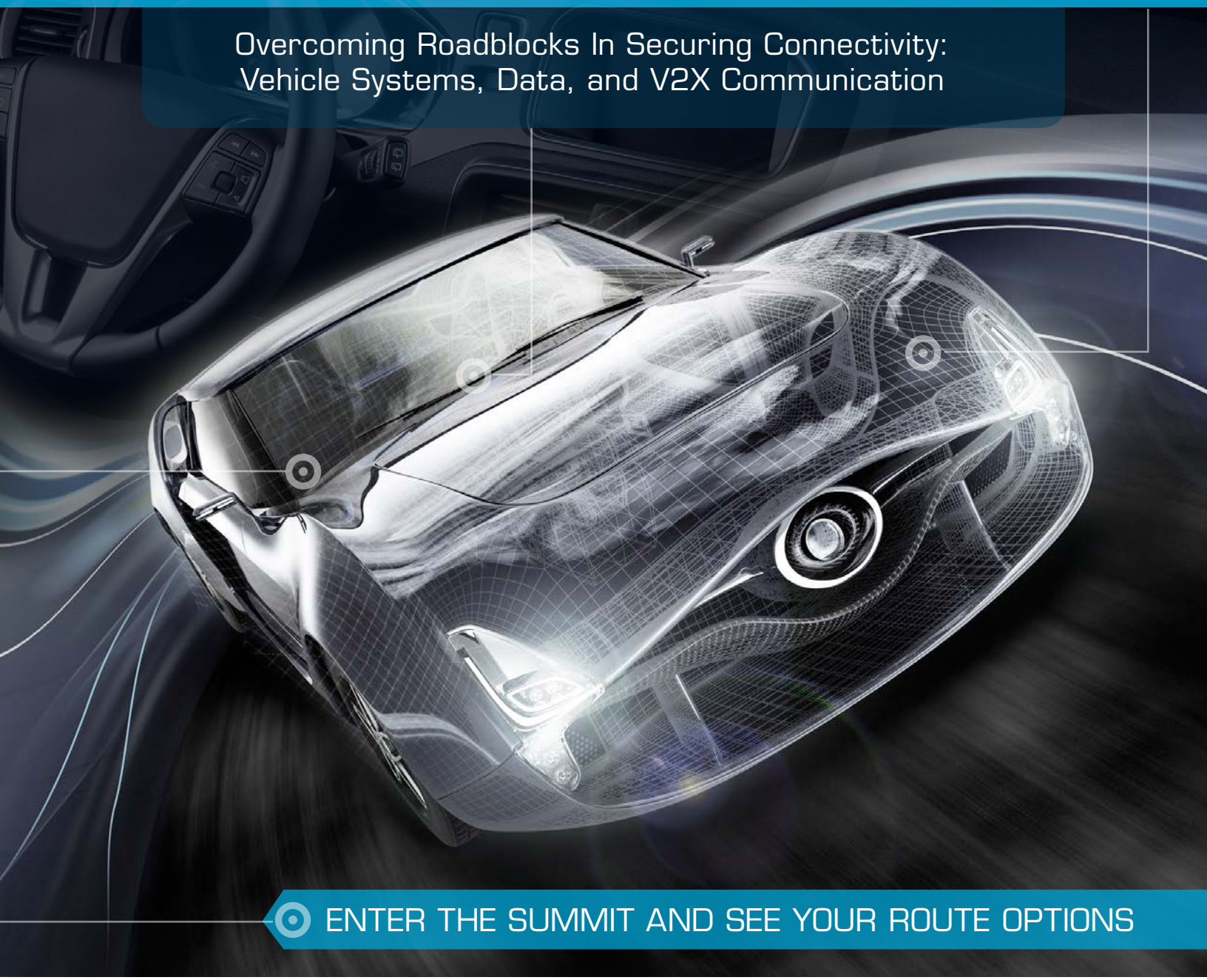
5TH AUTOMOTIVE CYBER SECURITY SUMMIT

Pre-Summit Workshop Day: March 27, 2017 • **Main Conference:** March 28-29, 2017 • **Cobo Center,** Detroit, MI

Overcoming Roadblocks In Securing Connectivity: Vehicle Systems, Data, and V2X Communication



ENTER THE SUMMIT AND SEE YOUR ROUTE OPTIONS

Sponsors:

HORTONWORKS · FireEye · Micron · NowSecure · BAYSHORE · Green Hills SOFTWARE · Solera · Capgemini · Karamba Security · TRUSTINSOFT

Media Partners:

AUTO-ISAC · AutoHarvest.org Collaborate, Innovate and Win · Automotive Electronics & Embedded Software · AMP · Autonomous Vehicles · CVTA · Information Security · iMobile · Real-Time Embedded · MTAM

REGISTER TODAY! www.AutomotiveCyberSecurity.com • 1-800-882-8684 • EnquiryIQPC@IQPC.com

5TH AUTOMOTIVE CYBER SECURITY SUMMIT

DRIVING CYBER SECURITY FORWARD

To All Key Players Involved In The Auto Industry, is this not your current situation?

OPPORTUNITY/FEAR: As cars become smarter and are designed to communicate not only with each other, but with the surrounding infrastructure as well as backend data centers, the number of potential attack surfaces will increase. The looming possibility of hackers taking over safety-critical functions within the vehicle and causing large-scale destruction certainly exists.

CHALLENGE: With added infotainment systems and telematics inserted into vehicles, the amount of data being collected on passengers will exceed billions of gigabytes. How will auto makers secure, store, and utilize this data? What consumer privacy concerns will arise and how will the industry handle this ecosystem of connectivity? Can they come together with regulators to establish the necessary security standards to reach in vehicle design and development?

TRUTH: Unfortunately, a wide-scale cyber attack on vehicles will occur; at this point, it is simply a question of when. Those prepared and ready to implement cyber incident response tactics are in the best position to minimize the overall damage dealt.

PREPARE: In order to facilitate conversations on these topics and better prepare the industry in confronting cyber challenges, the **5th Automotive Cyber Security Summit** will be returning to Detroit, MI on March 27-29, 2017. Join us as cyber security experts from both inside and outside the auto industry are brought together to share their thoughts on how cyber security should be tackled.

Sincerely,

Frankie Yip
Program Director
Automotive iQ
a division of IQPC

HEAR FROM THE INFAMOUS HACKER

CHARLIE MILLER

Distinguished Engineer, Autonomous Transportation Security
Didi Chuxing

Recognized globally for his ability to identify vulnerabilities in consumer products, Dr. Charlie Miller is "one of the most technically proficient hackers on Earth", according to Foreign Policy.com.

Currently the Senior Security Engineer at Uber's Advanced Technologies Center, Dr. Miller has made waves within the field of automotive security for his work alongside research partner, Chris Valasek. First demonstrating that with direct access to a vehicle, the physical systems of a Ford and Toyota could be controlled by an attacker, he then expanded this research to show that these attacks could be done remotely. Dr. Miller and Valasek made headlines and exposed serious security flaws in automobiles with their remote compromise of a 2014 Jeep Cherokee, in which they obtained physical control of the vehicle from more than 10 miles away; the results led Fiat Chrysler to recall 1.4 million vehicles.

Dr. Miller previously served on Twitter's computer security team after five years as a computer hacker for the National Security Agency. The 4-time winner of the "Super Bowl" of computer hacking, the annual Pwn2Own competition, Dr. Miller has publicly demonstrated many security exploits, specifically of Apple products and is the first person to remotely hack the iPhone, as well as the Android smartphone (on the day it was released). He is the co-author of three books, including iOS Hacker" Handbook, and has been featured in a range of media outlets, including NBC, ABC, CNN, NPR, CNBC, The New York Times, USA Today and Forbes.

Don't miss Charlie's session on Day 1 @ 9:15 am on A Hacker's Eye View

MEET THE ONES FACING AUTO CYBER SECURITY HEAD-ON

Gain insight from our expert pool of speakers who bring years of experience in the cyber security domain either from a technical, organizational, or policy prospective.

LOOKING TOWARDS THE FUTURE

Become part of discussions on how the auto cyber landscape will evolve as developments in self-driving vehicles continue, standards are set by regulators, and consumer privacy concerns heighten.

IN-DEPTH CONVERSATIONS WITH YOUR PEERS

Are you up-to-date on the best cybersecurity measures for the auto industry? Attend our workshop sessions for group discussions and interactive lessons on how to confront growing cyber challenges.

UNBEATABLE NETWORKING

From Cyber Security Experts and IT Specialists to Systems Engineers and Software Designers, our Summit attracts a wide range of attendees from all levels of the organization. Who will you meet to help achieve your goals?

MEET THE CYBER SECURITY EXPERTS

FEATURING

HENRY BZEIH
Managing Director, Connected & Mobility Division, **Kia Motors**
Board Member, **Auto-ISAC**

KEVIN BALTES
Director & CISO, Product Cybersecurity
General Motors

GABOR LENGYEL
Technical Fellow, Security
Lucid Motors
CHAIRMAN

JOSEPH KRISTOFIK
Global Functional Safety Manager for Passive Safety
Autoliv
CHAIRMAN

BOB GRUSZCZYNSKI
OBD Communication Expert
Volkswagen

ANDRE WEIMERSKIRCH
VP Global Cyber Security
Lear Corporation

JUSTIN MONTALBANO
Cybersecurity Lab Technical Manager
Delphi

JOHN KRZESZEWSKI
Cybersecurity Engineering Technical Manager
Delphi

DAVID CONNETT
Cybersecurity Process and Tools Technical Manager
Delphi

CHANDRASEKHAR POTLURI
Sr. Functional Safety Controls Engineer
Mercedes-Benz Research & Development

RUSS BIELAWSKI
Engineer in Research Lead
University of Michigan Transportation Research Institute (UMTRI)

ANEESH MATHAI
Architect, Automotive Infotainment & Driver Information Systems
HARMAN International

LUKE DEMBOSKY
Partner
Debevoise & Plimpton

ANASTASIA CORNELIO
Cyber Security IP Developer
Magneti Marelli Italy

GARY STREELMAN
Director, Advanced Engineering and New Concepts
Magneti Marelli

SCOTT SHULTZ
Director, Electronics Program Management
Magneti Marelli

KIRK STEUDLE
Director
Michigan Department of Transportation

DAVID BEHEN
Department of Technology, Management, and Budget Director & CIO
State of Michigan

SCOTT MCCORMICK
President
Connected Vehicle Trade Association

BEAU WOODS
Deputy Director, Cyber Statecraft Initiative
Atlantic Council

DARIUSZ MIKULSKI
Senior Research Scientist
US Army TARDEC

CATHERINE MUIR
Of Counsel
Baker & McKenzie

ANDREW HOOG
CEO
NowSecure

DAVID SEQUINO
VP/GM of INTEGRITY Security Services
Green Hills Software

ROBERT CALDWELL
ICS Manager
Mandiant

SRINI ADIRAJU
Director of Cybersecurity
Visteon Corporation

NICK GILL
Chairman, Global Automotive Sector
Capgemini

LUKE SIMON
Lead Counsel, Autonomous Vehicles
General Motors

DAVID BARZILAI
Executive Chairman & Co-Founder
Karamba Security

FABRICE DEREPAS
Founder & CEO
TrustInSoft

MICHAEL GER
General Manager, Manufacturing and Automotive
Hortonworks

MICHAEL SCHIEBEL
General Manager, Cyber Security
Hortonworks

HIGHLIGHTS FROM THE AUTO CYBER SECURITY SERIES

TOTALED RESULTS ACROSS PAST FOUR SUMMIT ITERATIONS

400+ ATTENDEES

70+ PRESENTATIONS

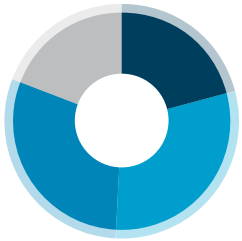
80+ SPEAKERS

35+ SPONSORS

ATTENDEES TRAVELED FROM:

UNITED STATES	UNITED KINGDOM	INDIA	CANADA
FRANCE	NETHERLANDS	SOUTH KOREA	BRAZIL
ITALY	JAPAN	SINGAPORE	
		GERMANY	

ATTENDEE SENIORITY



- 21% Director
- 30% Engineer
- 30% Manager
- 19% C-Suite / President / VP

PAST ATTENDING ORGANIZATIONS:

Continental, Delphi, Denso, Bosch, GM, Harman, Hitachi Inspire the Next, Honda The Power of Dreams, Honeywell, Hyundai, Lear Corporation, Magna, Magneti Marelli, Mercedes-Benz, Mitsubishi, Nissan, NHTSA, Paccar, Tardec, Toyota, Uber, ZF TRW

PAST SPONSORS:

Akamai, Argus Cyber Security, Beyond Security, CDK Global, Cisco, Coalfire, Dell, Deloitte, freescale semiconductor, Grammatech, Green Hills Software, Hortonworks, inmarsat, LogRhythm The Security Intelligence Company, Microsemi, NexGen, NTT Security, Palamida, RogueWave Software, Security Innovation, Stroz Friedberg, Symantec, Synopsys, TATA Consultancy Services, TrustNSoft, Venafi, VisualThreat

NEW YEAR, NEW TECHNOLOGIES, NEW DESTINATIONS

WHICH ROUTE WILL YOU TAKE TO REACH YOUR DESTINATION?

To provide deeper insight and focused discussions into key auto cyber challenges faced by the industry, the agenda will split into Routes A/B and C/D on Day 1 of the Main Summit.

ROUTE A: In-Vehicle Cyber Security

With telematics, infotainment, ADAS, and V2X capabilities, it is becoming increasingly more difficult to secure the access routes into control/safety-critical systems that can be exploited by hackers. Furthermore, more and more external devices that can be connected either wirelessly or through the OBD-II port are being introduced to the market. Are these devices designed to prevent unauthorized access? Ultimately, all vehicles have an incredibly large attack surface and it is up to auto makers to secure as many security vulnerabilities as possible. Enter this track to gain a deeper understanding of how to confront this endless challenge.

ROUTE B: Manufacturer Security / Strategy

The vehicle is a blueprint of IP held by OEMs and suppliers. If a hacker gains access into the vehicle's systems, imagine the manufacturer data they could collect. And it doesn't stop there, since connected vehicles will relay data back to IT backend receivers, are steps being taken to secure these control towers? In the end, cyber security measures are liabilities but they also should be viewed as new growth opportunities for auto makers to explore. Enter this route to gain a deeper understanding of challenges faced by auto makers as connected technologies and IoT expands.

WHO SHOULD ATTEND?

OEM / Tier 1 Suppliers

CIOs, CTOs, CSOs, CISOs
VP/Director/Manager/Team Lead/Chief Engineer/Researcher of:

- Vehicle Cyber Security
- Safety / Functional Safety
- Connected Cars / Self-Driving Vehicles
- Software Solutions / Connected Systems
- Vehicle IT / Telematics / Infotainment / Driver Information Systems
- IT / IT Infrastructure / IT Security
- Cyber Security Analyst / Program Manager
- Security Engineer
- Security / Embedded Software Developer
- Intrusion Detection Specialist / Embedded Penetration Tester
- Technology / Technical Fellow
- Policy Developer

Vendors / Industry Solution Providers

VP/Director/Team Lead of...

- Business Development
- Business Systems
- Marketing
- Technology Sales
- Regional Representative
- Sales Engineer
- Commercial Manager
- Product Services Manager
- Technical Solutions Manager
- Security Engineer / IT Specialist

Vendor Categories

- Information and Technology Security / Services / Software
- Automotive Cyber Security
- Code Coverage Analysis
- Threat Detection / Incident Response
- Predictive Analysis
- Software Testing / Validation
- Cyber Security Consulting
- Memory / Cloud Tools / OTA Technology

BECOME PART OF THE EXPERIENCE

"A good opportunity to meet suppliers and customers in the cyber security field."
-Product Architect, Magna International

DEMO DRIVE:

See up-close demonstrations of the vehicle and data security software solutions being offered by our esteemed sponsors.

REGULATION LANDSCAPE:

How will the auto industry and regulators handle evolving cyber challenges? Who is held liable in the event of an attack? Hear opinions of key industry players from OEMs and Tier 1s to security counselors and policy makers.

VEHICLE CAN BUS SECURITY:

Representatives from Magneti Marelli Italy showcasing their new developments in Trojan Intrusion Detection Systems for Vehicle CAN Bus Security.

DRINKS RECEPTION

Spend the evening amongst your newly formed connections, enjoy some drinks and exchange ideas on what you've learned so far!

NEW TOPICS:

What exciting sessions do we have in store?

- Cyber Security As An Innovation Strategy Rather Than A Complication
- Executing Cyber Incident Response Tactics And Developing Disclosure Programs To Mitigate Harm

QUESTIONS TO BE ANSWERED:

- How Can Open Source Components In Vehicle Software Reveal Security Vulnerabilities To Hackers?
- How Can Vehicles Protect Themselves From External Devices That Connect Wirelessly Or Directly Through The OBD-II Port?

"Very insightful into this new field. More aware of the entry points of intrusion into a vehicle by hackers."
-Electrical Hardware Engineer, ALPS Electric North America

PRE-SUMMIT WORKSHOP DAY

27TH MARCH 2017

The focuses for the Pre-Summit Workshop Day have been modeled after the key cybersecurity functions available in the "Automotive Cybersecurity Best Practices" report released by the Auto-ISAC in 2016. By attending all four workshops, you will gain a better understanding of how to address cyber security challenges through both a technical and organizational perspective.

8:30 **Refreshments & Registration**
As you register for today's workshops, enjoy some refreshments and lively peer-to-peer networking!

9:00 **ROAD 1: Cyber Security Governance**

Adopting A Cyber Security Mindset Across All Levels Within The Auto Sector To Prepare For Cyber Threats

Why Travel This Road? Cyber security must be emphasized from vehicle conception to delivery and even afterwards in terms of maintenance. This mentality should be embedded into the company culture and promoted by all managerial levels. Doing so ensures that all teams are complying with regulations and internal policies as well taking the necessary steps to address cyber threats

- Emphasizing cyber security from the top-down and preparing all members for the paradigm shift in vehicle security
- Cyber security as potential competitive advantage for companies
- Moving from securing system components piece by piece to security by design
- Working with partners and suppliers to implement security protocols

Gary Streelman
Director, Advanced Engineering and New Concepts
Magneti Marelli

Scott Shultz
Director, Electronics Program Management
Magneti Marelli

10:45 **Quick Detour: Morning Networking & Refreshment Break**

11:00 **ROAD 2: Incident Response and Recovery**

Where Does The Responsibility Fall? - Understanding Your Role In The Face Of Cyber Attacks

Why Travel This Road? In the event of a cyber attack, every employee will have a role in dealing with the crisis, whether it is legal preparing an investigation, engineers submitting software data, or analysts scanning for errors. Auto makers who have not properly prepared their employees for cyber attacks risk substantial backlash from stakeholders. Understanding where your role lies and the necessary steps to take can lead to speedier recovery and minimize damages.

- Mitigating damages, investigating the incident, providing the necessary data, and remedying the situation
- Following the proper procedures laid out in a cyber incident response plan
- Working together with legal, management, and other teams to collect evidence and close the incident

Luke Dembosky
Partner
Debevoise & Plimpton

12:45 **Pit Stop: Networking Lunch**
You covered a lot in the AM sessions, join us for a delicious lunch and a chance to introduce yourself to some new faces!

1:45 **ROAD 3: Risk Management and Assessment**

Prioritizing Cyber Security Testing To Detect And Discern Early Product/System Weaknesses

Why Travel This Road? Identifying potential security risks early-on during the development process is a surefire way to mitigate safety and data privacy threats. Taking a proactive approach towards testing and validating security systems can help auto makers identify and address these threats. Those actively pursuing security by design will ultimately create a competitive advantage for themselves.

Creation of a laboratory to oversee all cyber security activities both in-house and through third-party contracts

- Integrating best cyber security practices from the IT side into design/engineering teams
- Purpose and objectives of cyber security engineers and specialists from the Tier 1 perspective
- Conducting penetration testing to evaluate and improve the security design of auto components

Justin Montalbano
Cybersecurity Lab Technical Manager
Delphi

3:30 **Quick Detour: Afternoon Networking & Refreshment Break**

3:45 **ROAD 4: Threat Detection and Protection**

Finding and Responding to Threats to the Connected Car

Why Travel This Road? So you just realized that you've connected your car to the Internet. What now? Let's take the lessons learned from securing Internet applications and Internet IoT devices and apply them to designing and monitoring the connected car. What does the secure development lifecycle for the connected car look like?

- Design lifecycle: Applying threat modeling to discover design level security requirements
- Development lifecycle: Applying application security principles to connected car software development
- Operation Lifecycle: Concepts for the connected car security operations center
- How does the connected car operate in the connected world?

Michael Schiebel
General Manager, Cyber Security
Hortonworks

5:30 **Closing Remarks**

5:35 **End of Pre-Summit Day - Congratulations! You Made It To Your Main Destination!**

MAIN SUMMIT DAY ONE
28TH MARCH 2017

7:30 **Refreshments & Registration**

Enjoy some morning refreshments before getting the show on the road!

8:15 **Chairman's Welcome & Opening Remarks**

Gabor Lengyel
Technical Fellow, Security
Lucid Motors

8:30 **KEYNOTE: Bridging The Gap Between Industries: The Need For Auto Players To Embrace The Cyber Security Frontier**

- Is the automotive industry equipped with the necessary resources and knowledge base to confront growing threats in auto cyber security?
- Expediting the process of fortifying connected vehicles through cross collaboration within and beyond the auto industry
- Adopting a company and industry-wide mentality focused on cyber security
- Bringing in everyone from engineering to business development

Henry Bzeih
Director, Connected & Mobility Division
Kia Motors America

9:15 **Automotive Security: A Hacker's Eye View**

Both for better and worse, automotive security is headline news and garnering tremendous widespread attention from media, consumers, manufactures, and hackers alike. The security of today's vehicles involves many moving parts, but while manufactures take a majority of the blame, multiple parties contribute to the security debt in today's vehicle ecosystem. This keynote takes a deep dive into automotive security, current attacks, and vulnerabilities. It also looks toward the future and onset of autonomous vehicles. The audience can expect to hear candid calls to action and highly distinctive insight into vehicle security from this famed hacker's perspective.

Charlie Miller
Distinguished Engineer, Autonomous Transportation Security
Didi Chuxing

10:00 **Quick Detour: Demo Drive & Morning Networking**

Learn more about cutting edge cyber security solutions that will enable your team to develop a safe and secure vehicle, protect essential data, and ensure the integrity of IT infrastructure.

11:00 **Adding The Necessary Cyber Defenses For In-Vehicular Systems To Bolster Functional Safety Without Compromising Vehicle Performance**

- Breaking down and integrating cyber security into every aspect of the automotive product lifecycle
- Ensuring security protocols do not infer and cause potential time lags with intended functions of ECUs
- Balancing functional safety with connectivity in the vehicle
- Building resilience into powertrain components while integrating functional safety

Chandrasekhar Potluri
Sr. Functional Safety Controls Engineer
Mercedes-Benz Research & Development

11:45 **Installation Of Trojan Intrusion Detection Systems For Vehicle CAN Bus Security**

- Capabilities and usefulness of an Intrusion Detection for automotive applications
- Implementation of an anomaly detection module, from scheduling to intrusion recording
- Properly reacting to detected intrusions: a focus on the features to be ensured by recovery strategies

Anastasia Cornelio
Cyber Security IP Developer
Magneti Marelli Italy

12:30 **Pit Stop: Networking Lunch**

Join us for a delicious lunch with your peers before splitting up into the key focus areas that speaks to you!

1:30 **Mobile App Crashworthiness: Securing Vehicle-To-Device (V2D) Interfaces And Communications**

- How do vulnerable mobile apps and insecure V2D communications put drivers and manufacturers at risk?
- Applying crashworthiness and safety ratings concepts to mobile app and connected car cybersecurity
- How to manage mobile app security defects and vulnerabilities in the connected car and mobile app development process

Andrew Hoog
CEO
NowSecure

Break Out Time: Choose Your Path to Security

ROUTE A: IN-VEHICULAR CYBER SECURITY	ROUTE B: MANUFACTURER SECURITY / STRATEGY
2:15 **In-Vehicle Infotainment And Driver Information Systems: Security And Safety Impact On Consolidation / Distribution Of ECUs** • Trends and motivation for Consolidation / Distribution of Infotainment, Telematics and Display ECUs • Considerations for external connectivity – Bluetooth, WIFI, 4/5G etc. • In- vehicle networks – CAN, MOST, Ethernet, Flexray, etc.	**Safeguarding Vehicles From Industry Espionage Using Encrypted Communication Protocols** • Using vehicles to hack into manufacturers' IT networks and gain access to confidential data • Attacking vehicles to sabotage brand reputation and cause intentional accidents

ROUTE A: IN-VEHICULAR CYBER SECURITY

Session continued

- Security and safety aspects with SOTA/FOTA, Remote Diagnostics, Telematics functions, etc.
- Safe guards with Consolidation and Distribution of ECUs - Virtualization, Hypervisor, Network Security, etc.

Aneesh Mathai
Architect, Automotive Infotainment & Driver Information Systems
HARMAN International

ROUTE B: MANUFACTURER SECURITY / STRATEGY

Session continued

- Implementing encrypted communication protocols as a possible strategy to protect intellectual property

David Connett
Cybersecurity Process and Tools Technical Manager
Delphi

2:45

Preventing External, Connected Devices From Compromising Vehicle Systems

- Vehicle data access vs. vehicle security (make this the first bullet point)
- Current status of efforts to address security issues , including Congress/NHTSA involvement
- Move the "Entering a car's core systems" bullet point to beneath the first bullet point

Bob Gruszczynski
OBD Communication Expert
Volkswagen

Linking Cyber Security To Innovation And Utilizing Data As A Growth Strategy

- What doors will open up as vehicle components, apps, and third-party devices are designed to be secure?
- How can data collected from consumers be utilized by auto makers?
- Cyber security as a growth enabler for auto companies
- Spurring innovation and enabling new uses for technology through clearing cyber risks

David Behen
DTMB Director & CIO
State of Michigan

3:15

Implications Of Developing V2X Systems: Communication Networks Become Access Routes Into Vehicle Systems

- Potential security challenges as fixed pieces and infrastructure on roadways and cities become capable of wireless connectivity
- Being cautious of any system connected to a vehicle as it becomes an additional attack surface
- Protecting the vehicle from false or altered signals sent from V2X systems

Andre Weimerskirch
VP Global Cyber Security
Lear Corporation

OPEN FORUM DISCUSSION: Securing The IT Backend Receivers Of Vehicle Manufacturers To Allow For Proper Monitoring And Updating Of Data

- Targeting the data control center in order to spread malicious software over the connected vehicle network
- Creating secure storage centers for data transmitted from vehicles
- Detecting threats lurking within endless streams of vehicle data

Forum Leader:

Kevin Baltes
Director & CISO, Product Cybersecurity
General Motors

Moderator:

Fabrice Derepas
Founder & CEO
TrustInSoft

3:45

Quick Detour: Afternoon Networking & Refreshment Break

4:15

Cybersecurity For The Automotive Industry: Driving Digital, Securely

In this session, hear real-life examples of how OEMs and suppliers across the globe have identified key areas of threats and how they've worked to reduce or eliminate them. Learn how OEMs can gain actionable intelligence about the cybersecurity status of their connected vehicle fleets, including the security of their plants and enterprise IT.

Nick Gill
Chairman, Global Automotive Practice
Capgemini

4:45

Securing the Connected Car in a Connected World

In today's ever more complex and interconnected society, vehicle cybersecurity involves far more than just the vehicle itself. Rather, true cybersecurity involves a far wider ecosystem including (but not limited to) insurance providers, law enforcement, communications providers and Cybersecurity "as a service" providers. In this session, learn how modern connected data and analytics platforms can provide the historical and real-time insights necessary to detect and prevent impending threats and improve vehicle safety.

Michael Ger
General Manager, Manufacturing and Automotive
Hortonworks

Michael Schiebel
General Manager, Cyber Security
Hortonworks

5:30

Chairman's Closing Remarks

Gabor Lengyel
Technical Fellow, Security
Lucid Motors

5:35

End Main Day One - Drinks Reception

Before heading back, spend some time in the evening with your peers and engage in conversations while enjoying a refreshing cocktail.

MAIN SUMMIT DAY TWO

29TH MARCH 2017

7:45

Refreshments & Registration

Enjoy some morning refreshments before we take off!

8:15

Chairman's Welcome & Opening Remarks

Joseph Kristofik
Global Functional Safety Manager for Passive Safety
Autoliv

8:30

PANEL DISCUSSION: The Road To Self-Driving Vehicles Begins With Developing A Secure Connected Vehicle

- How will the driving landscape change in the next 10 years and where is the automotive industry heading as a whole?
- How will challenges in cyber security become more prevalent as self-driving and connected technologies advance?
- How will cyber security solutions in today's connected vehicles serve as a blueprint for the development of autonomous vehicles?
- Handling the increasing number of vehicle vulnerabilities as IoT infrastructure expands
- Potential risks of cyber attacks and associated ramifications towards passengers, vehicles, OEMs, etc.

Moderator:

Scott McCormick
President
Connected Vehicle Trade Association

Panelists:

Fabrice Derepas
Founder & CEO
TrustInSoft

Andre Weimerskirch
VP Global Cyber Security
Lear Corporation

Justin Montalbano
Cybersecurity Lab Technical Manager
Delphi

Dariusz Mikulski
Senior Research Scientist, Ground Vehicle Robotics
US Army TARDEC

David Sequino
VP/GM of INTEGRITY Security Services
Green Hills Software

9:15

Breaking the Cycle: Foiling Attackers From Reaching Their Goals

Protection of connected vehicles begins long before they take to the road, both during design and manufacturing

- Implementing a security development lifecycle can address risk during design and development
- Security controls for the plant are essential to protecting the vehicle during manufacturing

Robert Caldwell
ICS Manager
Mandiant

10:00

Determining How Regulations And Standards Will Impact The Development Of Connected Vehicles And Components

- How do various regulatory bodies at the state and federal level plan to tackle rising concerns over consumer safety and privacy?
- Bringing together various players in the automotive, regulatory, and cyber spaces to determine necessary security standards
- Using cyber security as another measure to determine overall vehicle safety and quality level of automotive components

Kirk Steudle
Director
Michigan Department of Transportation

10:45

Quick Detour: Morning Networking & Refreshment Break

11:15

Autonomous Security: Demo Of Real Life Cyberattacks And How ECUs Autonomously Prevent Them With Zero False Positives

David Barzilai
Executive Chairman & Co-Founder
Karamba Security

12:00

Developing Systems To Deliver Secure OTA Updates To Repair ECUs And Close Security Gaps

- Delivering secure software and firmware updates OTA to remove bugs and improve functionality
- Utilizing gateways to defend the cloud and transfer of data between connected systems
- Detecting and removing any corrupted updates that have been sent over to vehicles
- Shorten the time for installing software updates into vehicles

John Krzeszewski
Cybersecurity Engineering Technical Manager
Delphi

12:45

Pit Stop: Networking Lunch

Join us for a delicious lunch with your peers and share what you've learned so far throughout the Summit!

1:45

POLICY DISCUSSION: Input From Multiple Key Players Involved With The Auto Industry On Emerging Cyber Challenges

- Should successful infiltration of security loopholes be regarded as model defects and subjected to the same ramifications?
- With countless manufacturers and suppliers having a role in the development of connected vehicles, which party will be held liable in the aftermath of a successful cyber attack?
- Where does the consumers' role lie and should they be held responsible for failing to install software updates on their own devices?
- How will vehicle crimes related to cyber hacks be handled in the future?

Moderator:

Catherine Muir
Of Counsel
Baker & McKenzie

Panelist:

Beau Woods
Deputy Director, Cyber Statecraft Initiative
Atlantic Council

Luke Simon
Lead Counsel, Autonomous Vehicles
General Motors

2:30

Ready Or Not: Open Source Software In Automotive Electronics

- Open source model as an integral part of developing vehicle software
- Exercising caution when using any third-party codes and knowing where your code comes from
- Checking open source components for security vulnerabilities and preventing exploits from hackers

Russ Bielawski
Engineer in Research Lead
University of Michigan Transportation Research Institute

3:15

Quick Detour: Afternoon Networking & Refreshment Break

3:45

Cybersecurity: Process To Solutions

- Foundation for Cybersecurity
- Field Monitoring and responding immediately to threats
- Resolving security flaws in a speedy and efficient manner to increase consumer confidence in auto brands

Srini Adiraju
Director of Cybersecurity
Visteon Corporation

4:15

Evaluating Risks And Developing Disclosure Programs To Warn The Public Of Potential Threats

- Determining when and whether consumers need to be informed of potential vehicle security threats
- Comparing the risks of withholding information from consumers versus revealing flaws in vehicle systems
- Notifying consumers of cyber threats and the necessary precautions to protect themselves

Beau Woods
Deputy Director, Cyber Statecraft Initiative
Atlantic Council

5:00

Chairman's Closing Remarks

Joseph Kristofik
Global Functional Safety Manager for Passive Safety
Autoliv

5:05

End of Main Summit- See You Next Year!

MEET YOUR BUSINESS OBJECTIVES THIS 2017

Networking

Ensure that you have the opportunity to engage with the key decision makers within your industry. We can create a platform for you to effectively interact with your top customers and prospects in the environment of your choice. This can range from formalized private meetings / workshops right through to less structured networking events such as sponsored drinks receptions, coffee breaks or lunches. Ultimately whatever you decide is the right forum; we will support you in your quest to advance relationships with the key people who can influence the future of your business.

Branding

Your company can be elevated to a position where they are seen as a market leader. In a fiercely competitive market you need to ensure that your brand is differentiated from the competition. Failure to create a clear identity will see your organization fade into the background. We ensure that we do everything we can to effectively lift your brand before, during and after the event. Not only do we create a fully integrated marketing campaign, which your company can be part of, but we also offer high impact premium branding opportunities for example on bags, water bottles, pens lanyards etc.

Thought Leadership

If you think that you should be viewed as a true industry leader then your need to demonstrate your market knowledge and expertise through a thought leadership opportunity, such as speaking or chairing. This is a highly unique opportunity for your company to educate the market, and as long as you are credible enough to fit into a high level event program, we can position your organization alongside top customers and prospects in our speaker faculty. As part of this speaker faculty your company will be set apart from other industry attendees giving you the competitive edge required to make further strides in the market.

8 REASONS WHY THE 5TH AUTOMOTIVE CYBER SECURITY SUMMIT CAN BENEFIT YOU!

1. **Generate new sales leads:** Our event will bring together the industry's key-decision makers, all of whom have strong business reasons for attending the event. By exhibiting and presenting, you can impact on these buyers. By the very nature of the high quality of delegate attendance, the contacts generated will lead to very high conversion rates.

2. **Launch new products or services:** Use the event as a launch pad to promote your latest products or system. With the most senior figures from the industry in attendance, plus carefully selected media partners at the event, innovative new technology will always generate a buzz.

3. **Demonstrate thought leadership:** Speaking on the program will allow you to demonstrate your market knowledge and expertise to an audience of high level decision makers.

4. **Enter new markets:** Sponsorship is one of the most effective ways to enter new markets. It is a great opportunity to research and network whilst gaining exposure to a new qualified database.

5. **Building customer loyalty:** Face-to-face contact at conferences, and showing continued support of the market, helps develop client loyalty as well as cementing your position as an industry player.

6. **Positioning your company brand:** Being part of this highly influential industry event establishes your company as a strong brand and highlights your company's abilities and strengths. Commitment to this event also demonstrates your capability as a global player.

7. **Building relations with the media:** We have researched the market in order to find the most influential media partners. We understand that opportunities for editorial coverage and developing better relations can be integral to your companies' success, so our media partnerships offer additional benefit above and beyond the standard sponsorship package.

8. **Brokering new business partnerships:** Currently there are huge opportunities to partner with OEM suppliers actively looking to adjust their supply chains.

To learn more about the opportunities available contact:

Chris Ritchie // T: (+1) 212-885-2799 // E: Chris.Ritchie@iqpc.com

PRICING & REGISTRATION

OEMs, Tier 1 Suppliers, & Government	Standard Pricing
Main Conference	$2,495
Main Conference + 1 Workshop	$2,995
Main Conference + 2 Workshops	$3,445
Main Conference + 3 Workshops	$3,845
All Access: Main Conference + 4 Workshops	$4,245
One Workshop	$549

Tier 2 Suppliers & Vendors	Standard Pricing
Main Conference	$2,995
Main Conference + 1 Workshop	$3,495
Main Conference + 2 Workshops	$3,945
Main Conference + 3 Workshops	$4,345
All Access: Main Conference + 4 Workshops	$4,695
One Workshop	$549

Group Discounts	Savings
Groups of 3-4	10% off
Groups of 5+	15% off

*IQPC reserves the right to determine who is considered an End-User or a Vendor upon registration for an event. Those who are determined a vendor will be denied access to End- User pricing. These prices are featured as a limited time only promotion. IQPC reserves the right to increase these prices at its discretion.

Please note multiple discounts cannot be combined. A $99 processing charge will be assessed to all registrations not accompanied by credit card payment at the time of registration.

MAKE CHECKS PAYABLE IN U.S. DOLLARS TO: IQPC

*CT residents or people employed in the state of CT must add 6.35% sales tax.

Details for making payment via EFT or wire transfer:
Bank Name: JP Morgan Chase & Co.
Name on Account: Penton Learning Systems LLC dba IQPC
Account #: 937-332641
ABA/Routing #: 021000021
Reference: IQPC: 24870.005

Team Discounts: For information on team discounts, please contact IQPC Customer Service at 1-800-882-8684. Only one discount may be applied per registrant.

Payment Policy: Payment is due in full at the time of registration and includes lunches and refreshment. Your registration will not be confirmed until payment is received and may be subject to cancellation.

For IQPC's Cancellation, Postponement and Substitution Policy, please visit www.iqpc.com/cancellation

Special Dietary Needs: If you have a dietary restriction, please contact Customer Service at 1-800-882-8684 to discuss your specific needs.

DON'T GO ALONE!

Take advantage of our team discounts!

Contact us today to secure your spots!

3 EASY WAYS TO REGISTER:

Visit: www.AutomotiveCyberSecurity.com

Call: 1-800-882-8684

Email: enquiryIQPC@IQPC.com

VENUE & ACCOMMODATION

Cobo Center
1 Washington Blvd
Detroit MI 48226
United States

Website: www.cobocenter.com
Phone: (313) 877-8777

When it comes to filling your free time, there is no shortage of things to do in America's Motor City. Make sure to check-out of our hand-picked sights while you're not at Automotive Cyber Security Summit!

Ford Rouge Factory Tour @ The Henry Ford
20900 Oakwood Blvd.,
Dearborn, Mich. 48124

GM Renaissance Center
Jefferson Ave,
Detroit, MI 48243

Detroit Institute of Arts
5200 Woodward Ave.,
Detroit, Mich. 48202

ABOUT AUTOMOTIVE IQ

Automotive IQ, a division of IQPC, is an international online platform focusing on providing automotive industry professionals with a central resource for knowledge on topics such as Autonomous Vehicles, Cyber Security Powertrain, Electrics/Electronics, Chassis Systems and Car Body & Materials. Most importantly, the Automotive IQ is a community. We are dedicated to creating a learning environment for sharing best practices and finding solutions to challenges within the automotive industry.