THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS

Automotive Cybersecurity Summit

Program Guide

@SANSInstitute #SANSAutoSummit

Agenda

All Summit Sessions will be held in Crystal Ballroom (unless noted).

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

Monday, May 1

7:00-8:30am	**Registration & Coffee** (LOCATION: CRYSTAL BALLROOM FOYER)
8:30-8:45am	***Opening Remarks & Introductions*** ***Mike Assante****, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute* ***Matt Carpenter*** *(@Ma77Carpenter), Principal Researcher, Grimm*
8:45-9:00am	***So What Does It Mean To "Hack" A Car?*** The term "Hacking" has been used to describe everything from modifying the backup-lights on your '78 Monza to remote-controlling someone else's Jeep whilst they drive it. I often get requests to "hack" someone's car (mostly professionally speaking), which typically sparks a long conversation trying to determine what precisely their desire is. In light of research made public in 2015 and 2016, "car hacking" can evoke a certain sense of dread. However, in an industry which is still in the process of engaging appropriate security assessment practices and relationships, we need more than just dread. We need a common understanding. Before we kick off the Summit, let's make sure we have a shared definition of what "hacking" a car means. ***Matt Carpenter*** *(@Ma77Carpenter), Principal Researcher, Grimm*
9:00-9:45am	***If You Can't Hack It, You Don't Own It*** Learn about the current trends for the increasingly-digital automotive industry. We will cover software over-the-air update methodologies. We will discuss the right way to do updates and the wrong way. Often, security professionals overlook the rights of consumers in their quest to lock everything down. We will also discuss ways you can safely have both a secure environment and consumer ownership. ***Craig Smith****, Research Director of Transportation Security, Rapid7; Author, "The Car Hacker's Handbook"*
9:45-10:30am	***Your Car is Trying to Kill You, and Other Reality Checks*** In 2015, researcher Corey Thuen fueled our paranoia by demonstrating how in-car dongles distributed by major insurance providers could be an attack vector for anything from the theft of personal data to major destruction on the nation's highways. What have we learned since then? Where is the industry still failing to apply adequate security controls? Where should we be funneling security investments to see real, measurable ROI? Corey will share a number of recent assessments that might yield concrete answers to these frightening questions. ***Corey Thuen*** *(@CoreyThuen), Senior Consultant, IOActive*
10:30-11:00am	**Networking Break and Vendor Expo** (LOCATION: CRYSTAL BALLROOM FOYER)

Monday, May 1

11:00-11:45am

Road to the Future

This presentation & discussion examines the history, current footprint, and future effects of cybersecurity in the automotive, transportation, and smart infrastructure space. It addresses direction of policy, development, and research; it also describes business and research opportunities ranging from individually sourced through large organizations. The intent is to be operationally substantive, leaving participants with a sense of the likely “roadmap” that cyber will follow and that industry and policy will dictate while highlighting opportunities for the enterprising as they arise over the next 15 years.

Karl Heimer, Sr. Tech Advisor for Cybersecurity, Michigan’s MEDC Auto Team and Defense Center; DHS Government Vehicle Fleet Manager Steering Committee; Founding Partner, Autoimmune Inc.

11:45am-12:30pm

V2X Security and Privacy

The National Highway Traffic Safety Administration (NHTSA) recently published a Notice of Proposed Rulemaking (NPRM) for vehicle-to-vehicle (V2V) communications. This talk will provide an overview of the security and privacy aspects around V2X. First, the relevant aspects of the communication security standard IEEE 1609.2 and the security credential management system (SCMS) PKI are presented. Then cybersecurity aspects of the V2X computing platform are presented, including minimum performance requirements specified in SAE J2945, a secure communication interface, separation to safety-critical vehicle features, and integrity protection.

Dr. André Weimerskirch*, VP Cyber Security, Lear Corporation*

12:30-1:30pm **Lunch**

1:30-2:15pm

Next-Gen Car Communications: Exploring Potential Future Capabilities

The platform is the purpose, as it is not just a product; it is the thing we rely on to move us through modern-day life. People rely on their cars – from the day they purchase them to the day they send them to the scrap heap – to safeguard them and their precious cargo. These facts make decisions about the future of car communications a critical matter. Join us to discuss the merits of sticking with CAN or moving to Ethernet to best navigate the road ahead. This panel will consider the risks, opportunities, and trade-offs of approaches to the backbone of a car’s communications. There are few other decisions that will so impact the future for connected cars.

MODERATOR: ***Mike Assante****, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute*

PANELISTS: ***Kevin Harnett****, Principal investigator/Security Researcher, Dept of Transportation/ Volpe Center*

Craig Smith*, Research Director of Transportation Security, Rapid7; Author, The Car Hacker’s Handbook*

Justin Montalbano*, Technical Manager, CyberSEAL Lab, Delphi Automotive*

Monday, May 1

2:15-3:00pm	***Using Formal Methods Tools to Improve Security in an Autonomous Military Truck*** Formal Methods are often described as rigorous system-design techniques used to mathematically prove both facts about a system and the absence of certain types of errors. However, historically, these techniques have been largely ignored by the professional engineering community due to their expense, limits, and challenging usability. But now, new open-source tools coming out of the DARPA High Assurance Cyber Military Systems (HACMS) program aim to change this perception. This talk will review a number of these tools and describe how they have been applied to improve security in a U.S. Army autonomous truck. ***Dr. Dariusz Mikulski, Ph.D.*** *(@DariuszMikulski), Senior Research Scientist, Ground Vehicle Robotics (GVR) | U.S. Army TARDEC*
3:00-3:30pm	**Networking Break and Vendor Expo** (LOCATION: CRYSTAL BALLROOM FOYER)
3:30-4:15pm	***Building a Cybersecurity Testing Lab within a Tier 1 Supplier*** Have you thought about testing your embedded systems for cybersecurity during development? Should these assessments be performed internally or externally? This talk will be about the successes and difficulties of developing a cybersecurity testing lab within an automotive tier 1 supplier. The presentation will examine different processes used during development; tools used for hacking automotive components (both cheap and expensive); the people that make up a cybersecurity testing lab and how to find these people; facilities needed to perform assessments on vehicles and their components; the importance of contracts with 3rd parties for testing; and, lastly, how a cybersecurity testing lab can help shape and define the standards to be used for cybersecurity testing and implementation. ***Justin Montalbano****, Technical Manager, CyberSEAL Lab, Delphi Automotive*
4:15-5:00pm	***Closing the Gap: What IT Staff and Automotive Engineers Need to Learn to Tackle the Evolving Challenges*** Historically, the IT security and engineering departments have only connected to discuss security requirements vs. developers' and engineers' work demands, or for incident response. With IT taking on a much more important role in future vehicles, the way these different teams interact and work together has to change dramatically. From learning the other side's language, requirements, limitations, and methodologies to developing mixed teams, this talk will show how to close the gap that usually exists between these departments and pave the way to a more integrated, holistic approach to car security. ***Kai Thomsen*** *(@kaithomsen), IT Security Architect, Audi AG*
5:45-7:00pm	**Networking Reception**

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 2

7:00-8:45am	**Registration & Coffee** (LOCATION: CRYSTAL BALLROOM FOYER)
8:45-9:15am	***Navigating the Exciting Future of Automation*** The new age of automation is revolutionizing how we make, move, and power the world. Systems on which we rely are gaining new capabilities that increase safety, performance, reliability, and comfort, yet they present a new set of challenges. One of the most important skills is the ability to anticipate the implication of a greater reliance on automated systems and the ability to envision paths to unlock benefits while minimizing risks. Our future design principles and capabilities must be able to deal with the implications of scale, consequences, convergence, concentration, control, and access. We must examine existing models that have achieved success while avoiding well-known pitfalls. ***Mike Assante****, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute*
9:15-9:25am	***Overview of the Automotive ISAC*** The Automotive Information Sharing and Analysis Center (ISAC) is an industry-operated environment created to enhance cybersecurity awareness and collaboration across the global automotive industry – light- and heavy-duty vehicle OEMs, suppliers, and the commercial vehicle sector. But what does that mean for you on a daily basis? How can the Auto ISAC help you improve your security posture, and how can you contribute to this important industry effort? Get a quick peek into the ISAC in this overview. ***Faye Francy****, Executive Director, Automotive Information Sharing and Analysis Center (Auto-ISAC)*
9:25-9:45am	***Safeguarding and Securing Automotive Manufacturing Systems*** Jeff will discuss a currently-implemented ICS Security solution for Manufacturing Control Systems, and share his thoughts regarding what is available versus what the needs are in an Industrial Security Appliance. ***Jeff Smith****, Automotive Industry Consultant; USCAR Representative*
9:45-10:30am	***Building Communities: How do we Foster an Ecosystem to Protect our Future?*** The digital race is on and the drivers are jockeying for position; but for what purpose? Join us for an honest look at the state of automobile security and how we can work together. This fast-paced panel will debate everything from responsible disclosure to security testing. MODERATOR: ***Mike Assante****, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute* PANELISTS: ***Mike Ahmadi****, CISSP, Global Director – Critical Systems Security, Synopsys Software Integrity Group* ***Kevin Baltes****, CISSP, Director & CISO – Product Cybersecurity, General Motors* ***Faye Francy****, Executive Director, Automotive Information Sharing and Analysis Center (Auto-ISAC)* ***Jeff Smith****, Automotive Industry Consultant; USCAR Representative*
10:30-11:00am	**Networking Break and Vendor Expo** (LOCATION: CRYSTAL BALLROOM FOYER)

Tuesday, May 2

11:00-11:45am	***RKE (Key Fob) Replay Attack Using Roll Jam Technique – Explained*** Last year Sami Kamar described his Roll Jam device but never released details about how it may work or how it was made. So we took the best parts of his sister talk (Open SeseMe) and made our own Roll Jam. Now we can capture Key Fob Messages from many manufacturers and using a Corrupt-Capture-Corrupt-Replay-style attack, we can replay key fob commands by Jamming the key fob message despite it having a rolling code or encryption. In this talk we'll discuss the tools needed test your own vehicle for this vulnerability. ***Robert Leale****, Founder, CanBusHack Inc.*
11:45am - 12:30pm	***Secure Product Design Lifecycle for Connected Cars*** In the past decades, we have seen increasing automation on our vehicles. This starts with numerous driving assist technologies, such as lane keeping, adaptive cruise control, parking assist, trailer backing assist and etc. The automotive industry is currently embracing autonomous driving technologies. In the meantime, we are getting used to various connectivity technologies on cars. It is common to see vehicles with interfaces such as cellular, WiFi and Bluetooth. Many vehicles are now able to communicate with other vehicles (known as the V2V technology) and public infrastructure (V2I). The benefit of increased automation and connectivity is multitude. Cars are now easier and more fun to drive. They deliver better energy efficiency, offer higher customer convenience and improve public safety. Nevertheless, we should also realize that vehicles are now cyber-physical systems and part of the Internet of Things. Although cybersecurity is a relatively new topic to the automotive industry, it has to be addressed appropriately because vulnerabilities in cybersecurity could impact safety. Fortunately, proactive thinking and design measures can be taken to address cybersecurity issues. The presentation brings awareness to several guidelines and standards that could be referenced to help bring a cybersecurity mindset to an organization and be integrated into the Product Design Lifecycle. ***Lisa Boran****, Manager – Vehicle Cybersecurity, Ford Motor Co.*
12:30-1:30pm	**Lunch**
1:30-2:15pm	***Securing the Internet of BIG Things*** The anticipated "Internet of Things" is suddenly mainstream for many consumer products. In late 2015, Caterpillar Inc. Chairman and CEO Doug Oberhelman stated: "Caterpillar goes beyond the Internet of things, to the Internet of big things." It's no secret that IOT depends on a secure foundation. The evolution of network security laid a foundation, yet with redefined boundaries and resource constraints, IOT security requires new innovation. The final answer to secure the IOT is in process. Caterpillar's big engines and machines depend on the same embedded digital technology as IOT. While embedded security covers more than IOT, many parallel issues are included in the security framework. This talk discusses the security threats and challenges facing IOT in a comparison with security requirements for the heavy machinery industry segment. ***Paul Bierdeman****, Senior Engineer, Caterpillar Inc.*

Tuesday, May 2

2:15-3:00pm

Heavy Vehicle Cybersecurity Update

National Motor Freight Traffic Association, Inc. (NMFTA) represents over 500 carriers who collectively operate close to 200,000 power units generating approximately $100 billion in freight revenue. NMFTA member motor carriers perform a vital service to our nation's economy by delivering the goods necessary to keep commerce flowing. As a key stakeholder in heavy vehicle cyber security (HVCS), NMFTA hosts industry workshops exploring cybersecurity issues such as incident response, risk mitigation, data anomaly detection, and many others. This session offers an overview and update of the NMFTA HVCS program, along with some specific resources available to fleet operators to improve their security posture today.

Urban Jonson*, Chief Technology Officer, National Motor Freight Traffic Association, Inc. (NMFTA)*

3:00-3:20pm **Networking Break and Vendor Expo**

3:20-4:05pm

Applying Cybersecurity Processes to Autonomous Vehicles

As autonomous vehicles begin to transition from experimental to more integrated second generation prototypes, the methods of protecting vehicle systems from cybersecurity threats becomes increasingly important. Published remote attacks on modern vehicles demonstrates that auto manufacturers and suppliers must incorporate cybersecurity practices into the vehicle lifecycle. As manufacturers begin to address the challenges of incorporating security processes and requirements, the difficulties of assessing threats to autonomous systems remains relatively unexplored. This paper describes some of the popular methods and unique challenges of applying cybersecurity to the future autonomous vehicle.

Daniel Zajac *(@DanielZajac83), Senior Research Engineer - Embedded Systems Security Group, Southwest Research Institute*

4:05-4:50pm

Securing the Electric Vehicle Infrastructure and Protecting the Energy Sector

The Idaho National Laboratory has worked with the Department of Energy (DOE) for many years to aid in securing the electric grid. With the introduction of electric vehicles into this infrastructure, as well as the enhanced connectivity between these vehicles and smart grid enabled components, there is a continued need for research into the potential security impacts of this integration. This presentation will outline the current efforts by DOE to secure the electric vehicles and the charging infrastructure.

Kenneth Rohde*, Cyber Security R&D, Idaho National Laboratory*

4:50-5:00pm

Closing Remarks

Mike Assante*, Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute*

Matt Carpenter *(@Ma77Carpenter), Principal Researcher, 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.

@SANSInstitute **#SANSAutoSummit**