Closing the Gap
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
- SANS Instructor for ICS515 (ICS Active Defense and Incident Response)
Disclaimer

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

Electric Vehicles

Ride Sharing
Safety vs. Security

- Safety: protect the world from the car
- Security: protect the car from the world
The role of (IT) Security

- What are my business risks?
- What threats am I facing?
- How do I keep the threats from realizing those business risks?
- Finally: do something about countering the threats!

In other words: security is about understanding your environment and how to keep it from doing you harm.
Threats

Does your IT Security team already think this way? Or is it still rather GRC-driven?
Perceived Risk vs Actual Threat
Thinking like an Attacker

- Systems are most vulnerable where different modules meet
- Especially when these modules were created under widely differing assumptions and constraints
- Why do cars get attacked? Today mostly theft and fraud
This cyber thing might introduce new criminal business models 😊
Agile meets ISO26262
Of course this doesn’t only apply to cars 😊
We’ve been saying software is the real differentiator in modern vehicles for long time. Why doesn’t it get the same attention as design and engines?
Attack Surface
Cultural Differences

- Language
- Development styles
- Requirements / Constraints
- Management Style
- Appreciation
- NIH Syndrome
How to close the Gap

The German approach 😊
How to close the Gap

• Have teams spend time together
• Start with small projects
• Learn the other team’s area of expertise enough to at least have meaningful conversations
• Don’t forget to involve Management
Ownership Questions

• Who owns vehicle safety in your organization?
• Who owns vehicle and connected systems security?
• Who owns IT Security responsibilities?
Ownership

Ownership for IT security issues needs to be with the managers responsible for developing and operating IT systems and components!

IT Security teams are responsible for governance, consulting, and active defense.
Risk Assessment Methods

- Most RA Methods barely work in our complex corporate environments, they will fail in a world of interconnected (semi-)autonomous transportation systems.
- IRAM2: ❔ maybe for the common language.
- For evaluation of complex systems, look at work done at USAF, USACE, DARPA, Fraunhofer Gesellschaft.
Attack Trees

- A formal way of modeling threats against computer(ized) systems
Keep this in Mind

„For every security problem there is a solution that is simple, elegant, and wrong.“
- Dan Geer, Cybersecurity as Realpolitik, Blackhat 2014 Keynote
Can we build secure systems at all?

A tentative yes 😊
Things that Work

- Isolation (Sandboxing, ASLR, DEP)
- Separation (ACLs, Network Zoning)
- Signed Code
- Good update procedures (never forget that lifecycle 😊)
- These are well-known methods; Google will find you lots of papers...
Things that don’t Work

- Do not rely on IDS’ses and other magical boxes
  - IDS’ses are useful in Active Defense situations
  - There is no Incident Response Team for your car
  - Trying to fully automate IDS runs you against unsolvable IT problems (Halting Problem, P=NP, O(n²))
  - Machine Learning isn’t ready for this - yet
If we do this right...

LITTLE BOBBY

ARE SELF-DRIVING CARS DANGEROUS?

NO-- BUT A BETTER QUESTION IS ARE THEY LESS DANGEROUS THAN HUMAN DRIVERS.

AND WITH PEOPLE TEXTING WHILE DRIVING I WOULD SAY YES!

by Robert M. Lee and Jeff Haas

MAYBE I SHOULD HAVE MY CAR STOP UPDATING ITS FACEBOOK STATUS THEN.
Take-Aways

• Make sure that your IT Security has the right level of maturity
• Enable vehicle R&D and IT Security teams to become a team of teams
• Find the right risk & threat modeling methodologies for your organization
• Better architecture and software quality will actually help
There’s never enough time.

Thank you for yours!

Email: iamtkai@google.com, Twitter: @kaithomsen