, Chief Technical Officer, Thatcham Research UK*

Monday, May 7

2:30-3:15 pm

Zombie Car-pocalypse: Protecting Legacy Connected Vehicles

For the past decade, we have been demanding and purchasing increasingly connected vehicles. Long before the Jeep hack, cellular devices were being installed in modern vehicles. Even in the midst of current security awareness trends, many future questions are left unanswered. This panel will address these difficult questions:

- How can we secure already-shipped vehicles designed before secure segmentation was a value-add?
- How long will vendors provide security updates to ECU firmware?
- How will we continue to drive cars securely past their expiration date?

MODERATOR:
Doug Wylie*, CISSP, Director – Industrials & Infrastructure, SANS Institute*

PANELISTS:
Kevin Baltes*, Director & CISO – Product Cybersecurity, General Motors Company*
Matt Carpenter *(@Ma77Carpenter), Principal Researcher, Grimm*
Urban Jonson*, Chief Technology Officer, National Motor Freight Traffic Association, Inc. (NMFTA)*
Suzanne Lightman*, Sr. Advisor, Information Security, Computer Security Division, National Institute of Standards Technology (NIST)*

3:15-3:35 pm **Networking Break** (LOCATION: PRE-FUNCTION BALLROOM AREA)

3:35-4:05 pm

Large-Scale Attack Trees Applied to Connected Transport Systems: Case Studies

Engineers are subject matter experts for the systems they design. As a result, they are the most qualified to understand the data flow relationships in these systems. This is a key part of threat modeling software. In order to successfully identify the security needed to effectively protect the system, engineers must threat model early on in the design process to yield a much more robust and resilient system. This session will provide engineers with training on threat models and large-scale attack trees. This presentation will also give engineers that are interested in securing their systems, but with little to no knowledge of threat modeling, the understanding necessary to perform attack tree analysis. The session will also share a handful of sample attack trees with attendees. All parties involved will be kept anonymous, so the specifics of some parts of the attack trees will be more vague than would otherwise be modeled. As the goal of attack trees includes modeling the relative impact of mitigations (which will be covered in detail during the presentation), the focus on the review of attack trees will be on the marginal benefits of mitigations, as modeled in these connected systems. Attendees should leave the presentation with a better understanding of the marginal benefits of some mitigations, as captured by the model, including anti-debugging, anti-reverse engineering, integrity- verification, anti-exploitation, data transformation, certificate pinning, data encryption at rest, kernel hardening, etc. We'll also examine the pitfalls in large-scale attack tree modeling and share open source tools available to perform attack tree modeling.

Ben Gardiner*, Principal Security Engineer, Irdeto*

Monday, May 7

4:05-4:50 pm

Don't Reinvent the Wheel; Re-use It

Connected and autonomous vehicles bring new attack surface, vulnerabilities, and risks to the industry. But at their core, vulnerabilities are simply defects and automotive manufacturers already know how to manage defects. This talk will speak to how to leverage existing non-security capabilities and core competencies to help reduce security challenges in automotive products. From requirements creation and management to quality control, Rob and Phil will illustrate that connected vehicle cybersecurity doesn't require a broad swath of new capabilities, but can be done largely with existing capabilities.

Rob Shein*, Manager – Cybersecurity and Privacy, PricewaterhouseCoopers Advisory Services LLC*

Philip Swarbrick*, Director – Cybersecurity and Privacy, PricewaterhouseCoopers Advisory Services LLC*

4:50-5:35 pm

Everything You Wanted to Know About Retail but were Afraid to Ask

It's no secret that our industry tends to be siloed when it comes to designing and manufacturing vehicles versus selling and servicing them. But those silos can lead to security vulnerabilities if we don't all work together to secure the entire industry – the entire supply chain – from OEM and Tier I all the way to the dealer and the customer on Main Street USA. Manufacturers often feel they have little control over the dealership environment, and dealers often say the same about the vehicles they're shipped to sell. So what does the dealership environment look like? What are the issues in retail that you need to be considering when securing not just the car, but the industry? We – an OEM, a dealer, a technology provider, and a leading industry non-profit – will detail our shared insight into the world of automotive retail. We'll also share what you can achieve when you break through the silos and work together in partnership to better secure the industry.

Lisa Plaggemier*, Director, Risk, Culture of Security, and Client Advocacy, CDK Global*

5:35-7:00 pm

Networking Reception (LOCATION: PRE-FUNCTION BALLROOM AREA)

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Tuesday, May 8

7:00-8:30 am

Registration & Coffee (LOCATION: ROCK RIVER I & II)

8:30-9:15 am

Preparing for the Autonomous/Connected Vehicle Future: Los Angeles Case Study

Los Angeles pioneered traffic signal automation in the early 1980s in preparation for the 1984 Olympic Games. Today, the city's Automated Traffic Surveillance and Control Program (ATSAC) is believed to be one of the largest urban traffic control automation systems of its kind in the world and has endured for more than 30 years. But as the city prepares for a future that includes connected and automated vehicles, cybersecurity is a key challenge. This presentation will focus on the recent work the city has engaged in to prepare for the connected and automated vehicle future, its approach to technology innovation, partnership developments, and some key considerations as it seeks to mitigate cyber risk. This is especially timely as Los Angeles prepares for another Olympics in 2028.

Michael Lim*, Partner, Public Worx; Executive Advisor (former), City of Los Angeles Department of Transportation*

9:15-10:00 am

Smart Cities, and What They Mean to Smart Vehicles and Smart Infrastructures

Smart cities present tremendous opportunities for industrial IoT vendors, but the technical challenges, vast number of players in this ecosystem, and the fact that it bridges private, public, and consumer realms makes navigating and succeeding in this market a challenge. Cybersecurity, connectivity and working with municipal bureaucracy remain the biggest challenges, but other obstacles include; exponential data volume growth, data cleansing speed, the need to go from cloud to edge architectures, quantifying results, interoperability, and human fears/resistance to transformational change such as Artificial Intelligence. Smart Transportation is one of 12 key smart city application sectors the ARC Advisory Group has identified. This session will discuss the trends that are driving the rapid emergence of Smart Cities and include particular focus on how connected vehicles will interact with these emerging systems infrastructure.

Sid Snitkin*, VP Cybersecurity Services, ARC Advisory Group*

10:00-10:25 am

Networking Break (LOCATION: PRE-FUNCTION BALLROOM AREA)

10:25-11:10 am

Deploying Uptane Onto Production Infrastructure

Vehicle manufacturers are looking to employ wireless frameworks to update vehicle firmware without inconvenient trips to a dealer or expensive individual mailers. The ability to distribute patches silently and to quickly combat cybersecurity threats and protect brand image is becoming increasingly urgent. However, deploying a method for firmware updates over-the-air (OTA) securely presents several extremely challenging logistical and technical obstacles. With the ever-increasing role that software plays in vehicle safety, secure OTA updates are necessary for the next generation vehicle. The OTA framework (Uptane) has been created through an industry and academic cooperative funded by the Department of Homeland Security (DHS). Uptane is an open source, auditable, and secure method of firmware delivery that solves many of the logistical and technical challenges of distributing updates over an unprotected infrastructure. This talk will discuss deploying the Uptane framework onto production infrastructure, including the lessons learned and best practices to incorporate when deploying an OTA framework. Additionally, this talk will highlight the risks posed to the OTA framework that arise from common server configuration, management, and logging tools. Lastly, attendees will walk away with an actionable plan on how to have their OTA framework, including its infrastructure, tested to ensure all attack paths are assessed.

Allen Cain*, Research Analyst, Southwest Research Institute*

Tuesday, May 8

11:10-11:55 am

Electric Vehicle Charging System Standards and Security

Present-day Electric Vehicle (EV) charging systems include dispensers for service delivery; applications allowing drivers and station owners to configure, monitor and control services; and a cloud-based management system that brings all the parts and data together. At this stage, these are traditional thick client/server systems with a mix of machine-to-machine and point-of-sale functionality; there is little if any communication or integration with other local devices. Not surprisingly, commercial networks supporting monetary and/or legal transactions have the highest levels of device and system sophistication.

Since EV charging systems manage the delivery of electricity at increasingly high levels of power and energy, they're also emerging as critical cyber-physical systems. To date, standards for EV charging systems have focused almost exclusively on the dispenser's electrical interfaces: ingress (connection to AC supply) and egress (connection to the EV), with a strong emphasis on safety. While there are also standards for EV-charging station communication, infosec concerns haven't been material – the vast majority of charging sessions are controlled by analogue circuitry that's not susceptible to cyber-attack. Between charging station and cloud (management system), standards-based cybersecurity measures (e.g. PCI DSS) are mandated only when the station has Point of Sale capabilities. However, the industry is at a turning point and a thoroughgoing, systematic approach to infosec management is now a critical necessity. In this session, I'll provide an overview of current EV charging system architecture and standards. I'll then describe a set of emerging standards (IEC/ISO 15118, IEC 63110, IEC 63119, NEMA EVSE 1.2) that introduce new actors, agency, architectural levels, systems and interfaces and greatly expands the threat surface of EV charging systems. I'll characterize and analyze the associated vulnerabilities and proposed controls, and begin a discussion about ways that the infosec community can help to influence and improve the security design of next-generation EV charging infrastructure.

Craig Rodine*, Director – Standards, ChargePoint, Inc.*

11:55am-12:25 pm

Connecting the Community: Auto-ISAC's Role in the Automotive Industry

Today's automobiles are constantly evolving to accommodate rapid changes in connectivity and autonomy technology, enabling safer, cleaner, more fuel efficient, and smarter vehicles. Increasingly, these connected vehicles require Original Equipment Manufacturers (OEMs) and other automotive industry stakeholders to adapt to emerging cyber security threats. Automakers are taking many actions, including implementing security features in every stage of the design and manufacturing process, collaborating with public and private research groups to share solutions, and participating in multiple cyber forums on emerging issues. In anticipation of these threats, key stakeholders in the automotive industry united to develop an Automotive Information Sharing and Analysis Center (Auto-ISAC) to improve cybersecurity threat awareness and coordination across the global industry.

The Auto-ISAC is a trusted, sector-specific membership organization that provides operational capabilities that include the collection, analysis, and dissemination of alerts, incident reports, and other intelligence regarding cyber and physical threats and vulnerabilities. It provides an electronic, trusted portal for its membership to exchange and share information on threats that assist the membership in defending respective components of critical infrastructure.

This presentation will describe the role of the Auto-ISAC and its success as measured by several factors including growing membership and fostering a trusted environment to enable vibrant information sharing across the globe. It will discuss the governance, leadership structure and decision-making model the organization employs to handle automotive industry issues as they arise, including the Auto-ISAC's supporting role in coordinated vulnerability disclosures and industry-wide incident response plans.

Faye Francy*, Executive Director, Auto-ISAC*

12:25-1:30 pm

Networking Lunch (LOCATION: PRE-FUNCTION BALLROOM AREA)

Tuesday, May 8

1:30-2:00 pm

I Am, Therefore IR

This session is an in-flight analysis of one OEM's evolving IR journey, from initial overload to a recent IR reckoning. GM's Product Cybersecurity IR manager will provide a quick overview of lessons learned since program inception.

***Matt Mackay**, Senior Risk Manager – Product Cybersecurity, General Motors*

2:00-2:45 pm

Panel: Automotive Cybersecurity Incident Response: Preparing for When, Not If

Locked inside your vehicle…hot air and heated seats won't shut off…brakes won't fully engage… steering wheel starts to shake…dashboard goes dark…you've just entered a school zone. And, the radio starts to play disco music! Now you know, your car has just been hacked.

The best minds in the Automotive Industry are hard at work to help protect the connected mobile assets we rely on to move us from point-A to point-B, to safeguard our most precious cargo as well as other people in our surroundings. The adage of "When, Not If" is an unfortunate reality that spans the digital world and it equally applies to our connected vehicles, roadways and critical infrastructures. As the industry balances consumer demands with laws and regulations, it continues to accelerate down a road that requires more than ever for it to Identify, Detect and Protect owners and operators against known and unknown security threats. Success will never be an absolute here. Vigilance and forward thinking are required by companies and the industry to be prepared for a time when the inevitable will happen—when it becomes necessary to execute cybersecurity incident Response and Recovery activities at scale. These are the fundamental building blocks of an effective incident response program.

In this session, we will start a lively discussion with our expert panelists to explore the scope of the cyber physical security challenges the Automotive Industry is sure to face with connected vehicles and connected infrastructures. What might we expect should an isolated incident grow into an all-out broad-scale attack? How are manufacturers and others preparing for the inevitable car or truck hack? Who will have the authority to take action and set priorities to help the public? How will accurate, timely, and trustworthy information be circulated to those who need it? What's the expected role of the government? What might a containment strategy for a V2X event look like in real-time? Who will be blamed and held accountable? How might consumers, law enforcement and the media react? What will matter more in the heat of the moment, careful forensics or just getting the traffic moving again? All of this is fair game for the panel, but don't necessarily expect answers to every question.

Moderator:
***Doug Wylie**, Director, Industrials & Infrastructure Portfolio, SANS*

Panelists:
***Faye Francy**, Executive Director, Automotive-ISAC*
***Suzanne Lightman**, Sr. Advisor, Information Security, Computer Security Division, National Institute of Standards Technology (NIST)*
***Matt Mackay**, Senior Risk Manager – Product Cybersecurity, General Motors*

2:45-3:15 pm

Networking Break (LOCATION: PRE-FUNCTION BALLROOM AREA)

Tuesday, May 8

3:15-4:00 pm

Automotive Cybersecurity, the C-suite, and You

Organizations in the automotive industry face many cyber risks, from hacks against connected vehicles to disruption of manufacturing or theft of Intellectual Property. Risks can exist across the enterprise and supply chain. To manage all these cybersecurity risks, organizations need a coherent, whole-of-enterprise strategy that engages teams across the c-suite, from info sec and physical security to the counsel's office, procurement, human resources, communications, and more, all with management by the CEO and oversight by the board. But communicating these risks to the c-suite and board is hard because they can be highly technical and difficult to quantify due to lack of historic data. This presentation will provide actionable recommendations and best practices that infosec professionals can use to communicate effectively with the c-suite and board. Examples may include reporting dashboards, stories, and strategies for persuading executives.

Emilian Papadopoulos*, President, Good Harbor*

4:00-4:45 pm

Vehicle Forensics: Infotainment & Telematics Discussion and Demo

The automotive industry is one of the leading industries in the world, topping $2.6 trillion in annual sales. Over the past several years, automotive manufacturers have been adding advanced technology to seamlessly and safely integrate access to our digital lives from within our vehicles. The industry is evolving from making vehicles that simply take us from one destination to another, to vehicles that create an experience that entertains and informs us, all while facilitating voice and data communications as we travel.

With continued consumer demand of these sophisticated infotainment and telematics systems, the forensic benefit lies in the storage of vast amounts of data such as logging vehicle routes, odometer readings, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and in some cases velocity logs indicating hard braking and hard accelerations. Several vehicle systems also record vehicle events such as gear shifts, when and where a vehicle's lights are turned on, which doors are opened and closed at specific locations, and even where the vehicle is when and where Bluetooth or WiFi connections occur. All of this data can be critical evidence in an active investigation.

Ben LeMere*, CEO, Berla Corporation*

Tuesday, May 8

4:45-5:30 pm

When CAN CANT

The Controller Area Network (CAN) bus has been mandated in all cars sold in the United States since 2008. But CAN is terrible in many unique and disturbing ways. CAN has served as a convenient punching bag for automotive security researchers for a plethora of reasons, but all of the available analysis tools share a shortcoming. They invariably use a microcontroller with a built-in CAN peripheral that automatically takes care of the low-level (ISO layer 1 and 2) communication details, and ensures that the CAN peripheral plays nicely and behaves at those low levels. However, a good hardware hacker understands that the sole purpose of the electron is to be bent to our will, and breaking assumptions by making “That CANT happen!” happen is a surefire way to find bugs.

CANT is a (partial) CAN bus peripheral implemented in software that allows security researchers to exercise the electrical bus-level error handling capability of CAN devices. The ability to selectively attack specific ECUs in a manner that is not detectable by automotive IDS/IPS systems (see ICS-ALERT-17-209-01) is invaluable to automotive security researchers as more automakers integrate advanced security measures into their vehicles.

Tim Brom, *Security Researcher, GRIMM*

Mitchell Johnson, *Security Research, GRIMM*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.