AUTOMOTIVE
CYBERSECURITY
DETROIT

ENSURING VEHICLE CYBER RESILIENCY IN 2019 & BEYOND

CONTRIBUTORS

Nicholas Multari, PhD
Principal PM, Cybersecurity
Pacific Northwest National Laboratory

John Krzeszewski
Chief Engineer of Cyber Security
Aptiv

Dr. André Weimerskirch
Vice President, Cybersecurity and Functional Safety
Lear Corporation

Automotive iQ

FORWARD

Ahead of the **Automotive Cybersecurity Summit**, taking place this March 27-29 in Detroit, we sat down with the members of our advisory board to discuss:

- The role of artificial intelligence in automotive cybersecurity and how it will evolve over the next five years
- Key objectives and priorities for cybersecurity in 2019
- How to most accurately secure V2X communications
- The largest cybersecurity threats facing the entire automotive industry today
- Why you can't afford to miss the upcoming Automotive Cybersecurity Summit

2019 ADVISORY BOARD MEMBERS:

Nicholas Multari, PhD
Principal PM, Cybersecurity
Pacific Northwest National Laboratory

Nicholas J. Multari is the principal program manager for research in cybersecurity at the Pacific Northwest National Lab (PNNL) in Richland, Washington. He establishes the direction and leads the execution of the various research projects resulting in a rigorous foundation upon which security concepts are matured and implemented.

John Krzeszewski
Chief Engineer of Cyber Security
Aptiv

John Krzeszewski is the Chief Engineer of Cybersecurity at Aptiv, where he and his team are responsible for cybersecurity architecture for IT and vehicle applications. He was selected as one of the U.S. representatives and chair, on the development of the upcoming SAE-ISO 21434 “Road vehicles: cybersecurity engineering” standard.

Dr. André Weimerskirch
Vice President, Cybersecurity and Functional Safety
Lear Corporation

Dr. André Weimerskirch is Vice President Cybersecurity and Functional Safety at Lear Corporation. Before that, André established the transportation cybersecurity group at the University of Michigan Transportation Research Institute (UMTRI), and co-founded the embedded systems security company ESCRYPT which was sold to Bosch in 2012.

HOW DO YOU SEE THE ROLE OF ARTIFICIAL INTELLIGENCE IN AUTOMOTIVE CYBERSECURITY EVOLVING OVER THE NEXT FIVE YEARS?

Nicholas Multari, PhD
Principal PM, Cybersecurity
Pacific Northwest National Laboratory

I can only see the role of AI increasing over the next several years. Although used today, as automobiles move up the autonomy ladder, the use of AI will have to significantly increase and improve. The situations they will have to withstand will potentially grow exponentially. This includes many situations that will be novel and have to be learned. The learning process could be sped up with the sharing of "experiences" between autos enabling fewer and fewer new situations being experience (potentially with negative consequences) by each individual auto.

John Krzeszewski
Chief Engineer of Cyber Security
Aptiv

Used to detect and defend against attacks in the vehicle. Likewise, I also see it being used to attack vehicles.

Dr. André Weimerskirch
Vice President, Cybersecurity and Functional Safety
Lear Corporation

AI is already used in the SOC/cloud to detect patterns that point to cybersecurity attacks. I don't believe that AI or machine learning will be used significantly inside of the vehicle to detect or prevent attacks, but deterministic rules will be applied in the vehicle. Those are more efficient and predictable.

AI/ML running in vehicles, e.g. to support automated controls, might become a target for attackers though. Hence such AI systems running in vehicles must be carefully considered, designed, and protected.

LEARN MORE ABOUT AI AT THE SUMMIT!

SESSION TOPIC:

CONSIDERATIONS ON THE USE CASE FOR AI & MACHINE LEARNING FOR AUTOMOTIVE DEFENSE

CLICK HERE TO LEARN MORE ON PAGE 12 OF THE AGENDA

TENTATIVELY, WHAT ARE YOUR KEY OBJECTIVES/ PRIORITIES FOR CYBERSECURITY IN 2019?

Nicholas Multari, PhD
Principal PM, Cybersecurity
Pacific Northwest National Laboratory

My top priority is **ensuring vehicle cyber resiliency**. This is based upon the assumption that complex systems will never be fully secured. Given the lines of code and functions in a vehicle and their connectivity, the expectation is there will always be software weaknesses that can be exploited by a determined attacker. However, the catastrophic failure by these complex systems can and will have significant impacts on the transportation sector as well as individual safety. Therefore, cyber resilience is required. The goal would be the continued functioning of critical safety components even in a completely contaminated environment. An example of minimum functionality would be determining an attack has successfully occurred and compromised the operation of the vehicle followed by a decision to immediately pulling over out of the flow of traffic, applying the brakes to stop, and turning off the engine. This will entail understanding the minimal safety functionality requirements, the components critical to this functionality, and the minimum connectivity required to protect the vehicle, passengers and pedestrians. In short, the minimum safety functionality must be resilient against all attacks.

John Krzeszewski
Chief Engineer of Cyber Security
Aptiv

Get practical information as how particular IDS/IPS systems actually perform in the field, as perhaps some early versions of them are in 2020 MY vehicles.

HOW CAN WE MOST ACCURATELY SECURE V2X COMMUNICATIONS?

Nicholas Multari, PhD
Principal PM, Cybersecurity
Pacific Northwest National Laboratory

The easy (but not really) is using encryption. The difficulty with encryption is with key management. However, to me, **the key to securing the V2X communications is the protection of the endpoints.** It is the endpoints that send and receive the messages. A malicious endpoint, regardless whether through compromise or a malicious user) can send messages (whether the communications is secured or not) to all resulting in their operating on faulty data. To attempt to detect malicious messages is by the use of multi-sourcing. That is, if your endpoint is reporting an issue but no others in the area are, the message may be considered malicious. However, if multiple endpoints are sending the messages on the same issue, the likelihood of it being valid is higher.

John Krzeszewski
Chief Engineer of Cyber Security
Aptiv

Using parsers that detect for invalid format and then leveraging existing signature checking. CRLs could be updated via cellular, to take advantage of the fact cellular coverage is extensive; that way the latest CRLs can be downloaded. Likewise, existing vehicles could report anomalous vehicles, for a server to analyze and determine if the reported vehicle should be added to a CRL.

Dr. André Weimerskirch
Vice President, Cybersecurity and Functional Safety
Lear Corporation

V2X communication security has been specified in several standards, and has been reviewed thoroughly. There are still some **open challenges around the detection of defect and misbehaving vehicles as well as operations of the underlying security credential system** though.

LEARN MORE ABOUT V2X AT THE SUMMIT!

SESSION TOPIC:
DELIVERING SECURE VEHICLE TO VEHICLE COMMUNICATIONS SECURITY FOR IMPROVED AUTOMOTIVE SAFETY

CLICK HERE TO LEARN MORE ON PAGE 14 OF THE AGENDA

IN YOUR OPINION, WHAT DO YOU BELIEVE TO BE THE LARGEST CYBERSECURITY THREAT TODAY FACING THE ENTIRE AUTOMOTIVE INDUSTRY?

John Krzeszewski
Chief Engineer of Cyber Security
Aptiv

Overworked/overloaded cybersecurity individuals (since everyone is understaffed since cyber people are hard to find and there is an insufficient number), thus the car companies may not look at the cybersecurity posture of vehicles as rigorously. This is more even urgent with the rise of autonomous vehicles, even level 2 and above, as they could be hacked to force a vehicle to steer into people/traffic.

Nicholas Multari, PhD
Principal PM, Cybersecurity
Pacific Northwest National Laboratory

Autonomous vehicles before we know how to fully secure them or make them truly resilient. Otherwise, I believe we have a disaster waiting to happen.

Dr. André Weimerskirch
Vice President, Cybersecurity and Functional Safety
Lear Corporation

I don't think there's a single threat we need to be concerned about. There are several opportunities though to improve cybersecurity, such as **continuously strengthen supply chain security and reducing the time it takes to fix software vulnerabilities.**

AS AN ADVISORY BOARD MEMBER AT THE UPCOMING AUTOMOTIVE CYBERSECURITY SUMMIT, WHAT IS ONE MESSAGE YOU HOPE ATTENDEES WILL TAKE AWAY FROM THE EVENT?

John Krzeszewski
Chief Engineer of Cyber Security
Aptiv

How we can work together, collaboratively, to solve the particular common problems/challenges.

Nicholas Multari, PhD
Principal PM, Cybersecurity
Pacific Northwest National Laboratory

In addition to trying to design in cybersecurity mechanisms into the vehicles of the future, we must consider that failsafe line resulting from also incorporating cyber resiliency concepts into the design. We will never reach the point where we can guarantee the security of our systems from all attacks. Therefore, they must be able to fail safely protecting the vehicle, passengers and pedestrians.

Dr. André Weimerskirch
Vice President, Cybersecurity and Functional Safety
Lear Corporation

Product security is a rather broad topic that goes beyond the cybersecurity engineering process, technical solutions, and protection of manufacturing sites. It also includes the supply chain, privacy protection and privacy regulations, protection of the development environment to avoid tampering with the product's design and implementation, developer's awareness and training, and many more aspects.

CONTINUE THE CONVERSATION AT THE SUMMIT!

AUTOMOTIVE
CYBERSECURITY
DETROIT

MARCH 27 - 29, 2019
DETROIT, MI

INTERESTED IN LEARNING MORE ABOUT THE UPCOMING SUMMIT?

COMPLEX PROTECTION. RAPID RESPONSE.

The **Automotive Cybersecurity Summit** features leading cybersecurity experts working in automotive, mobility and parallel sectors. We will discuss key essentials like threat modelling, building in physical security, AI and deep machine learning, cybersecurity throughout the supply chain, and much more!

Cybersecurity has become an important differentiator between auto makers, mobility and other transportation companies as these industries are challenged with emerging and growing cybersecurity threats and challenges in increasingly complex security environments with connectivity, ADAS, and autonomous tech.

You will be able to network with other security professionals across several sectors and at various senior and technical managerial levels. In the past, this summit has attracted 100 + attendees from industry to top management from various OEMs and Tier 1 suppliers, such as CEOs, Presidents, Vice Presidents, and Directors of Engineering/Seating and solution providers.

LEARN MORE:

DOWNLOAD AGENDA

VIEW SPEAKER FACULTY

VIEW PAST ATTENDEE LIST

SPONSORSHIP OPPORTUNITIES