3RD ANNUAL

AUTOMOTIVE CYBER SECURITY SUMMIT

MARCH 21-23

THE BARONETTE RENAISSANCE DETROIT-NOVI HOTEL // DETROIT

DON'T MISS THE FORD SITE TOUR

SEE ON PAGE 6

Sponsors: Akamai ARGUS CYBER SECURITY HORTONWORKS POWERING THE FUTURE OF DATA LogRhythm The Security Intelligence Company Microsemi NEXUM We Mean Security PALAMIDA Application Security for Open Source Software STROZ FRIEDBERG Symantec TATA CONSULTANCY SERVICES

WWW.AUTOMOTIVECYBERSECURITY.COM // ENQUIRYIQPC@IQPC.COM // 1-800-882-8684

HEAR WHAT YOUR PEERS ARE SAYING:

"Excellent networking opportunities, broad representation from industry."

– Lead Cybersecurity Engineer (MITRE)

DENSO

"The event was high level in terms of technical content. This is great for Management level."

– Software Developer (Robert Bosch LLC)

BOSCH

"Great overview of current situation for cyber security."

– Senior Quality "Planning Engineer (Denso)

DENSO

"Excellent high-level overview of automotive cyber security."

– Director, Cyber Security Engineering (Delphi Corporation)

DELPHI

"Very informative event which provided a window into the current state of the automotive OE's and contact resources for Tech expert companies."

– Principal Engineer (Harley-Davidson Motor Co.)

MOTOR HARLEY-DAVIDSON COMPANY

YOUR INDUSTRY'S #1 EVENT

200+ ATTENDEES

30+ SPEAKERS

15+ SPONSORS

20+ SESSIONS

HIGHLIGHTED COMPANIES THAT ATTENDED LAST YEAR:

Allstate You're in good hands. · ARGUS CYBER SECURITY · ARXAN · Booz | Allen | Hamilton · BOSCH · CDK Global · CHRYSLER · CISCO · Coalfire · Deloitte. · DELPHI

DENSO · FISKER · Ford · freescale semiconductor · GE · GM · GRAMMATECH · HARLEY-DAVIDSON MOTOR COMPANY · HARMAN · HITACHI · HONDA · Hortonworks

IBM · intel · MAGNA · MAGNETI MARELLI · Microsemi Power Matters. · MITRE · MITSUBISHI MOTORS · nexteer AUTOMOTIVE · NTT Communications | NTT Com Security · NVIDIA

NXP · Panasonic · QUALCOMM · Raytheon · RogueWave SOFTWARE · sas · Security Innovation THE APPLICATION SECURITY COMPANY · TOYOTA · TRW · VENAFI · VisualThreat

WELCOME

Industry Peers,

We can all agree that the automotive community is fast tracking towards unprecedented sophistication of vehicles. It seems that “Back to the Future” is only a few years away! Customer demand and the competitive nature of the industry is the driving force to achieve many revolutionary advancements and make them a reality.

With cyber threats becoming more prevalent, exposing the car and its drivers and passengers to multiple risks, we need to take a stance on protecting the car. According to a recent study from IHS Automotive, in seven years 78% of the cars sold globally will be connected which is up from the 30% in the market now. With such increase of connectivity in cars on the road, the race to the finish is upon us on determining the best practices, strategies and solutions to protect and secure the car inside and out.

Long-term cybersecurity will be required for all cars that have any type of connection throughout. As we all know, the world today is unable to function without some type of connectivity including every day driving. To secure the customer data transmitted throughout the car automotive industry needs to find all vulnerable entry points and to “plug” them before anything happens.

At the **3rd Annual Automotive Cyber Security Summit**, you will have a unique opportunity to answer all your questions, discuss any concerns you might have and learn best practices from top industry executives. Come join us at **THE EVENT OF THE YEAR on March 21- 23 in Detroit.** I look forward to meeting you!

Sincerely,

Erin Butler
IQPC Program Director
Automotive IQ

2016 EXPERT SPEAKER LINEUP:

Chris Valasek
Security Lead
UBER's Advanced Technology

Kevin Baltes
Director & CISO-Product Cybersecurity
General Motors

Samantha Davison
Security Awareness & Education Program Manager
UBER

Gary Streelman
Director Advanced Engineering and New Concepts
Magnetti Marelli

Ian Simmons
VP Business Development and Corporate Engineering and R&D
Magna International

Cem Hatipoglu
Division Chief
National Highway Traffic Safety Administration

Doug Moeller
VP of Connectivity
Lear Corporation

Joern Ihlenburg
Engineering Manage-Electronics & Corporate Engineering, R&D
Magna International

John Krzeszewski
Cybersecurity Engineering Technical Lead
Delphi

Michael Reinhold
Software Engineer
Robert Bosch LLC

Barbara Czerny
Senior Technical Specialist Safety and Cybersecurity
ZF TRW

Pankil Vyas
Senior Manager, Cyber Security
Harman

PRE-SUMMIT DAY

March 21, 2016

8:00AM

WORKSHOP A: Futuristic Cars Are Only a Day Away: What Are the Safety Features of the Connected and Autonomous Car and How to Protect Them?

OEM companies, Tier 1 Companies and Solution providers alike are all working towards the "next big thing". In order to deploy this hot car into the market, safety precautions and implementations need to be met. How does your design measure up? During this workshop, colleagues and peers within the automotive industry will discuss and deliberate how these futuristic cars will governor the safety features and what it will take to protect them.

Daniel Bartz, Automated Vehicle Engineer/Strategist

10:30AM

WORKSHOP B: Improving the Detection Intensity of Security Incidents and Finding the Needle in the Haystack is Key to Managing Risk

The number of recent high profile breaches in the media sends a stark reminder to the enterprises that the existing investments in people, process and technology does not adequately manage the risk. Furthermore, Verizon Data Breach Investigation Report synopsis of 11 years of real security incident and breach data from 70 International contributors highlights the need for the industry to re-evaluate their existing cyber security strategy and focus on "improving the detection Intensity" as vital to defending against the dynamic, persistent and continuous Threat! There are two kinds of CISO's – those who know they have been breached, and those who have yet to learn that they have been breached. It is a question of when and not if when it comes to data breaches; irrespective of who you are and size of your organization. Hence, the starting position of "you have been breached" is more realistic then otherwise to develop a cyber-security strategy for the enterprise. So what are the potential solutions to consider and where can one start?

Bhavesh Chauhan, Principal Client Partner, **Verizon Enterprise Solutions**

12:00PM

Lunch

1:00pm

WORKSHOP C: Technology Overdrive: Understanding the Security Impact that the Advanced Machinery has Throughout the Infrastructure of the Car

Is there ever a thing as too much technology? The answer, no! But this will impact the infrastructure and the security understanding including Bluetooth, roadside assistance, and personal data. Although the technology will benefit consumer demand, companies might not fully understand the security impact that will occur from these advancements. Join this workshop and take advantage of the considerations throughout multiple points of view in the industry on necessary security implications for all the new machinery.

Barbara Ciaramitaro, Lead Professor, Information Technology and Cybersecurity, Director, **Center for Cybersecurity Leadership-Walsh College**

3:00PM

Henry Ford Site Tour

America's greatest manufacturing experiencing. Put yourself at the center of sheer manufacturing might. During the tour, you will be immersed into some eye-opening encounters with the technology of tomorrow today. Join this tour and surround yourself with the past, present, and future of the American automobile manufacturing.

6:30PM

Meet-and-Greet Cocktail Reception

After this informative first day, relax and take a moment to meet with your fellow peers in the industry. Join the Meet-and-Greet Reception, to develop relationships and discuss the future of automotive cyber security.

7:30am

Registration and Coffee

8:45AM

Chairman Remarks

9:00AM

FUTURE PREDICTIONS FROM THOSE ON TOP

KEYNOTE PANEL: The Next Steps for OEM and Tier 1 Companies in Standardizing Cybersecurity Mitigation

There is no denying, the collaboration within the automotive industry could be better. Whether that be agreeing to share information, work together or discuss case studies. Without this collaboration, there could be a loss of progression towards the next big thing. Experts will discuss the steps that the automotive industry needs to face together in order to combat the increasing issues with regulating cybersecurity precautions.

Moderator: **Chris Valasek,** Security Lead, **Uber's Advanced Technologies Center**

Kevin Baltes, Director & CISO-Product Cybersecurity, **General Motors**

Joern Ihlenburg, Engineering Manager-Electronics & Corporate Engineering, R&D, **Magna International**

LaVern Sula, President North America, **Argus**

9:45AM

Safety vs Security: Is One Compromising the Other With the Increase of Technology?

Safety has been the major concern in the automotive industry ever since the first car has been deployed. Today, with the increase in connected and autonomous vehicles, security has arguably become the frontrunner of industry challenges. Consumers and automakers now have personal and company information embedded into the car that equally needs to be protected. During this session, you will discover how the switch has changed the deployment factor now that security plays a critical role in bringing these vehicles to market.

Ian Simmons, VP Business Development and Corporate Engineering and R&D, **Magna International**

10:30AM

Networking Break and Demo Drive

11:30AM

Building Comprehensive Security into Cars & Trucks Automotive

Security threats have gone from theory to reality. Tech-savvy thieves steal cars throughout the world, and mainstream videos show hackers remotely hijacking cars. Technology exists to solve these problems, but no single silver bullet can deliver effective security. Effective security has to be composed carefully from a short list of key ingredients, and this has to be done within the constraints of automotive engineering, which are far more demanding than traditional information technology (IT) systems. During this session, Brian Witten will frame the role, value, strengths, and limitations of crucial types of security technology that can compliment each other to produce meaningfully safe & secure vehicles, and update the audience on progress toward industry standards in critical areas.

Brian Witten, Senior Director, IoT, **Symantec**

Sponsored by **Symantec**

Symantec.

12:15PM

Networking Lunch

1:15PM

CASE STUDY PRESENTATION: Cyber Security Strategies Recommended for the Automotive Industry

The layers of cyber security within the car seem to be never ending. First step to securing the car is through the developmental cycle and the architectural design. In this case study presentation, Doug Moeller will tear back each of these layers and provide a migration strategy towards a more secure solution.

Doug Moeller, VP Connectivity, **Lear Corporation**

2:00PM

Current State of Automotive Attacks and Protections or "Adventures in Automotive Networks and Control Units"

As we know previous research has shown that it is possible for an attacker to get remote code execution on the electronic control units (ECU) in automotive vehicles via various interfaces such as the Bluetooth interface and the telematics unit. During this session we will expand on the ideas of what such an attacker could do to influence the behavior of the vehicle after that type of attack.

Chris Valasek, Security Lead, **Uber's Advanced Technologies Center**

3:00PM

The State of Internet Security

Many key automotive applications and processes moving to the cloud and online and are subject to the fast growing amount of performance related issues and cybersecurity attacks. Akamai delivers between 15-30% of all web traffic, which enables us to have great insight into what happens online. During this session, walk through the current state of web security, including the most common attack types, attack tools, location of attach traffic origins and how it relates to the automotive industry. In addition, hear a case study from one of our key customers, Red Bend, discussing how this platform had helped secure over the air updates.

Tony Lauro, Sr. Enterprise Security Architect-**Akamai**

Luke Harvey, US Director of Technology-**HARMAN's Redbend**

Sponsored by **Akamai**

3:45PM

Networking Break

4:00PM

Connecting the Phone to the Car: Protecting Personal Information and Securing the Interface

Having the ability to "plug in your life" through Bluetooth and USB has lead the automotive industry in the right direction towards technologically advanced vehicles. When drivers and passengers upload their information to the car, this is inviting the idea that personal information could be stolen. Join this session to learn how to protect this sensitive data from hackers.

John Krzeszewski, Cybersecurity Engineering, Technical Lead, **Delphi**

4:45PM

More In-Vehicle Data Means More Security Precautions: Protect from Cyber Threats to Ensure Customer's Full Control of the Vehicle

Now that automotive manufacturers are offering data plans, deploying vehicle updates over the air and sensors outside the car to ensure full knowledge of the road, the amount of in vehicle data has increased to a tremendous amount. Protecting this information is a necessary precaution that the automotive industry needs to do. During this session, learn about the technologies to help consumers stay in control of the car regardless of the situation.

Michael Reinhold, Software Engineer, **Robert Bosch**

5:30PM

Closing Remarks End of Day 1

5:45PM

Entry Point Cocktail Reception

Don't let the conversation end! Are all your entry points secured? During this cocktail reception, discuss with colleagues and peers what you had learned the first main day of the event.

MAIN DAY TWO

March 23, 2016

8:00am

Registration and Coffee

9:00AM

Opening Remarks

Barbara Ciaramitaro, Lead Professor, Information Technology and Cybersecurity, Director, **Center for Cybersecurity Leadership-Walsh College**

9:15AM

Is Your Customer and Employee Data Safe? Detecting Vulnerabilities That Could Impact the Safety of Your Customer and Employee's Personal Information

Customer and employee's data is now being transmitted not only throughout the car but also from car to car. The constant stream of information is a gold mine for some hackers and breaches looking to gain knowledge on the information. Samantha Davison will dive into the topic of how to education not only your customers but also your employees to ensure that all data is secure and safeguarded.

Samantha Davison, Security Awareness & Education Program Manager, **Uber**

10:00AM

Is the Car Lying to You? Connected Car Software Implementation to Determine Accurate Positioning to Keep Drivers Safe

Connected cars are right around the corner. What does this mean for the automotive industry and for the consumers? Having the cars to "speak" with one another and share information is a colossal step in the direction of a fully automated car. Even though the cars will be communicating about the road and other cars on the road, the software implementation holds a significant role for protection. Join this session to understand what technology is out there to ensure that the driver is aware of the "truth" when it comes to the information that will be reported back.

Pankil Vyas, Senior Manager, Cyber Security, **Harman**

10:45AM

Networking Break

11:15AM

Modern Data Platform for the Connected Vehicle

Big Data, the Internet of Anything (IoAT) and the Connected Car have created a new Information Superhighway that fundamentally changes the relationship between automakers and drivers. Previously, automakers had an incomplete feedback loop after they sold a vehicle but the connected car has changed all of that. Now, automakers can establish a complete feedback from each vehicle that can constantly send sensor data from each car on how it is driven, how it responds to driving conditions, and how it might be improved in future models. With today's Information Superhighway, one of the key determinants of future success in the industry will be speed: how quickly and accurately can automakers capture and understand data, then use that insight to innovate the kinds of vehicles and mobility services that consumers expect?

Grant Bodley, GM, Global Manufacturing Industry Solutions, **Hortonworks**

Sponsored by **Hortonworks**

12:15PM

PANEL DISCUSSION: How to Be Mindful of Customer Safety While Fast Tracking the Advancements and Implementation of the Latest Technologies

Is the autonomous car closer than we expect? OEM and technology companies have begun to promise that the self driving car is right around the corner! Customers will hardly be able to contain their excitement, but how will this affect the critical infrastructural design and the distraction level of the driver? This technologically driven panel will discuss how advancements are increasing security throughout the car to ensure customer demand is met while still keeping them safe.

Gary Streelman, Director Advanced Engineering & New Concepts, **Magneti Marelli**

Joseph Kristofik, Technical Specialist Functional Safety DAS, **ZF TRW**

Cem Hatipoglu, Division Chief, **National Highway Traffic Safety Administration**

1:00PM

Networking Lunch

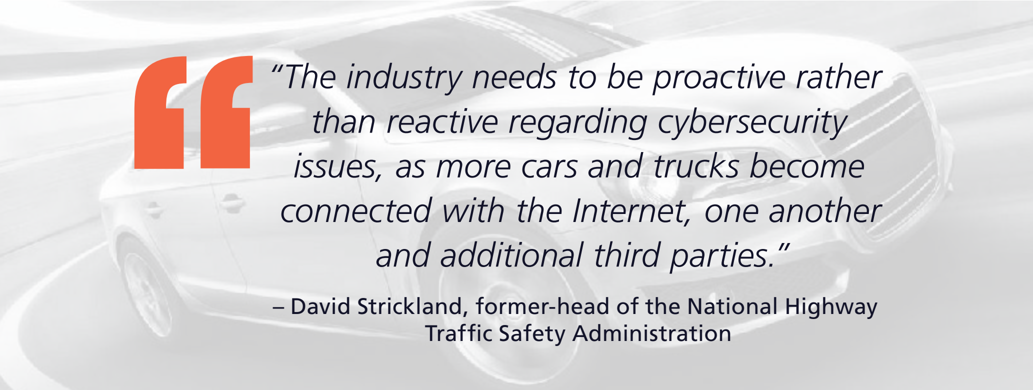
2:00PM

Connected Car Security: How Much is Enough?

With ever increasing car connectivity, we face a seemingly endless barrage of newfound electronic system vulnerabilities that exploit design oversights, software bugs, social engineering and leaked information. Attackers have the luxury of repeatedly prodding a system, needing only to find a single exploitable opportunity, whereas we must secure all paths into the system. But how much security is enough? In this session, we'll explore best practices for preventing remote infiltration, attempting to handle successful system intrusion, and as the last line of defense, mitigating malicious messaging on vehicle busses such as CAN. Join us to learn how to make informed, systematic, risk-based security decisions to safeguard the connected vehicle.

Brian Sutton, Embedded Systems Engineering Lead, **MicroSemi**

Sponsored by **MicroSemi**



> *"The industry needs to be proactive rather than reactive regarding cybersecurity issues, as more cars and trucks become connected with the Internet, one another and additional third parties."*
>
> – David Strickland, former-head of the National Highway Traffic Safety Administration

2:45PM

Implemented Regulations and the Emerging Technologies for Cyber Security

Cybersecurity rose out of necessity to protect these vital systems and the information contained within them. Applied to vehicles, cybersecurity takes on an even more important role: systems and components that govern safety must be protected from malicious attacks, unauthorized access, or anything else that might interfere with safety functions. Failure to tackle the cybersecurity challenge would threaten the technology-driven safety transformation we all want to achieve.

To do this, cybersecurity must be an integral part of vehicle engineering, manufacturing, and enforcement. In this session, hear from NHTSA about how the federal regulatory agency is laying the groundwork towards safeguarding the safety of vehicles in the face of emerging cybersecurity risks.

Cem Hatipoglu, Division Chief, **National Highway Traffic Safety Administration**

3:30PM

Networking Break

3:45PM

Coordinating Cybersecurity and Safety through Systems Engineering

In this presentation, we describe an approach to coordinate safety and cybersecurity development from a systems engineering perspective. Though the two areas are distinct and require different expertise for the analysis and process development activities, coordination and integration of the development activities is necessary to help ensure consistency and completeness between safety and cybersecurity, and to avoid interference between cybersecurity and safety countermeasures and design selections. We purport that the coordination is best addressed as part of the systems engineering process. The coordination of activities will be illustrated with a small example.

Barbara Czerny, Senior Technical Specialist Safety and Cybersecurity, **ZF TRW**

4:30PM

Chairman Closing Remarks

PRICING & REGISTRATION

OEMs and Tier 1 Suppliers Package	Standard
Main Conference	$2,495
All Access: Main Conference + All 3 Workshops	$3,895
Ford Site Tour	$549
One Workshop	$549

Vendors Package	Standard
Main Conference	$2,995
All Access: Main Conference + All 3 Workshops	$4,395
Ford Site Tour	$549
One Workshop	$549

Team Discounts*

Number of Attendees	Savings
3 to 4	10%
5 or more	15%

*Discounts apply to registrations submitted together, at the same time. Cannot be combined with any other discount

*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.

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.

Details for making payment via EFT or wire transfer:
JPMorgan Chase - Penton Learning Systems LLC dba
IQPC: 937332641
ABA/Routing #: 021000021
Reference: 24870.003

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.

REGISTER ONLINE, BY EMAIL, PHONE, FAX OR MAIL

Web: www.AutomotiveCyberSecurity.com
Email: enquiryiqpc@iqpc.com
Phone: 1-800-882-8684
Fax: 212-973-1042
Mail: IQPC
535 5th Avenue, 8th Floor
New York, NY 10017

LOCATION & LODGING INFORMATION

The Baronette Renaissance Detroit-Novi Hotel

27790 Novi Road, Novi,
Michigan 48377, United States

The special room rate of $169 has been established to make your reservation process easy. Simply call 1-800-468-3571 or 248-349-7800 and give the group name Automotive Cyber Security no later than March 1, 2016. In addition the special rate has been extended to three days before and after the conference.

CONNECT WITH US

ABOUT THE ORGANIZER

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 Powertrain, Electrics/Electronics, Chassis Systems and Car Body & Materials.

Membership is free. By becoming a member you have access to a plethora of industry-relevant information through expert interviews, white papers, our blog, presentations and podcasts. You will also find links to our upcoming automotive conferences focusing on current topics and future trends within the auto industry.

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. For more information, visit www.automotive-iq.com.