PENTESTING CARS
Improving Security by Breaking it
WHO AM I

- Gerhard Klostermeier
- IT security consultant, Pentester
- B.Sc. IT security
- Specialized in
  - Hardware hacking
  - IoT / wireless systems
  - NFC/RFID
  - Car IT security
  - Android apps
SYSS GMBH

- Founder and CEO: Sebastian Schreiber
- Founded in 1998
- Over 100 employees
- Located in Tübingen, Germany
- Services
  - Pentest
  - Digital forensics
  - Trainings
  - Live hacking
IT SECURITY

- Authentication & Authorization
- Integrity
- Confidentiality
- (Availability)
Live Hack
A HISTORY OF CAR HACKS

- 05.2015: Auto, öffne dich! Sicherheitslücken bei BMWs ConnectedDrive
- 07.2015: Hackers Remotely Kill a Jeep on the Highway - With Me in It
- 07.2015: General Motors: Hacker knackt OnStar-Fahrzeugsystem
- 08.2015: Hacker's $30 Device Unlocks Just About Any Keyless Entry Car
- 03.2016: Radio Attack Lets Hackers Steal 24 Different Car Models
- 08.2016: Sicherheitslücke bei 100 Millionen Autos entdeckt
WHAT NOW?

- Nearly every IT system needs security
- But: there is no such thing as a 100% secure system
- What now?
  - IT security is a process not a status
  - IT security has to be part of every IT-related process
  - The IT security of systems must be checked on a regular basis
HACK TO IMPROVE

- Hacking is a good thing
- Knowing your IT security issues is a good thing
- You can’t fix issues that you are not aware of
- Hacking is one of the few ways to compare the desired condition with the actual state

→ Go, get your cars hacked
IT SECURITY FOR CARS

- IT security for cars is hard
  - Complex systems with 100+ computers (ECUs) per car
  - Long lifespan
  - Long development cycles
  - Access for service/updates
  - Safety often depends on security
  - Limited computing power
  - Huge attack surface
IT SECURITY FOR CARS

Source: https://argus-sec.com/attack-surface/
PENTESTING CARS

- Pentesting cars is hard
  - Complex systems / time consuming
  - Every aspect of a car is important (e.g. even how it is produced)
  - Lots of “security through obscurity”
  - Car industry is not very cooperative when it comes to pentests
  - Less generic tools because every car is different
CONCLUSION

- Think of IT security as early as possible (security by design)
- Make IT security a part of every IT-related process
- Don't blame the developers, IT security is a task for the management
- “Development Department as a Hacker Space” - Jürgen Belz, Senior Consultant Safety & Security, PROMETO GmbH
- Check your security (pentest)
  - Improve security by breaking it
  - Hacking is a good thing
  - Go, get your cars hacked
Thank you