The Auto Industry’s Paradigm Shift^3

Kai Thomsen
whoami

- Kai Thomsen, DFIR lead @ AUDI AG
- Background in Network Admin & Design, IT Security, IT Continuity
- For the past 6+ years trying to bridge the gaps between ICS/ITsec, and now Automotive/ITsec
Disclaimer

The views expressed here are my own and do not in any way represent the views of my employer, AUDI AG.
Buzzword Warning!

But I wanted to give you a glimpse of what our Sales & Strategy are currently talking about.
Assisted Driving

Electric Vehicles

Ride Sharing
On-Demand Payed Features and Upgrades

• They are already here! Tesla Ludicrous Speed Mode.

• Automakers are planning more of these in the near future

• They depend on a lot of crypto capabilities inside a car’s control units

• As far as I know car development, there are certainly „cheat codes“ for testing

• This is a perfect monetary reason to get into car hacking. Get features for free!
Why Paradigm Shift?

• Assisted/Autonomous Driving, the switch from combustion to EV, Ride Sharing/Car Sharing instead of ownership are fundamentally changing personal transportation

• Enablers: Internet, Big Data, Machine Learning. Yes, welcome to buzzword heaven ;-) 

• As in other industries before, the impact of IT will change the automotive industry in very fundamental ways 

• Software moves from a differentiating factor in certain features to the foundation of vehicles and transportation 

• In other words: very soon you are not buying just a car, but rather some form of personal transportation service that might or might not include car ownership.
Safety vs. Security

I like this nuanced definition on safety vs. security espoused by Robert Bates of @mentor_graphics. #medsec

I like this definition too :)
Safety and Security

- Safety: ISO/IEC 26262 Software Verification Requirements

- Security: ???

- Well, there are the Auto-ISAC „Automotive Cybersecurity Best Practices“ Guidelines. @MalwareJake has a pretty good review on his blog ([http://malwarejake.blogspot.com/2016/07/automotive-isac-cybersecurity.html](http://malwarejake.blogspot.com/2016/07/automotive-isac-cybersecurity.html) and [http://malwarejake.blogspot.com/2016/07/automotive-isac-cybersecurity_25.html](http://malwarejake.blogspot.com/2016/07/automotive-isac-cybersecurity_25.html))
Software Safety Requirements vs. Agile Web 2.0 Scrum Development
Suppliers vs OEM’s

- Consider that in a modern car 75% of all parts come from external suppliers.
- A supplier is sometimes the *only* supplier for a certain part.
- Most of the time a supplier is chosen because he is the cheapest.
- I have no idea which is worse security wise ;-) 
- OEM’s specialities are design, integration, and the car body.
Who owns the data?

- In your car
- In a shared ride
- In a rental or shared car
- And what about on-demand features?
What are the trust boundaries?
Autonomous Driving

Opens new roads for old crimes (theft, extortion, kidnapping, …)
It will change transportation in ways we cannot really predict. Singularity anyone ;-)?
Lifecycle

- Designing and building secure devices is a hard problem.

- A car’s lifecycle is comparable to that of ICS (15 years)

- What’s needed is an architecture that separates between components that must be easily swappable/upgradeable for security reasons and safety components.

- But keep in mind: safety components can’t be changed without (very) extensive testing. Which takes time. So much for agile.
Ecosystem

- Remember: most car parts come from suppliers. As does most software.
- Internet services consumed in modern cars’ entertainment systems come from all over the place.
- Mobile devices and peripherals get connected via Bluetooth, Wifi, and OBD II all the time.
- Enthusiasts “optimize“ their vehicles.
- Very soon cars will talk to other vehicles and transportation infrastructure. EV’s already talk to charging stations and „phone home“ to optimize their charging profiles.
What needs to be done

• Develop/adjust Risk Assessment Methodologies to cover the whole Connected Car ecosystem

• Secure coding guidelines

• Standardized, modular, upgradeable architectures for vehicle infotainment and communication systems

• Assessments, Audits, Pentests, Red Teaming to find those bugs before the bad guys do

• Develop IR and forensics procedures and technologies and build up IR teams

• Somewhat, somehow, somewhere these things are being done. But with too little transparency and standardization. The NIH syndrome is strong in the auto industry. As are regulation and protectionism.

• Yes, all of this sounds familiar. But remember the last slide? The difference to other areas of ITsec is the complexity of the ecosystem.
This might be one way to get started
The show is over. We are safe now ;-)

As much as I appreciate the work done by @0xcharlie and @nudehaberdasher their hacks are not very practical. Criminals either want to steal cars or DoS a car’s functions to extort money. The real fun hasn't even started yet.
So much to do, so little time.

Thank you for yours!

Questions?
Twitter: @kaithomsen, Email: iamtkai@gmail.com