9th International VDI Conference

Cyber Security for Vehicles

June 28-29, 2023, Frankfurt, Germany

- The Future Trends of Cyber Security
- Regulations, Standards & Processes
- Security for Automated Vehicles
- Connected Vehicle Security & Privacy Challenges
- Security of E-Mobility/ E-Vehicles

+ **International Best Practices**
+ **Panel Discussion**

Meet international Experts from:

ARGUS · Aston Martin · AUTOCRYPT · AVL · Bosch Engineering BOSCH · COM|CODE · Continental · CYRES CONSULTING · BB Dissecto · Hochschule RheinMain University of Applied Sciences Wiesbaden Rüsselsheim · irdeto · MAGNA Forward. For all. · MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY · NAVINFO · NXP · TÜV SÜD · virtual vehicle

An event organized by VDI Wissensforum GmbH
www.vdi-international.com/ 01KO907023

Supporting Experts

Dr. Mathias Dehm, Chief Product Security Officer, Continental AG, Germany
Prof. Dr. Christoph Krauß, Head of Automotive Security Research, INCYDE GmbH and Head of Research Group Applied Cyber Security Darmstadt, Darmstadt University of Applied Sciences, Germany
Prof. Dr. Jörn Eichler, Head of Security Engineering, Electric/Electronic Engineering, Volkswagen AG, Germany
Dr. Christian Köbel, Senior Project Engineer Cyber Security, Honda R&D Europe GmbH, Germany

Reasons to attend

Meet the whole automotive security ecosystem

Network with technical experts & key decision-makers from leading OEMs & suppliers

Learn where the industry is headed & how to stay ahead of the curve

Discuss technical challenges, current developments & newest solutions

Prepare for two days full of insights, contacts & new ideas

Exhibition / Sponsoring

If you want to meet with and reach out to the first-rate experts attending this VDI conference and to powerfully present your products and services to the well-informed community of conference participants, please contact:

Jasmin Habel
Project Consultant
Exhibitions & Sponsoring
Phone: + 49 211 6214-213
Email: jasmin.habel@vdi.de

Already confirmed Exhibitors:
EnCo Software GmbH
Kugler Maag CIE GmbH
TRUSTONIC LIMITED
VicOne Trend Micro Deutschland GmbH

About us

VDI

The Association of German Engineers (VDI) is one of the largest technical-scientific associations in Europe. Throughout the years, the VDI has successfully expanded its activities nationally and internationally to foster and impart knowledge about technology related issues. As a financially independent, politically unaffiliated and non-profit organization the VDI is recognized as the key representative of engineers both within the profession and in public.

Sponsoring Partner

CYRES
CONSULTING

VicOne
a Trend Micro Subsidiary

08:45   Registration & Welcome Coffee

10:00   Chair's Welcome & Opening Address
Dr. Mathias Dehm, Chief Product Security Officer, Continental AG, Germany

10:15   Beyond UN Regulation No. 155 - Upcoming Automotive Cybersecurity Compliance Challenges
- Overview on global cybersecurity regulations
- Landscape of compliance and conformity challenges
- The possible future of ISO/SAE 21434 and UN Regulation No. 155

Dr. Markus Tschersich, Product Cybersecurity and Privacy Office, Head of Security & Privacy Research and Governance, Continental AG, Germany

I. Regulations, Standards & Processes

10:45   The Cybersecurity Resource Gap – Our own Fault?
- Automotive industry stuggle to find cybersecurity experts for the implementation of new regulations
- Existing resources are currently rather focusing on paper-based compliance instead of improving cybersecurity practices
- Standards rely on safety-based processes and detailed documentation
- Threat modelling in ISO/SAE 21434 is complex and focusses on methods instead of people and collaboration

Florian Stahl, Team Manager Cybersecurity, AVL, Germany

11:15   Paving the Way to Certificate of Compliance for UN Regulation No 155: Insights/ Best Practices for conducting an Audit
- Practical insights and best practices for conducting an audit in accordance with UN Regulation No 155
- Examination of structures, procedures and processes based on the example of a luxury sports car manufacturer (Aston Martin Lagonda)
- Experiences and lessons learned as well as actionable practical tips (consulting perspective) - generally applicable for the establishment of a Cybersecurity Management System (CSMS)

Frank Langner, Manager Functional Safety and Cyber Security, Aston Martin Lagonda of Europe **& Manuel Sandler**, Partner, CYRES Consulting, Germany

11:45   Threat Analysis and Risk Assessment (TARA) Learnings from 250+ Cybersecurity Projects
- Our journey from component TARA to Vehicle System TARA
- There is no one-size-fits-all methodology - choose wisely
- Analysing the security of functions across multiple components

Gregor Joebstl, Project Security Manager, Bosch Engineering GmbH, Germany

12:15   Lunch

13:45   AUTOMOTIVE TARA: Challenges and Experiences of ISO/SAE 21434 and UNECE-R155 on Vehicle Level
- Threat Analysis and Risk Assessment on vehicle level
- Asset definition and attack path analysis at concept phase
- ISO/SAE 21434 vs. UNECE R155
- TARA perspectives in the supply chain

Dr. Klaus Kainrath, Senior Engineer Cybersecurity, MAGNA STEYR Fahrzeugtechnik GmbH & Co KG & **Nadja Marko**, Senior Researcher Dependable Systems, Virtual Vehicle Research GmbH, co-authors: Joaquim Castella Triginer & Dr. Helmut Martin, both: Virtual Vehicle Research GmbH; all: Austria

II. Future Cybersecurity

14:15   Post-Quantum Cryptography on Vehicle Network Processors
- When and how to migrate to PQC in the automotive domain
- Automotive requirements for PQC secure boot, secure update, and other protocols
- Impact of increased key size, code size & memory requirements on the system
- Hardware requirements for deploying PQC

Dr. Joost Renes, Cryptographer, NXP Semiconductors, The Netherlands

14:45   Post-Quantum Crypto Software -- Embedded and High-Assurance
- NIST recently selected 4 PQC schemes for standardization; upgrading to those schemes is a massive challenge
- pqm4 is a framework for testing and benchmarking PQC on Arm Cortex-M4 and includes optimized implementations of most NIST PQC schemes
- High-assurance crypto uses tools and techniques from formal methods to increase quality of (PQC) implementations

Peter Schwabe, Research Group Leader, Max Planck Institute for Security and Privacy (MPI-SP), Germany & Professor, Radboud University, The Netherlands

15:15   Networking & coffee Break

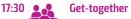**15:45   PQC and Crypto Agility from a Process Perspective**
- Overview of currently recommended transition/migration strategies
- Methods for determining the current state of readiness for transition
- Existing maturity models for crypto-agility as a prerequisite for transition to PQC
- Implications for supply chain lifecycle development, roles, and structures

Prof. Dr. Marc Stöttinger, Professor, Hochschule RheinMain, Germany

16:15   Panel Discussion: Securing the Future - Exploring the Driving Forces in Cyber Security for the Next Decades

17:00   End of Conference Day 1

17:30   Get-together

Dinner in a relaxed and informal atmosphere for in-depth conversations

09:25   Chair's Opening Address

III. Security Testing

09:30   Tales from a Penetration Testing Team - Insights from Zero-Day Automotive Vulnerabilities Discovered in Recent Years
- Introducing 4 vulnerabilities in 4 OEMs via 4 diverse communication methods:
- Arbitrary Remote Code Execution over CAN
- Fuzzing IPsec and SOME/IP-SD Communication Stacks
- Shaky Cryptography in Remote Command
- Remote and Persistent Vulnerability via Cellular Connection

Amit Geynis, Security Researcher, Argus Cyber Security, Israel

10:00   Fuzzing Test for SOME/IP Services: Strategy and Best Practices
- Introduction to Automotive Ethernet, SOME/IP and SOME/IP-SD
- SOME/IP fuzzing strategies: test environment setup, test cases generation, and pass/fail decision
- Real-world vulnerabilities discovered via fuzzing test
- Lessons learned from fuzzing test on the fields

Dr. Jonghyuk Song, Director of Vehicle Threat Research Lab, Autocrypt, Republic of Korea

10:30   The Results of Penetration-Testing Modern Electric Car
- Pen-testing processes for modern car
- Using hardware and software tools for cybersecurity testing
- Tested attack vectors
- Demo of post-exploitation scenarios

Sergey Razmakhnin, Head of Cybersecurity, NavInfo Europe, The Netherlands

11:00   ☕ Networking & coffee Break

IV.Security for Automated Vehicles

11:30   Fail-Operational Safety Measures in the Security Software Stack
- Safe and secure software architecture in scope of automated vehicles which require fail-operational software systems
- Safety measures for protection against unintended service interruption from security software modules
- Safety measures in the AUTOSAR security stack of real-time ECUs

Elisabeth Waitz, Senior Expert Cybersecurity & **Pavithra Tumkur Kumaraswamy**, Senior Architect Cybersecurity, both: Elektrobit Automotive GmbH, Germany

12:00   Homologation of Vehicles with Automated Driving Functions: Overview and current Challenges with Respect to Cybersecurity
- Overview on autonomous driving regulations in Germany an EU
- German Act for Autonomous Driving (AFGBV) versus EU regulations for Level 4 (2022/1426)
- Differences between series vehicles and single type approval

Dipl.-Ing Alexander Ersoy, Head of Automotive Security and Connectivity HAD, co-author: Jonas Herde, Senior Expert Safety and Regulations HAD, both: TÜV SÜD Auto Service GmbH, Germany

12:30   🍴 Lunch

V. Connected Vehicles Security & Privacy

14:00   The Necessary digital Forensic Capabilities for the Automotive Ecosystem
- The status of digital forensics in the automotive ecosystem
- How is the industry affected by forensics use cases and requirements?
- How can we address the existing and upcoming challenges associated with implementing forensic capabilities within vehicle technologies?
- Adoption of existing forensic frameworks for the automotive ecosystem

Markus Geier, CEO, ComCode GmbH, Germany; co-author: Parker Soares, Automotive Cybersecurity Specialist, ComCode GmbH, USA

14:30   Privacy-preserving Mobility Services in Connected Vehicles
- Privacy by Design
- From Privacy Requirements to Privacy Controls
- Regulations around the world (e.g. EU-GDPR)
- New standard ISO 31700-1:2023 "Consumer protection — Privacy by design for consumer goods and services"

Mario Hoffmann, Group Leader Cyber Security, ARRK Engineering GmbH

VI. Security of E-vehicles

15:00   Will the Charging ecosystem Built Today Last for Decades to Come?
- Automotive industry transitioning to EVs for a better environment: Biggest challenge is the rollout of the charging infrastructure
- Need for an open and secure charging ecosystem for EVs
- Easy charging as traditional refueling is the key to success
- Standards and regulations are gaining traction and regulators are supporting implementation, but the question – is it enough?

Juha Hytönen, Director of Embedded Security, Irdeto, The Netherlands

15:30   Conference Chair Closing Remarks

15:45   End of Conference

Become a speaker

Become a speaker at our international VDI Automotive Conferences. Make yourself known in the industry and discuss best practice examples with other international experts. We are looking for speakers on: Software Defined Vehicle, Autonomous Driving, E/E Architecture and Connected Off-Highway Machines. Please submit your topic to:

Annick Cathrin Pauwels
Product Manager International Business
Phone: +49 211 6214-8646
Email: Pauwels@vdi.de

Terms and Conditions

Registrations: Registrations for conference attendance must be made in writing. Confirmation of your registration and the associated invoice will be mailed to you. Please do not pay your conference attendance fee until you have received our invoice and its invoice number to be stated for transfer. German VAT directives apply. Please state your VAT-ID with your registration.

Conference venue
Relexa Hotel Frankfurt am Main
Lurgiallee 2
60439 Frankfurt am Main, Germany
Phone: +49 69/95778-0
Email: frankfurt.main@relexa-hotel.de

HRS
Das Hotelportal
You will find more hotels close to the venue at www.vdi-wissensforum.de/hrs

Hotel room reservation: A limited number of rooms has been reserved for the benefit of the conference participants at the Relexa Hotel Frankfurt am Main. Please refer to "VDI Conference". For more hotels: www.vdi-wissensforum.de/hrs

VDI Wissensforum service package: The conference package includes the conference documents (online), beverages during breaks, lunch and the get-together on June 28, 2023.

Conference attendance conditions and terms can be found on our website: www.vdi-wissensforum.de/en/terms-and-conditions/

Data protection: VDI Wissensforum GmbH captures and processes the address data of conference participants for their own corporate advertising purposes, enabling renowned companies and institutes to reach out to participants by way of information and offers within their own marketing activities. We have outsourced in part the technical implementation of data processing to external service providers. If you do not want to receive any information and offers in the future, you may contradict the use of your personal data by us or any third parties for advertising purposes. In that case, kindly notify us of your contradiction by using the email wissensforum@vdi.de or any other of the contact options mentioned.

Registration

9th International VDI Conference

Cyber Security for Vehicles

VDI

VDI Wissensforum GmbH | VDI-Platz 1 | 40468 Düsseldorf | Germany

Yes, I will participate as follows:

Participation Fee + VAT
☐ **VDI Conference 28.-29.06.2023**
(01KO907023) **€ 1990**

☐ I am interested in sponsoring and/or exhibition
☐ Participation Fee VDI-Members* Save 50 € for each Conference Day.
* For the price category 2, please state your VDI membership number

VDI membership no.	Title
First Name	
Last Name (Family Name)	
Company/Institute	VAT-ID
Department	
Street	
ZIP Code, City, Country	
Phone	Fax
Email	

Please state your invoice address if this differs from the address given

Participants with an invoice address outside of Austria, Germany and Switzerland are kindly requested to pay by credit card.
Please register at www.vdi-international.com. Your credit card information will be transmitted encrypted to guarantee the security of your data.