

Cybersecurity in the Automotive Domain Mobile Business II - Guest Lecture

Ahmad Sabouri | June 29th, 2017 | Goethe University Frankfurt

https://www.continental-automotive.com/

Corporate Systems & Technology





Security & Privacy Competence Center Corporate Systems & Technologies Public

Cybersecurity in the Automotive Domain Agenda





Security & Privacy Competence Center Corporate Systems & Technologies Public

"My" Continental Location Continental Teves | Frankfurt am Main





Security & Privacy Competence Center Corporate Systems & Technologies Public

Our Vision Your Mobility. Your Freedom. Our Signature.

Our world is made up of: Highly developed, intelligent technologies for mobility, transport and processing

We want to provide:

The best solutions for each of our customers in each of our markets For our stakeholders:

The most valuecreating, highly reliable and respected partner



We Shape the Megatrends in the Automotive Industry: Safety, Environment, Information, Affordable Cars



🔞 ntinental 🏂

Security & Privacy Competence Center Corporate Systems & Technologies Public

Continental Corporation

Over 140 Years of Innovation and Progress



Bateineitiereal **Spipipteiss**n

Nakagalistivitstilispapanded **Ootminutpinstilistis**aneticarc-**Oithtroumpinstiliser**bashosthye **Otfolijistigninstilistis**fotialtered **Santisangel/OfforGeenGare**s.





Security & Privacy Competence Center Corporate Systems & Technologies Public

Continental Corporation Overview 2017



🔞 ntinental 🏂

Security & Privacy Competence Center Corporate Systems & Technologies Public

Continental Corporation Overview 2016



Ontinental

Security & Privacy Competence Center Corporate Systems & Technologies Public

Continental Corporation Five strong divisions

	13% Conti <mark>Tech</mark>			22% Chassis & Safety	
Chassis & Safety	Powertrain	Interior	Tires	ContiTech	
Vehicle Dynamics	Engine Systems	Instrumentation & Driver HMI	PLT, Original Equipment	Air Spring Systems	
Hydraulic Brake Systems	Transmission 26%	Infotainment & Connectivity	PLT, Repl. Business, EMEA	Benecke-Kaliko Group	
Passive Safety & Sensorics	Hybrid Electric Vehicle	Intelligent Transportation	PLT, Repl. Business, The Americas	Compounding Technology	
Advanced Driver Assistance	Sensors & Actuators	Body & Security	PLT, Repl. Business, APAC	Conveyor Belt Group	
Systems (ADAS)	Fuel & Exhaust Management	Commercial Vehicles & Aftermarket		Elastomer Coatings	
			Commercial Venicle Tires	Fluid Technology	
	21% Interic)r	Two Wheel Tires	Power Transmission Group	
	interie	· ·		Vibration Control	

PLT – Passenger and Light Truck Tires



Continental – Achieving Success From Inner Strength Our BASICS

Our four values are the crucial element here



Trust

Passion To Win



Freedom To Act



For One Another



Cybersecurity in the Automotive Domain Agenda





Security & Privacy Competence Center Corporate Systems & Technologies Public

Increasing Complexity

Increasing number of ECUs

- > 1997: 5 ECUs in Audi A6
- > 2007: about 50 ECUs in Audi A4
- > today: about 80 to 100 ECUs

Change in ECU usage

- > Traditionally one task per ECU
- > New trend of
 - > distributing functions across ECUs
 - > Integration multiple functions on one ECU

Variety of Applications

- > Lane Assistance
- Collision avoidance
- Accident Reporting (eCall)
- > Autonomous and Cooperative Driving



ECU: Electronic Control Unit



Understanding Security





Security & Privacy Competence Center Corporate Systems & Technologies Public

Consequences from a lack of security

From Black Hat and Defcon

Researchers showed all manner of serious attacks on everything from browsers to automobiles

During the Hacking Conferences - "Black Hat Las Vegas & Defcon Las Vegas" Aug 2015 - a video was shown and distributed via social media.





Introduction to Automotive Security Consequences



"After this jeep hack, Chrysler recalled 1.4 Mill. vehicles for a security bug fix."

🔞 ntinental 🖄

Security & Privacy Competence Center Corporate Systems & Technologies Public

Stock Value Fiat Chrysler August 2015





Security & Privacy Competence Center Corporate Systems & Technologies Public

Introduction to Automotive Security Stock Value Fiat Chrysler August 2015

Lack of Security has a deep impact on a companies value

Even if the hack is done by only friendly scientists



Security & Privacy Competence Center Corporate Systems & Technologies Public

... and more attacks with increasing press perception

2004: DRIVING; Altering Your Engine With New Chip (NY Times)
 2003: Gentlemen, Start Hacking Your Engines (NY Times)

2002: How To Hack Your Car (Forbes)

- 2010: Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study (Rutgers, USC)
- 2010: Experimental Security Analysis of a Modern Automobile (Center for Automotive Embedded Systems Security)
- **2007:** Hackers can take over car navigation system (The Telegraph)
- 2005: RFID Chips in Car Keys and Gas Pump Pay Tags Carry Security Risks (John Hopkins University)
- 2005: Linux Bluetooth hackers hijack car audio (The Register)2005: Hacking the Hybrid Vehicle (Wired)

- 2016: Nissan Leaf electric cars hack vulnerability disclosed (BBC)
- 2014: A Survey of Remote Automotive Attack Surfaces (IOActive)
- 2014: Most Hackable Cars (CNN Money)
- 2014: How to Hack a Car (Vice)
- 2014: The Robot Car of Tomorrow May Just Be Programmed to Hit You (Wired)
- 2013: Digital Carjackers Show Off New Attacks (Forbes)
- 2013: Jury Finds Toyota Liable in Fatal Wreck in Oklahoma (New York Times)
- 2013: Adventures in Automotive Networks and Control Units (IOActive)
- 2013: Car Hacking: Your Computer-Controlled Vehicle Could Be Manipulated Remotely (CBS)
- 2013: How to Hack Your Mini Cooper: Reverse Engineering CAN Messages on Passenger Automobiles (Defcon 21)
- 2011: Can Your Car be Hacked? (Car and Driver)
- 2011: Comprehensive Experimental Analyses of Automotive Attack Surfaces (Center for Automotive Embedded Systems Security)
- < 2005 2005-2010 > 2010



Odometer Example: Good old times

Expertise	> Automotive mechanist			
Tools	> Specific tools or garage			
Time	> Hours	video: <u>https://www.youtube.com/watch?v=vOn-8GEnZJM</u>		
Evidence	> Mechanical Traces			

🔞 ntinental 🖄

Odometer Example: Nowadays



Ontinental

Introduction to Automotive Security Attackers and their Damage Categories

Thieves	> Stealing assets> Stealing vehicles
Owner/Driver	 Manipulating vehicle data Manipulating vehicle Settings Spoofing licenses
OEM/Tier-1	 Stealing business secrets Conducting product piracy
Software manufacturer	> Elevating privileges
Hacker, Virus, Malware	 Stealing of personal data Manipulating the functional safety

Damage Categories

> Property
> Image
> Business Model
> Legislation
> Know-How
> Reliability
> Functional Safety
> Privacy



Introduction to Automotive Security Trends on Automotive Products – IT Technology



> Simple mechanical vehicles change to intelligent, connected, and software-based IT-Systems

> Flexibility, compatibility, costs, and weight are driving the change



Trends on Automotive Products – Interconnectivity



- > Evolutionary step from closed system to a complex interconnected and interactive communication party
- > The need for an efficient and safe traffic regulation is one driver next to infotainment and internet connectivity.



Trends on Automotive Products – Scaleability of Attacks



- > Attacks are scaling from single manipulations of ECUs to organized network wide attacks
- > Driver for this development on various stakeholder (owner, companies, 3rd parties): fun, fame, sabotage



Automotive Security Threats

Increasing attack surface



🚺 🚺 🚺 🍈

Security & Privacy Competence Center Corporate Systems & Technologies Public

Cybersecurity in the Automotive Domain Agenda





Security & Privacy Competence Center Corporate Systems & Technologies Public

New Challenges of Automotive Megatrends Increasing Threats and Attack Potential at the Horizon

Electric Mobility

Autonomous Driving

Information



🔞 ntinental 🏂

Security & Privacy Competence Center Corporate Systems & Technologies Public

Megatrend: Electric Mobility

Infrastructure Necessary to be Protected

Charging Infrastructure

- Connects Automotive to the critical infrastructure "Electric Power"
- > Electromobility is highly depending on the availability of charging infrastructure
- Implications with NIS Directive Regulation on the horizon



Payment

 Needs to be secured to avoid financial harm for supplier and/or customer



Megatrend: Electric Mobility Attacks Based on Loss of Data Integrity

Attack on EV performance

- Different data sources used to extend range (weather, altitude difference, traffic volume)
- Manipulation can lead to unexpected performance of electronic vehicle

Attack on components

- Overheated battery triggered by manipulation of temperature sensor
- > Will cause financial harm



🙆 ntinental 🏂

Megatrend: Autonomous Driving SAE J3016 - Driving Automation Definitions

	SAE Level	Name	Steering, Acceleration, Deceleration	Monitoring of Driving Environment	Fallback Performance	System Capability (Driving Modes)
Human driver monitors the driving environment	0	No Automation	Human	Human	Human	n/a
	1	Driver Assistance	Human and System	Human	Human	Some driving modes
	2	Partial Automation	System	Human	Human	Some driving modes
Automated driving system monitors the driving environment	3	Conditional Automation	System	System	Human	Some driving modes
	4	High Automation	System	System	System	Some driving modes
	5	Full Automation	System	System	System	All driving modes



Security & Privacy Competence Center Corporate Systems & Technologies Public

Megatrend: Autonomous Driving

Automated Driving System takes over more responsibility

- Impact of errors/attacks increases due to higher range of functions
- Simple shut-down in case of attacks is not working
- > Need for redundancy and fallback systems
- Higher impact on privacy due to increased need of data collection and processing





Security & Privacy Competence Center Corporate Systems & Technologies Public

Megatrend: Information New Opportunities and Risks of Big Data

Collection, processing and connectivity

- > Improve driver assistant systems (Safety)
- > More attractive/interactive infotainment systems
- > Reduction of fuel/energy consumption
- > Mobility Services, Smart Cities, Smart Home

Arising Risks of Big Data

- > Increasing number of attack vectors
- > Compliance with different legal privacy frameworks
- > Higher attraction to data theft



🙆 ntinental 🏂

Megatrend: Information Over the Air is Enabler and Additional Risk

Opportunities

- Smart and fast way for bug fixing and security patches
- > Enables automotive app ecosystem
- > Provides live information

Attack Vectors

- > Connection interface can be attacked
- > Risk of infected automotive apps



@ntinental **☆**

Security & Privacy Competence Center Corporate Systems & Technologies Public

Cybersecurity in the Automotive Domain Agenda




Ensuring Device Reliability

Interplay of Functional Safety and Security Required

- > Safety a discipline with a long history in automotive
- Functional Safety and Security need to engage with each other to ensure high quality products
- > Both disciplines need to be considered by the organization.





Security & Privacy Competence Center Corporate Systems & Technologies Public

Differentiate Safety and Security A Functional Safety Perspective



Ontinental 🆘

Target: Intended functional behavior

Safety in use / Safety of the intended functionality

- > Is there any risk resulting out of the fault free functional behavior?
- > Actually not standardized, in discussion for ISO 26262 2nd ed.

Functional safety

- > Is there any risk resulting out of a faulty functional behavior?
- > Standard: ISO 26262

Security

- > Is there any risk resulting out of a faulty functional behavior resulting out of (criminal) intended or un-intended system changes?
- Partially reflected in ISO 26262 but only for "intended misuse", i.e. w/o criminal intention
 - \rightarrow sep. standard on the way: ISO-SAE 21434:2019 (ongoing)

Differentiate Safety and Security Security vs. Functional Safety

Functional Safety

 Protect human against threats proceeded from (known) technical systems.

Security (IT/Cyber)

 Protect a technical system against attacks (basically unknown) as well as disturbances from the environment or caused by human.





Security & Privacy Competence Center Corporate Systems & Technologies Public

Differentiate Safety and Security

Similarities between Safety and Security

Risk oriented approach

 What can go wrong? How likely is it? What will the consequences be? (note: differences in probability estimations)

Development process

 Safe and secure software is achieved by using a systematic development approach rather than reactive patching

Testing

 Comprehensive testing is essential for confidence in the final product

Redundancy

 Double instances of safety/security mechanisms does not necessarily lead to double safety/security

Ultimate objective

> Achieving a sufficiently safe/secure product

Culture and values

 Knowledgeable, motivated and committed management and employees is a success factor for achieving safe and secure products



Differentiate Safety and Security

Differences between Safety and Security

Classification of consequences

- In safety typically divided into several levels (e.g. SIL/ASIL/DAL)
- In security quite binary, system is either compromised or not

Threat analysis, risk assessment

- In safety we have pretty well known, static fault models and fault assumptions
- In security threats changes regarding motivation, knowledge and attack vectors

Non-experts understanding

- > In safety the consequences are easily understandable
- In security the threat models are often met with scepticism and might be judged as paranoid

Knowledge of experience

- In the safety domain there is a culture of discussion and sharing of experience
- In security, business actors tend to keep their experiences to themselves, thus efficiently slowing down the collective expertise



Challenges of Security in Automotive Variety of Challenges

Vulnerability in BMWs online-system ConnectedDrive



Compromised Entertainment Acceptable?

http://www.heise.de/autos/artikel/Sicherheitsluecke-in-BMWs-Online-System-ConnectedDrive-2533697.html 30.01.2015



Hackers remotely disrupt

a Jeep on the highway

Compromised Breaking System Acceptable?

https://www.wired.com/video/2015/07/hackerswireless-jeep-attack-stranded-me-on-a-highway/ 21.07.2015





Compromised Smart Phone Acceptable?

https://promon.co/blog/tesla-cars-can-be-stoler by-hacking-the-app/ 23.11.2016

ADAC-Investigation: OEMs collect Big Data



Compromised Compliance Acceptable?

ttp://www.heise.de/newsticker/meldung/ADAC-Intersuchung-Autohersteller-sammeln-Daten-inrossem-Stil-3227102.html

04.06.2016



Challenges of Security in Automotive Uncomfortable consequences in common

Tens of millions of airbags are defective. Even a minor fender-bender can cause these airbags to rupture, spraying metal shrapnel into drivers and passengers.

https://www.airbagrecall.com/ https://www.safercar.gov/rs/takata/takat alist.html

Recall Campaign FCA: 1.4M Vehicles 24.07.2015

Affected are certain vehicles equipped with 8.4-inch touchscreens a

- 2013-2015 MY Dodge Viper specialty vehicles
- 2013-2015 Ram 1500, 2500 and 3500 pickups
- 2013-2015 Ram 3500, 4500, 5500 Chassis Cabs
- 2014-2015 Jeep Grand Cherokee and Cherokee SUVs
- 2014-2015 Dodge Durango SUVs
- 2015 MY Chrysler 200, Chrysler 300 and Dodge Charger sedans
- 2015 Dodge Challenger sports coupes

Customers affected by the recall will receive a USB device that they software, which provides **additional security features** independer Alternately, customers may visit <u>http://www.driveuconnect.com/sof</u> Vehicle Identification Numbers (VINs) and determine if their vehicle



Challenges of Security in Automotive

Approaches to Address Challenges

Strategic Projects

Specific Products

Governance & Processes



- Generic ECU Security Requirements
- > V2X Security



- > Smart Keyless Entry
- Balancing requirements: comfort, performance, safety, security ... and costs(!)

Devergment Nalation SOP Production Generation Fraction Management Fraction Content Fraction

- Governance and Management Awareness
- Establishing standardized and harmonized processes (e.g. PLC, TARA/HARA, Common Language)

🛈 ntinental 🏂

Cybersecurity in the Automotive Domain Agenda





Security & Privacy Competence Center Corporate Systems & Technologies Public

Standardizing Cybersecurity Engineering Goals of the Initiative

The future standard shall...

1

- Give uniform definition of notions relevant to automotive security
- 2
- Specify minimum requirements on security engineering process and activities and define – wherever possible – criteria for assessment



Describe the state of the art of security engineering in automotive E/E development

- **Targeted effects on automotive industry**
 - Common and internationally agreed understanding of automotive cybersecurity engineering
 - > Sufficient rigor as reference for legislative institutions; ensure legal certainty



Standardizing Cybersecurity Engineering Goals of the Initiative: A Common Language





Goal

Current Situation

Standardizing Cybersecurity Engineering Goals of the Initiative: A Common Language

The future standard shall...

 Give uniform definition of notions relevant to automotive security

- Generate and foster a common and internationally agreed understanding of automotive cybersecurity engineering
- > Enable and improve cooperation in development, manufacturing and maintenance of products
- > Allow for efficient security processes





Goal

Targeted Effects

Standardizing Cybersecurity Engineering Goals of the Initiative: Minimum Set of Requirements

The future standard shall...

 Specify minimum requirements on security engineering process and activities and define – wherever applicable – criteria for assessment

- Uncertainty about level of security
- Avoidance of communication on security





Goal

Current Situation

Security & Privacy Competence Center Corporate Systems & Technologies Public

Standardizing Cybersecurity Engineering Goals of the Initiative: Minimum Set of Requirements

The future standard shall...

 Specify minimum requirements on security engineering process and activities and define – wherever applicable – criteria for assessment

- Achieve sufficient rigor in order to be accepted as reference for legislative institutions etc. and ensure legal certainty
- > Enable and improve cooperation in development, manufacturing and maintenance of products
- > Allow for efficient security processes





Goal

Targeted Effects

Security & Privacy Competence Center Corporate Systems & Technologies Public

Standardizing Cybersecurity Engineering

Goals of the Initiative: State of the Art

The future standard shall...



Describe the state of the art of cybersecurity engineering in automotive E/E development



- Uncertainty about security levels
- Traditional IT Security management processes not feasible





Standardizing Cybersecurity Engineering

Goals of the Initiative: State of the Art

The future standard shall...



Targeted Effects

Describe the state of the art of cybersecurity engineering in automotive E/E development

- > Raise automotive cyber security to the next level
- Establish automotive cybersecurity as a proper engineering discipline
- Generate and foster a common and internationally agreed understanding of automotive cybersecurity engineering





Road Vehicles – Cybersecurity Engineering Towards a joint ISO/SAE Standardization Project





Standardizing Cybersecurity Engineering ISO/SAE 21434 – Overview

Joint Working Group

Working Groups within ISO

- > ISO/TC22/SC32/WG11 Cybersecurity
- > JWG for ISO/SAE Cybersecurity Engineering

Co-Convenors

- > SAE: Lisa Boran (Ford, US)
- > ISO: Gido Scharfenberger-Fabian (carmeq/VW, DE)

Expert Groups

> 12 national delegations are involved

Standard

- > ID: ISO/SAE 21434
- > Title: Road vehicles Cybersecurity Engineering

Document

Scope

- > Requirements for cybersecurity risk management
- > process framework
- Common language
- Road vehicles (pre-defined by TC22)

Expected Publication Date

Begin of 2020



Structure and Organization

🗿 ntinental 🏂





Security & Privacy Competence Center Corporate Systems & Technologies Public

Standardizing Cybersecurity Engineering Security in the whole Product Life Cycle



🔞 ntinental 🏂

Security & Privacy Competence Center Corporate Systems & Technologies Public

V-Model: Security & Privacy



🙆 ntinental 🏂

Security & Privacy Competence Center Corporate Systems & Technologies Public

V-Model: Security & Privacy



🙆 ntinental 🏂

Threat Analysis and Risk Assessment (TARA*)



Security & Privacy Competence Center Corporate Systems & Technologies Public

🗿 ntinental 🏂

Scope and Timeline ISO/SAE 21434 – Project Groups



🗿 ntinental 🏂

Security & Privacy Competence Center Corporate Systems & Technologies Public

Scope and Timeline ISO/SAE 21434 – Overall Schedule



🔞 ntinental 🏂

Road Vehicles – Cybersecurity Engineering

Outreach and Interaction

Liaison with ISO/IEC JTC1/SC27

> Development of 27xxx standards series, Common Criteria ISO 15408 and further standards of relevance to our project

Liaison with ISO/TC22/SC31 Road vehicles – Data communication

 Development of several automotive standards that include cybersecurity mechanisms specifications

Exchange with UNECE WP.29 TF CS/OTA

 Prepares rules for vehicle cybersecurity, potentially relevant for type approval

Exchange with NHTSA





Cybersecurity in the Automotive Domain Agenda





Entry Possibilities at Continental This is Continental



- > Truly international team around the globe
- > Performance-oriented working atmosphere
- > Early responsibility and exciting job challenges
- > Achieving exceptional results through passion
- > Open & informal culture: open doors & open minds
- Innovative Technology
- > Significant contribution to sustainable mobility



Entry Possibilities at Continental From Internship to Permanent Position





Security & Privacy Competence Center Corporate Systems & Technologies Public

Entry Possibilities at Continental

Internship and Thesis

Requirements:

- > Apply 2 to 3 months before your preferred internship start date
- > Duration: 3-6 months
- Current certificate of matriculation
- > Very good language skills in English
- Proficient experience in working with MS Office (esp. Word, Excel, Power Point)

Take your chance!

Apply online:





Entry Possibilities at Continental Continental Trainee & Graduates Programs





Security & Privacy Competence Center Corporate Systems & Technologies Public

Entry Possibilities at Continental Overall Information Continental Trainee Programs





Security & Privacy Competence Center Corporate Systems & Technologies Public

Entry Possibilities at Continental Overall Information Continental Trainee Programs





Security & Privacy Competence Center Corporate Systems & Technologies Public

Continental Entry Program Overview



START MODULE C.OnBoard

BASIC MODULE Continental Entry Conference (CEC)

Optional Modules

- > Business Decisions (Basics)
- > Effective Presentations
- Team Excellence
- > Self Management
- > Cross-cultural competence



Developing Talent "Across Borders"... Cross Moves



... be manager of your own talent

- > Establish corporate thinking
- > Generate new networks
- > Improve your skills and expertise
- > Increase intercultural competence



Ontinental

Security & Privacy Competence Center Corporate Systems & Technologies Public

Application process





Online application

via Continental Career Homepage™

Recruiting process

Telephone interview or assessment center or personal interview

Final formal offer


Have we sparked your interest? Then spark ours!

www.careers-continental.com

www.facebook.com/ ContinentalCareer

www.continental-people.com





Corporate Employer Branding & Strategic Recruiting Public June 29, 2017 Ahmad Sabouri, © Continental AG

Corporate Systems & Technology Contact Details



Specialist Security & Privacy

Ahmad Sabouri

Continental Teves AG & Co. oHG Cross Divisional Systems Security & Privacy Competence Center Guerickestraße 7 60488 Frankfurt am Main, Germany Phone: +49 69 7603-1303

eMail: ahmad.sabouri@continental-corporation.com



Security & Privacy Competence Center Corporate Systems & Technologies Public

June 29, 2017 Ahmad Sabouri, © Continental AG