We strive to present the most relevant, timely and valuable content. As a result, this agenda is subject to change. Please check back frequently for changes and updates.

### Sunday, May 6th

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:00–8:00 pm</td>
<td><strong>Bonus Session</strong>&lt;br&gt;<em>Lifting the Sheets on Automotive Embedded Control</em> Systems&lt;br&gt;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 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 re-design 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.&lt;br&gt;&lt;br&gt;<em>Tim Brom, Security Researcher, GRIMM</em></td>
</tr>
</tbody>
</table>

### Monday, May 7th

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30–9:15 am</td>
<td><strong>Security, Safety, and Self-Driving Cars</strong>&lt;br&gt;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.&lt;br&gt;&lt;br&gt;<em>Bjoern Giesler, Head of L4 Autonomous Driving Functions bei ZF Group</em></td>
</tr>
<tr>
<td>9:15–10:00 am</td>
<td><strong>Security Considerations for Connected Autonomous Vehicles</strong>&lt;br&gt;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...</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Abstract</th>
</tr>
</thead>
</table>
| 10:20-11:05  | **ISO/SAE 21434 WIP -- Overview of work to create 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  | **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 |
| 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 provide 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 elaboration of traditional Internet versus automotive similarities and differences, while presenting example 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 application case study examples 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 (i) outlined by the Center of Internet Security and (ii) endorsed by NIST, ETSI, and NHTSA among others.

Dave Bares, Cybersecurity Senior Engineer, Lear Corporation

12:35-1:45 pm  Lunch & Learn Sessions

1:45-2:30 pm

Assessing and Mitigating the Risk of Automotive Cyber Crime
Thatcham Research are UK-based experts in automotive security, safety & 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 from 620,000 vehicles stolen in the UK in 1992 to the current level of around 90,000 – a reduction of 85%. 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 work closely with the OEMs to assist in their understanding of the security assessment and how it fits within their development cycle, as well as providing guidance on current & future elements of the assessment profile. With the emerging threat of automotive cybercrime, Thatcham are enhancing our knowledge & 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
Panel

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 chew on 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)

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

Irdeto’s cloakware for automotive program has had the distinct pleasure of collaborating with suppliers and OEMs to model attacks on their systems and to use these models to prioritize mitigations for their systems. Irdeto is a solutions provider; however, we provide this service for selected partners to help them plan the application of the mature security technologies from other industries. It is a process which Irdeto has used internally to develop its own security products. In our capacity as experts on the subject of large-scale attack trees and risk modeling using this tool we would like to 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, such as: 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
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
</table>
| 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 verses 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 St. 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 |

#SANSAutoSummit @SANSInstitute
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30-9:15 am</td>
<td><strong>Risk and the Future of Autonomous/Connected Vehicles</strong>&lt;br&gt;Los Angeles pioneered traffic signal automation in the early 1980s in preparation for the Olympic Games. Today, the City's Automated Traffic Surveillance and Control Program (ATSAC) is believed to be the largest urban traffic control automation of its kind in the world and has endured for more than 30 years. But as the City prepares for the future that includes connected and automated vehicles, cyber security is a key challenge. The presentation would focus on the technology future the City envisions and some of the key considerations as it seeks to mitigate cyber risk. This is especially timely as LA prepares for another Olympics in 2024.&lt;br&gt;&lt;br&gt;<strong>Michael Lim, Los Angeles DOT</strong></td>
</tr>
<tr>
<td>9:15-10:00 am</td>
<td><strong>Smart Cities, and What They Mean to Smart Vehicles and Smart Infrastructures</strong>&lt;br&gt;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 infrastructures.&lt;br&gt;&lt;br&gt;<strong>Sid Snitkin, VP Cybersecurity Services, ARC Advisory Group</strong></td>
</tr>
<tr>
<td>10:00-10:25 am</td>
<td><strong>Networking Break and Vendor Expo</strong></td>
</tr>
<tr>
<td>10:25-11:10 am</td>
<td><strong>Deploying Uptane Onto Production Infrastructure</strong>&lt;br&gt;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 quickly to combat cybersecurity threats to 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 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</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:10-11:55 am</td>
<td>Electric Vehicle Charging System Standards and Security</td>
</tr>
</tbody>
</table>

**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 bring 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 cyber-security 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 expand the threat surface of EV charging systems. I’ll characterize and analyze the associated vulnerabilities and proposed controls, and invite discussion of 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.**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:55am-12:25 pm</td>
<td>Connecting the Community: Auto-ISAC’s Role in the Automotive Industry</td>
</tr>
</tbody>
</table>

**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 cyber security 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 its respective components of critical infrastructure.

This presentation will describe the role of the Auto-ISAC and 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**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:25-1:30 pm</td>
<td>Networking Lunch &amp; Vendor Expo</td>
<td></td>
</tr>
<tr>
<td>1:30-2:00 pm</td>
<td>I Am, Therefore IR</td>
<td>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. <strong>Matt Mackay, Senior Risk Manager – Product Cybersecurity, General Motors</strong></td>
</tr>
</tbody>
</table>
| 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 (IR) 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 hold 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:**
- Ford Motor Company
- Faye Francy, Executive Director, Automotive-ISAC
- Matt Mackay, Senior Risk Manager – Product Cybersecurity, General Motors

### 2:45-3:15 pm

**Networking Break and Vendor Expo**

### 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 dollars in annual sales. Over the past several years, automotive manufactures 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 as well as facilitates voice and data communications while 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*

---

**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 researches 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*
Speaker & Advisory Board Biographies

Dave Bares, Cybersecurity Senior Engineer, Lear Corporation
Dave Bares is a Vehicle Cybersecurity Senior Engineer at Lear Corporation. Before joining Lear, Dave retired as a Lieutenant Colonel in the Air Force and was a Vehicle Cybersecurity Strategist at Fiat Chrysler Automobiles. Lastly, Dave is a CISSP with advanced degrees in Computer Engineering and Cyber Operations.

Kevin Baltes, Director & CISO – Product Cybersecurity, General Motors Company
Kevin Baltes was named Director and CISO, Product Cybersecurity, for General Motors Company effective April 1st, 2015. Baltes is responsible for leading the global team that is defining the strategies to reduce the risks associated with cybersecurity threats related to the vehicle and its components and services. His team manages the cybersecurity posture of the end-to-end connected vehicle ecosystem, including the electronic control modules, IT back office, telecom channels, mobile apps, and connected services such as telematics, infotainment, app shop, and V2X.
Prior to this role, he served as Engineering Group Manager, Vehicle Cybersecurity. During his time in this role, Baltes led the development of the in-vehicle cybersecurity technical solution. Joining GM in 1995 as an Embedded Controls and Software Engineer, Baltes has held multiple roles in Powertrain Engineering, Electrical, IT, and R&D. He holds 12 US patents, and several are pending. Kevin earned a Bachelor’s Degree in Electrical Engineering from the University of Dayton, and a Master’s Degree in Engineering from Rensselaer Polytechnic Institute. Kevin is a Certified Information Systems Security Professional (CISSP). He lives in Michigan with his wife. He enjoys live music and travelling.

Angela Barber, Senior Advisor, Product Cybersecurity for Mitsubishi Motors R & D of Americas; SAE member of Joint Working Group for ISO/SAE 21434
Angela Barber has been working in Automotive Cybersecurity since 2012, and is one of the authors of SAE J3061. She was selected by the SAE Vehicle Cybersecurity Systems Engineering Committee as an SAE expert member of ISO/SAE Joint Working Group (JWG) that’s creating the first automotive cybersecurity standard. She is also Secretary for ISO/SAE PG1 working on the "Risk Assessment" content for the Standard. Ms. Barber is the "Senior Advisor, Product Cybersecurity" with Mitsubishi Motors Research & Development of America, and is Mitsubishi Motors’ Auto ISAC alternate Board member.

Paul Bierdeman, Senior Engineer, Caterpillar Inc.
Paul Bierdeman, a senior engineer at Caterpillar Inc. in Peoria, Illinois, serves as technical steward for embedded security. His focus is software and hardware security architecture for next generation embedded control platforms and systems. Paul joined Caterpillar in 1979, and has worked on such projects as: industrial facility energy management, vital information management data analytics, autonomous haulage in mines, and hardened embedded network gateway. His passions include renovating British sports cars, canoeing the boundary waters and coaching FIRST Robotics Lego League.

Richard Billyeal, Chief Technical Officer, Thatcham Research UK
Richard joined Thatcham Research from Williams Advanced Engineering in 2017, bringing 20 years’ experience delivering cutting-edge engineering programmes across a variety of sectors. He is responsible for all of the organisation’s operational engineering functions, and leads research into physical & cyber security, and repair technologies.

Lisa Boran, Manager – Vehicle Cybersecurity, Ford Motor Co.
Lisa Boran is the Vehicle Cybersecurity Manager at Ford Motor Company focused on defining and instituting security functions within Product Development embedded systems (both cybersecurity and traditional security). Lisa has a MS from University of Michigan in Control Theory and a BS from Wayne State University in Electrical Engineering. Lisa has over 26 years at Ford including a wide variety of roles but mostly in the security

#SANSAutoSummit  @SANSInstitute
area. External to Ford, she chairs both a SAE and SAE/ISO Committee to develop a Vehicle Cyber Security Systems Engineering Process standard.

**Tim Brom, Security Researcher, GRIMM**
Tim Brom is a security researcher at GRIMM, specializing in automotive vulnerability research. His background includes specialized embedded software development, with a particular focus on the automotive and safety industries as well as background in other sectors including safety critical aerospace, and industrial control systems. He has contributed extensively to GRIMM’s open source “CanCat” CAN bus reverse engineering tool and on “3PO,” GRIMM’s mobile auto-hacking demonstration. Tim has also had publications about car hacking tools and techniques, like the recent Macchina M2.

**Allen Cain, Research Analyst, Southwest Research Institute**
Allen Cain is a Research Analyst at Southwest Research Institute in the Embedded Systems Security Group. Allen has worked on cybersecurity projects in industries ranging from medical, oil and gas, to automotive. Recently, Allen’s work has focused on cybersecurity of connected automotive ECU’s, autonomous vehicle sensors, and secure over-the-air updates.

**Matt Carpenter (@Ma77Carpenter), Principal Researcher, Grimm**
Matthew Carpenter is a Principal Security Researcher with Grimm (SMFS) performing deep security research for .com, .gov, and .mil. Matthew’s expertise is in reverse-engineering, vulnerability research, exploit weaponization, hardware/software/firmware/Automotive/IoT/ICS/AMI/Radio, Symbolic analysis, generalized hacker techniques, and teaching. He has a detailed background in Risk analysis/mitigation, Penetration Testing at all levels (hw/sw/net/web/physical). Matthew is former vice-chair of UCAIUG AMI-SEC Task Force and SG Security, and lead the Vulnerabilities team for NIST Cyber Security Coordination Task Force developing NISTIR-7628. He is a former member of the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), and was the Red-team lead for Advanced Security Acceleration Project (AMI-SEC/ASAP). Matthew is an entertaining and informative speaker, and is a repeat speaker at many Hacker/ICS/SCADA conferences, domestic and abroad.

**Faye Francy, Executive Director, Automotive Information Sharing and Analysis Center (Auto-ISAC)**
This position serves the global automotive industry through the analysis and sharing of trusted and timely cyber threat information about existing or potential cyber-related threats and vulnerabilities for on-road vehicle electronics and associated networks. Actively engaged with private-sector stakeholders, partners and government agencies to facilitate information sharing and strengthen the industry’s capability and capacity to detect, prevent, respond to, and mitigate disruptions related to the connected vehicle and supporting infrastructure. Responsibilities include developing, maintaining and executing a Strategic Plan that outlines strategic and operational priorities for the automotive industry. Build and maintains key relationships with Chief Information Officers (CIOs), Chief Information Systems Officers (CISOs), Product Development leadership, and other executives across the automotive industry responsible for securing vehicles and connected infrastructure. The Auto-ISAC is a non-profit organization operating in Washington, D.C.
Previously Ms. Francy was the Aviation ISAC Executive Director while she was working for the Boeing Company. Ms. Francy held numerous leadership positions at Boeing, including Cyber ONE Leader, Director Enterprise Technologies for Networked Systems, Director of Phantom Works Network Centric Thrust and Director of Engineering for Air Traffic Management.
Ms. Francy owned and operating two small businesses and held positions as a forensic chemist at Maryland State Police, Monroe and West Palm Beach County Sheriff’s Departments. Ms. Francy has a Bachelor’s Degree in Chemistry and Mathematics from Towson State University and a Master Degree in Forensic Chemistry from University of Pittsburgh. Faye is an American Institute of Aeronautics and Astronautics (AIAA) Associate Fellow, former Research Advisory Board member for Embry Riddle, and DC Analyst’s Roundtable Membership Chair.

**Ben Gardiner, Principal Security Engineer, Irdeto**
Ben Gardiner is a Principal Security Engineer at Irdeto and a member of the ethical hacking team, specializing in hardware and low-level software security. With more than 10 years of professional experience in embedded systems design and a lifetime of hacking experience, Gardiner has a deep knowledge of the low-level functions of
operating systems and the hardware with which they interface. He brings this knowledge to Irdeto, a pioneer in
digital platform and application security. With nearly 50 years of experience, its software security technology and
cyber services protects more than 5 billion devices and applications against cyberattacks for some of the world’s
best known brands. Prior to joining Irdeto in 2013, Gardiner held embedded software and systems engineer roles
at several organizations. Gardiner has a Masters of Engineering in Applied Math & Stats from Queen’s University.
He is also a member of and a contributor to SAE TEVEES18A1 Cybersecurity Assurance Testing TF (drafting J3061-2)
and the GENIVI security subcommittee.

Bjoern Giesler, Head of L4 Autonomous Driving Functions bei ZF Group
Björn has worked in the fields of autonomous robots and driverless vehicles for almost two decades. He got his
Ph.D at the robotics department at the University of Karlsruhe, Germany, working on augmented reality systems
for human-robot collaboration. In 2005, he joined AUDI to develop several in-vehicle systems for active safety,
driver assistance, and finally driverless cars. He moved on to head the Driver Assistance department at Elektrobit
GmbH in 2015, where he developed the robinos architecture, a block set for building driverless vehicle software.
He currently heads the Level 4/5 Autonomous Driving department at ZF AG, one of the largest automotive system
developers.

Harold A. Garza, Research Engineer, Southwest Research Institute
Mr. Garza is a research engineer in the Embedded Systems Security Group at Southwest Research Institute. Mr.
Garza works on developing and testing cybersecurity solutions for IoT, Automotive, and Autonomous Vehicle
industries. Within the Autonomous Vehicles industry, Mr. Garza has helped write several reports on the security
posture of AV sensors and architectures, and has also performed penetration testing on several AV sensors.

Jason Gay, Cybersecurity Engineer, Magna Electronics
Computer Engineer from Kettering University. Currently a Cybersecurity Engineer with the Secure Connectivity
team at Magna Electronics which is responsible for designing secure, connected automotive gateways and
telematics units. Past roles include being the system engineer for ultrasonic park assist and auto-park systems, as
well as infrared rain & light sensors.

Kevin Harnett, Principal Investigator/Security Researcher, Dept. of Transportation/Volpe Center
Program Manager for the United States Department of Transportation at the Volpe National Transportation
Systems Center located in Cambridge, Massachusetts. Mr. Harnett has over Thirty-Three years of combined project
management, technical consulting, and implementation skills. Kevin is a Cyber Security Program Manager (PM)
with experience providing technical leadership in planning, implementing and managing high priority programs
involving Cyber Security and risk management for the Department of Transportation (DOT), Federal Aviation
Administration (FAA), DOD/USAF, Defense Information Systems Agency (DISA), United Kingdom’s Communications
Electronic Security Group (CESG), NASA, Department of Homeland Security, Transportation Security
Administration, Coast Guard, and other agencies, with special emphasis on security risk management, security
policy, security training, certification/accreditation, penetration testing, security awareness, security
testing/evaluation, incident response capability and remediation.
Specialties: Airborne Network Security Research and Development (R&D) and operations. Experience and interests
include: Electronic Flight Bags (EFBs), In-flight Entertainment (IFE) systems, wireless technologies, authentication,
intrusion detection/auditing, global trust, Public Key Infrastructure (PKI), security simulators, NextGen Flight Object
(FO), security training, security policy, security architecture, penetration testing, and aircraft/airline maintenance
security.
Technical expertise over the past 3 years in automotive cybersecurity in support of National Traffic and Safty Adminisitration (NHTSA) in the areas of: automotive threat/risk assessment models and methodologies, vulnerability analysis/mitigation plan development, Information Sharing and Analysis Center (ISAC) Plan
development for the world-wide automotive industry, and consulting/technical support for SAE’s Vehicle Electrical
System Security (VESS) Subcommittee.

Mitchell Johnson, Security Researcher, GRIMM
Mitchell Johnson is a security researcher at GRIMM, specializing in automotive vulnerability research. His background includes specialized embedded software development, with a particular focus on the automotive and safety industries as well as background in other sectors including safety critical aerospace, and industrial control systems. He has contributed extensively to GRIMM’s open source “CanCat” CAN bus reverse engineering tool and on “3PO,” GRIMM’s mobile auto-hacking demonstration.

**Urban Jonson, Chief Technology Officer, National Motor Freight Traffic Association, Inc. (NMFTA)**
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 25 years of experience in information technology, complex systems analysis, and information technology security. NMFTA is nonprofit membership organization headquartered in Alexandria, Virginia who represents over 500 carriers who collectively operate close to 200,000 power units generating $100 billion in freight revenue. NMFTA is committed to helping less-than-truckload (LTL) carriers and members meet the challenges confronting the transportation industry through representation, research, education, and the publication of specifications, rules, transportation codes and dissemination of studies, reports and analyses.

**Ben LeMere, CEO, Berla Corporation**
Ben is the CEO and Co-Founder of Berla Corporation. Berla is an operationally focused consulting firm and solutions provider to the Department of Defense, Homeland Security and Law Enforcement Community. Berla focus on building advanced acquisition and analysis platforms to support digital medial exploitation and processing of data through forensics, reverse engineering, and high order analysis. Berla’s mission is to be forward leaning and solve tomorrow’s problems, today.

**Matt Mackay, Senior Risk Manager – Product Cybersecurity, General Motors**
Matt leads a diverse team that focuses on risk assessment, governance, and monitoring and response activities for GM’s Product Cybersecurity team. Specific responsibilities include incident response, coordinated disclosure, intelligence analysis, training, process refinement, and the development of IT applications that support risk-based decisions. Prior to joining GM, Matt served in the US Navy for 23 years in a variety of roles as a prior-enlisted Surface Warfare Officer, including submarine nuclear engineering and surface ship combat systems validation and deployment. Matt has a B.S. in Mathematics and an M.S. in Computer Science.

**Emilian Papadopoulos, President, Good Harbor**
Emilian Papadopoulos is president of Good Harbor, a premiere consultancy advising Boards, CEOs, and government leaders on cyber risk. Emilian has helped clients across sectors including aviation, manufacturing, energy, insurance, law, technology, and defense. Emilian is a graduate of the University of Toronto and the Kennedy School at Harvard University.

**Lisa Plaggemier, Director, Risk, Culture of Security, and Client Advocacy, CDK Global**
Lisa has spent her career branding and marketing cars and trucks, software and data, and now security. She’s combined her passion for the automotive industry with a fervor for security awareness to help CDK, OEMs, and dealers manage their risk and grow their businesses securely. Lisa worked for marketing for Ford Motor Company in the US, Europe, Africa and the Middle East. She is currently the Director of the Client Security Advocacy Office for CDK’s Global Security Organization. Lisa graduated from the University of Michigan and currently lives in Austin, TX.

**Rob Shein, Manager, PwC LLC, Advisory Cybersecurity and Privacy**
Rob is a Manager in PwC’s Cybersecurity and Privacy practice focusing on Strategy and Transformation with over 20 years of experience in cybersecurity in both the private and public sector. Most recently focused on IoT and connected-car security, he has done work for numerous major corporations, civilian federal government and two branches of the U.S. military. Able to speak in terms of both technical needs and business drivers, he excels at translating between stakeholders of divergent types to produce meaningful solutions.
Rob has performed most roles within cybersecurity, leveraging a personality trait known as the “malicious bit,” which enables certain individuals to view the world through the eyes of an attacker, without themselves having the motives or intent of one. His primary motivation is to accomplish useful change in the security posture of as much of the world as possible, while preserving business and operational functionality.

**Phil Swarbrick, Director, PwC LLC, Advisory Cybersecurity and Privacy**
Phil is a Director in PwC’s Cybersecurity and Privacy practice focusing on Strategy and Transformation. He is an experienced Information Security professional with extensive knowledge in information security risk management, enterprise risk assessments, vulnerability and penetration testing, security compliance, intrusion detection and prevention, security operations and continuous monitoring, incident response and threat management. He has led multiple assessments of ICS/SCADA and automotive components.
Phil has led multiple merger and acquisition projects focusing on cybersecurity and due diligence. Phil focuses his cybersecurity expertise within the power and utility and automotive industries. Phil holds a Bachelor’s of Science in Network Technologies with a concentration in Network Security, a minor in Business Administration, and a Master’s of Science in Computer, Information, and Network Security from DePaul University and has attended the DHS’s ICS-CERT training.

**Kai Thomsen (@kaithomsen), IT Security Architect, Audi AG**
Kai is the Incident Response team lead at AUDI AG and currently working on creating a modern CSIRT at Audi. Before that he established an IT Service Continuity organization at Audi and developed and executed crisis management training exercises for top management. Prior to Audi, he worked at SMS group, an engineering company for steel manufacturing plants. There he was responsible for network security architecture, NSM, and forensics. Kai holds an M.A. in computer science and English and American Literature. He is also currently a SANS Instructor in Development.

**Dr. André Weimerskirch, VP Cyber Security, Lear Corporation**
André Weimerskirch is VP Cyber Security at Lear Corporation. Before that, André established the transportation cyber security group at the University of Michigan Transportation Research Institute (UMTRI), and co-founded the embedded systems security company ESCRYP'T which was sold to Bosch in 2012.
André is active in all areas of automotive and transportation cyber security and privacy, published numerous articles in the area of automotive and embedded cyber security, and is co-founder of the American workshop on embedded security in cars (escar USA). André is vice chair of the SAE Vehicle Electrical System Security Committee, co-chairs the Michigan Mobility Transformation Center (MTC) cyber security working group, co-organizes the SAE ComVEC cybersecurity session, and is a member of the joint SAE/ISO Cybersecurity Working Group.