Car Manufacturer meets Security Community

Impressions from Germany's First Car Bug Hunting Event

#whoarewe

- Kevin Schaller | kschaller@ernw.de
  - Senior IT-Security Researcher & Analyst @ ERNW GmbH
  - 9 Years of experience in IT-Security
  - Researcher, primarily focused on Web, Mobile & IoT
  - Team lead of Mobile & IoT Security

#whoarewe

- Dr. Karsten Schmidt | karsten.schmidt@audi.de
  - Senior Security Engineer @ Audi AG
  - 4 Years of experience in Telecommunications
  - More than 15 years in the Automotive Industry
  - Primary focus now on network and hardware security

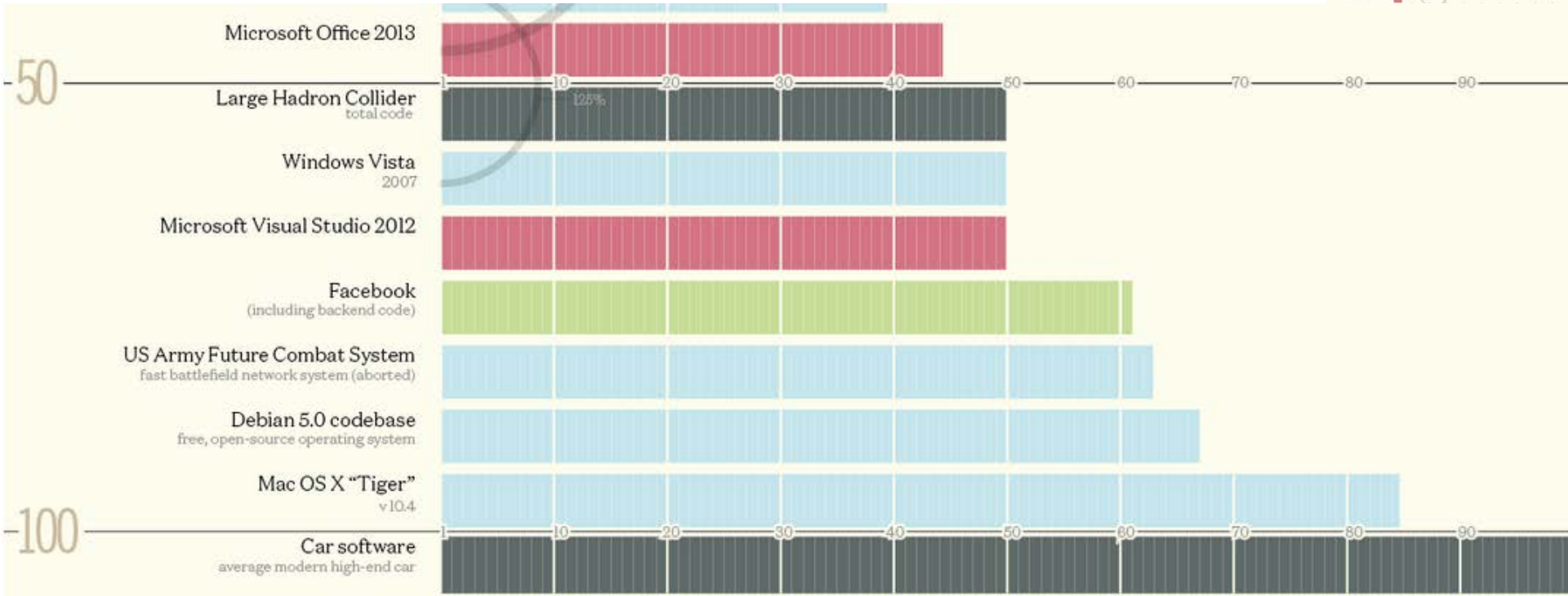
Agenda

- Motivation
- Organisation of a Bug Hunting Event
- Impressions of the Event
- Understanding the Automotive Domain
- Conclusion & Takeaways

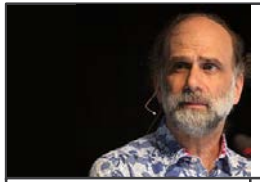
Motivation


BOSCH

Software


Microsoft Office 2013
50
Large Hadron Collider
total code
125%
Windows Vista
2007
Microsoft Visual Studio 2012
Facebook
(including backend code)
US Army Future Combat System
fast battlefield network system (aborted)
Debian 5.0 codebase
free, open-source operating system
Mac OS X "Tiger"
v 10.4
100
Car software
average modern high-end car
1
10
20
30
40
50
60
70
80
90

Challenges – Security as a Moving Target



"Complexity is the enemy of security.
As systems get more complex, they get less secure"
Bruce Schneier

A system is only as secure as its weakest link

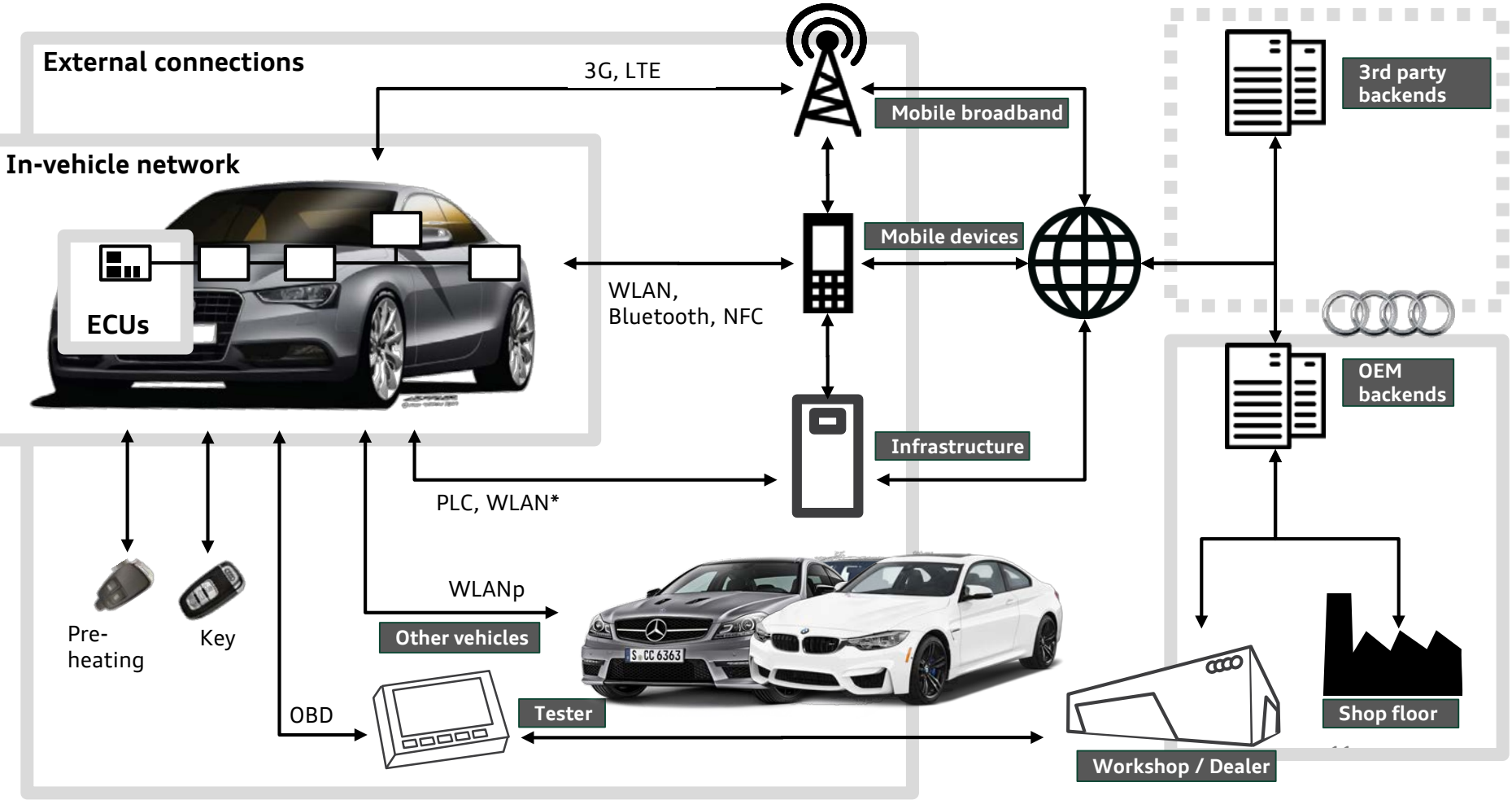
A Bug is hard to find
(attackers have time, developers don't)

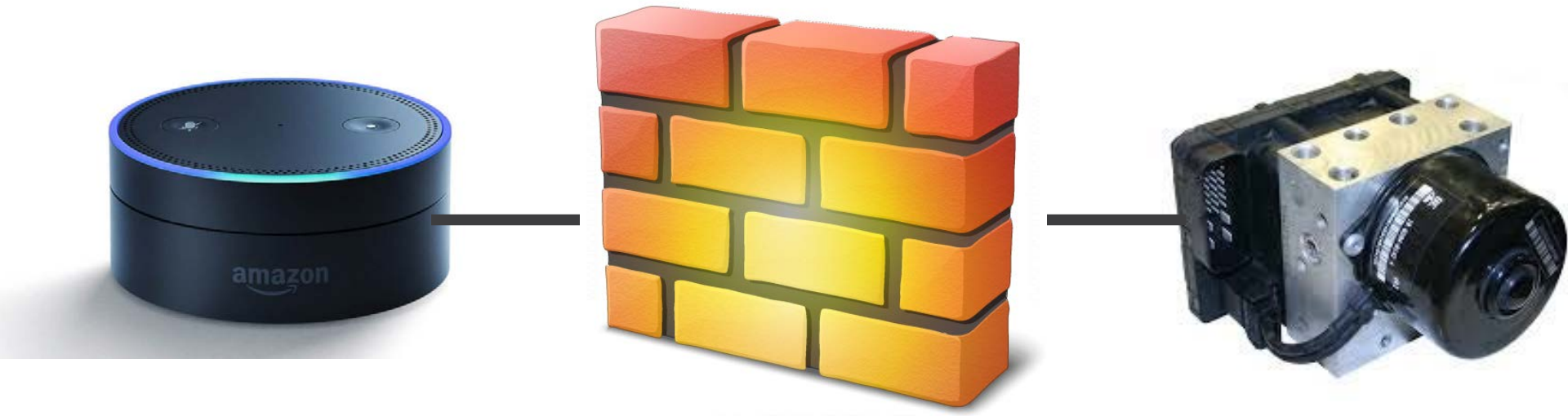
Only one entry point needed

Security by design = essential
Software (alone) cannot protect software

Focus Security: Vehicle, external connections and endpoints

Focus IT-Security:
IT-Systems + Endpoints





It works for me…..

What could possibly go wrong?

It’s All about Trust

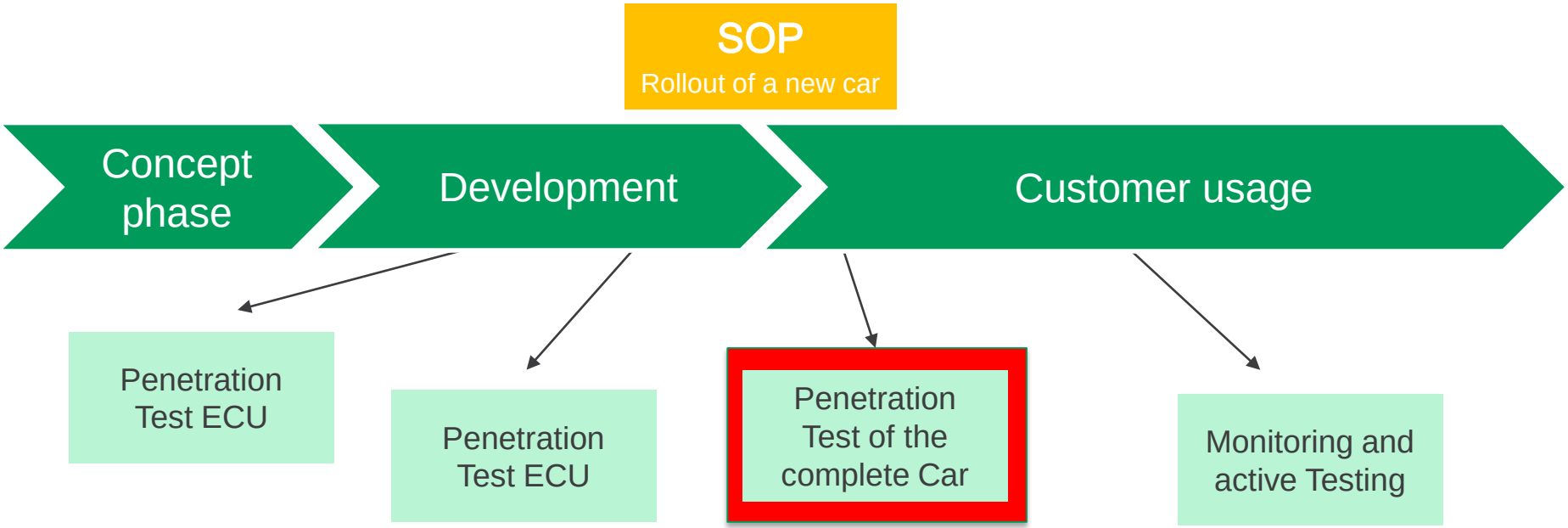
- Security from the users perspective → I can trust the car
- Security from the OEM perspective → Build trust in an economic manner!


SC34


Entsperren:
Nach oben schieben


Q key
The Keyless Scanner System

Overall Concept

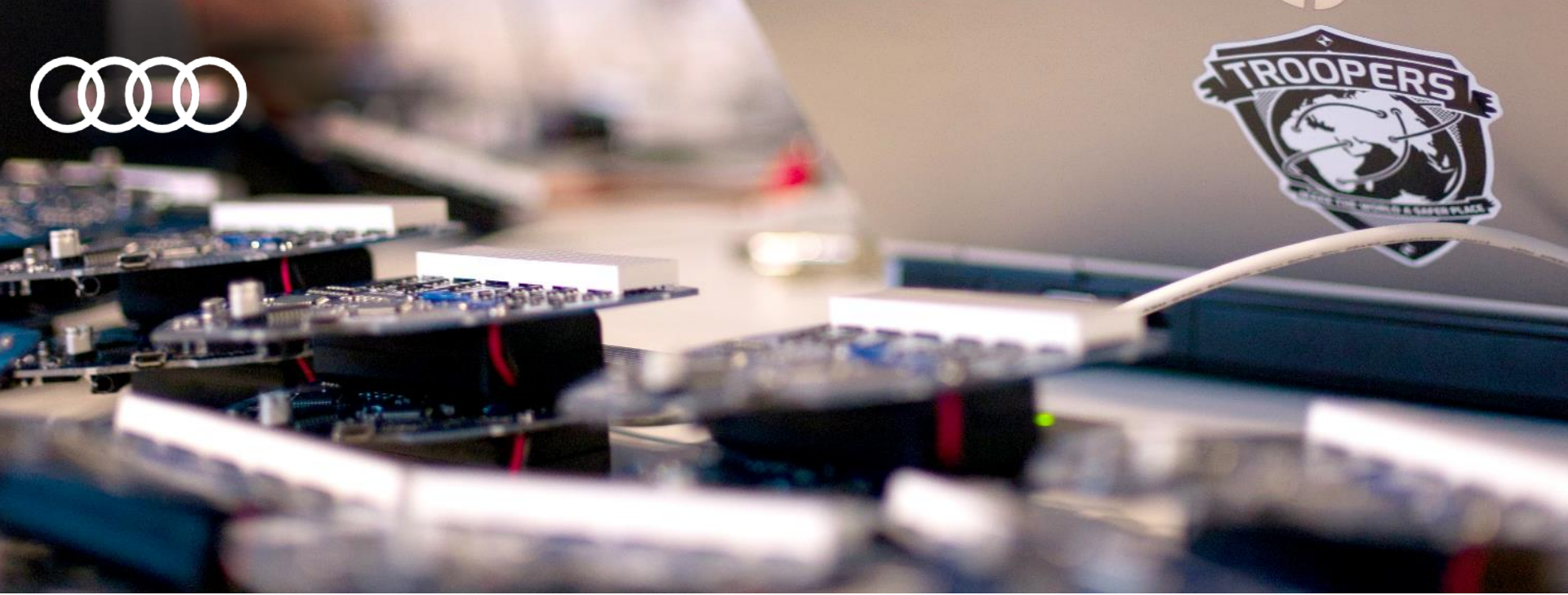


- Security Testing is already a defined part of the development cycle
  - Security Risk analysis in the beginning of the development process
  - Pentest for ECU and functions ongoing

    → How to improve?

Core Motivation

- Due to the complexity of cars, security assessments take huge amounts of time to reveal in-depth weaknesses
- Therefore, achieving knowledge exchange between security and (automotive) engineering community will bring both sides further
- → Knowledge exchange is the primary goal



Organisation of a Bug Hunting Event

Most Important Question

- What to do with the findings?
- Legal dept. vs. security community

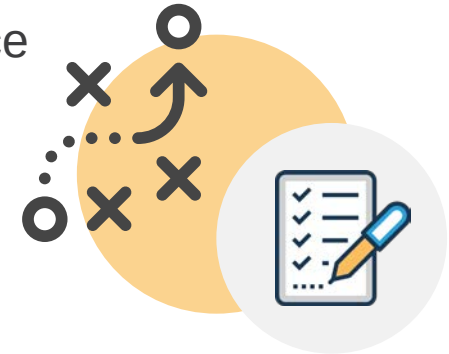
- In terms of our core motivation *Knowledge Transfer*, responsible disclosure would be the best way to go
- … along with publishing the results and methodologies used

How to Organize a Bug Hunting Event?

- Get and meet all legal requirements
- Set up a Bug Hunting policy
  - Definition of goals
  - How to submit the bugs?
  - What about third-party bugs?
  - Definiton of the scope
  - Definition of “out of scope” systems
  - Mention “worst case scenarios”
  - Define finding categories along with rewards

Defining the Mode

- Two weeks
- One huge garage with all necessary tools in place
- Full access to the site for all Bug Hunters
- Invite-Only
- 10-20 Bug Hunters
- Two Vehicles
- Several work spaces with *test racks*



Defining the Scope

- ECU-View
  - Central computer (MIB)
  - ConBox and central gateway
  - Engine immobilizer
  - Central driving assistance ECU
  - Charging Infrastructure
- Network view
  - Ethernet VLAN Architecture (IPv6-based!)
- External (incoming) connections
  - Conbox into Car
  - All telco interfaces
  - GPS, Radio (DAB+), etc...

Defining the Worst Case Scenarios

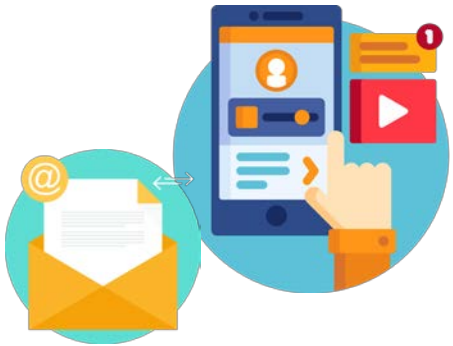
- Remote control of the car
- Battery overload → physical damage/explosion
- Function-on-Demand feature activation
- User data extraction (i.e. over air-interfaces)

Rewards

- Jury, consisting of members of both parties
- From 500 to 15’000 Euro, depending on the impact, the likelihood, the “attack path”, etc.
- Highest rewards for
  - Buffer overflows
  - Authentication bypasses
  - Vertical privilege escalation

Bug Hunters

- Wrote emails to ~25 internationally known members of the IT security community (& Troopers family ;-))
- Some did not want to attend due to moral reasons
- Eventually, the team consisted of 15 Bug Hunters



Impressions & Outcome of the Event

Schedule

- 08.10. – Bug Hunting Start – Introduction Workshop
- 09.10. – Bug Hunting
- 10.10. – Special Event #1
- 11.10. – Bug Hunting
- 12.10. – Intermediate Status Workshop
- 13.10. – 16.10. – Bug Hunting
- 17.10. – Special Event #2
- 18.10. – Bug Hunting
- 19.10. – Bug Hunting End – Final Workshop

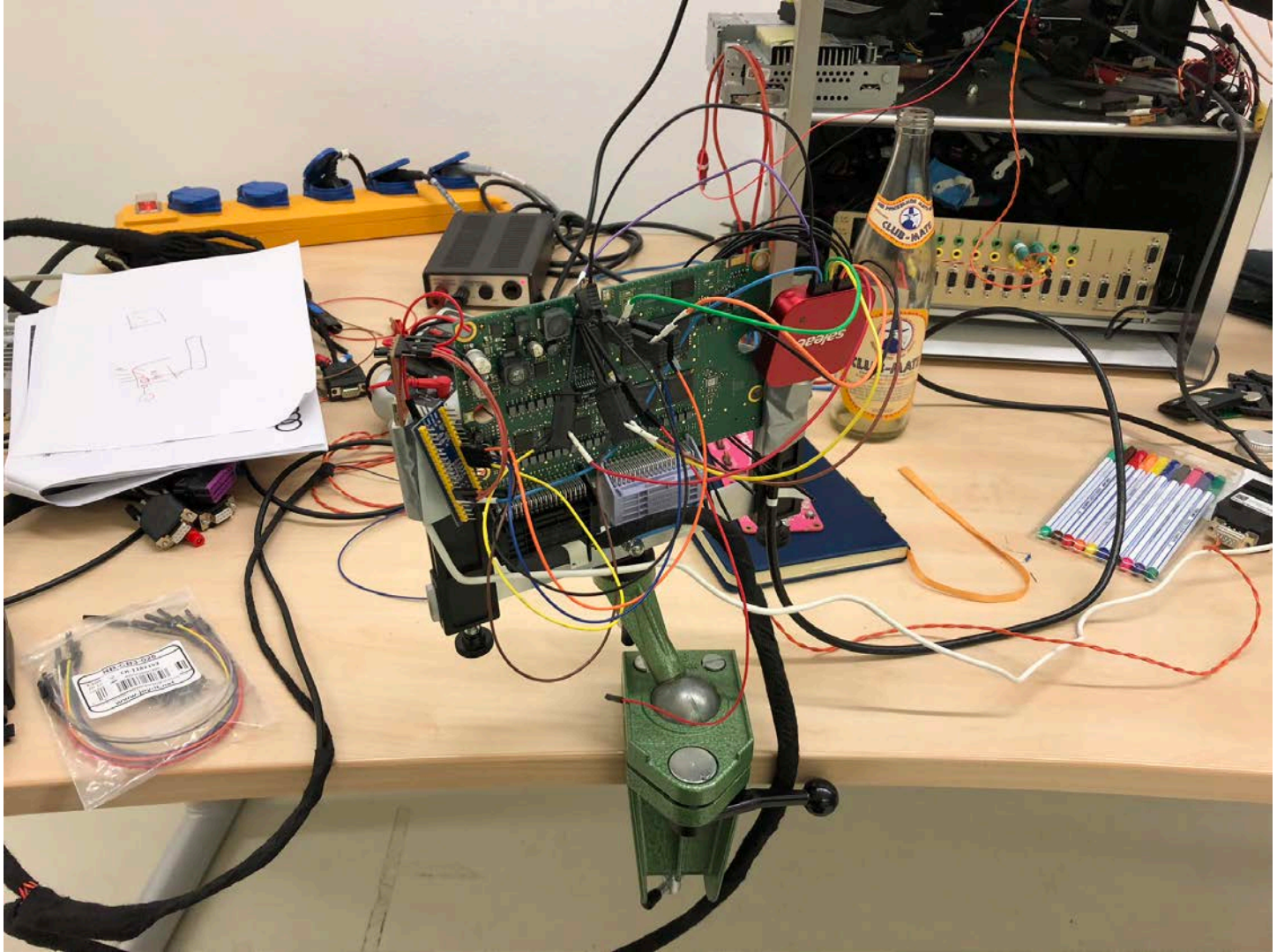
Main Bug Hunting Times

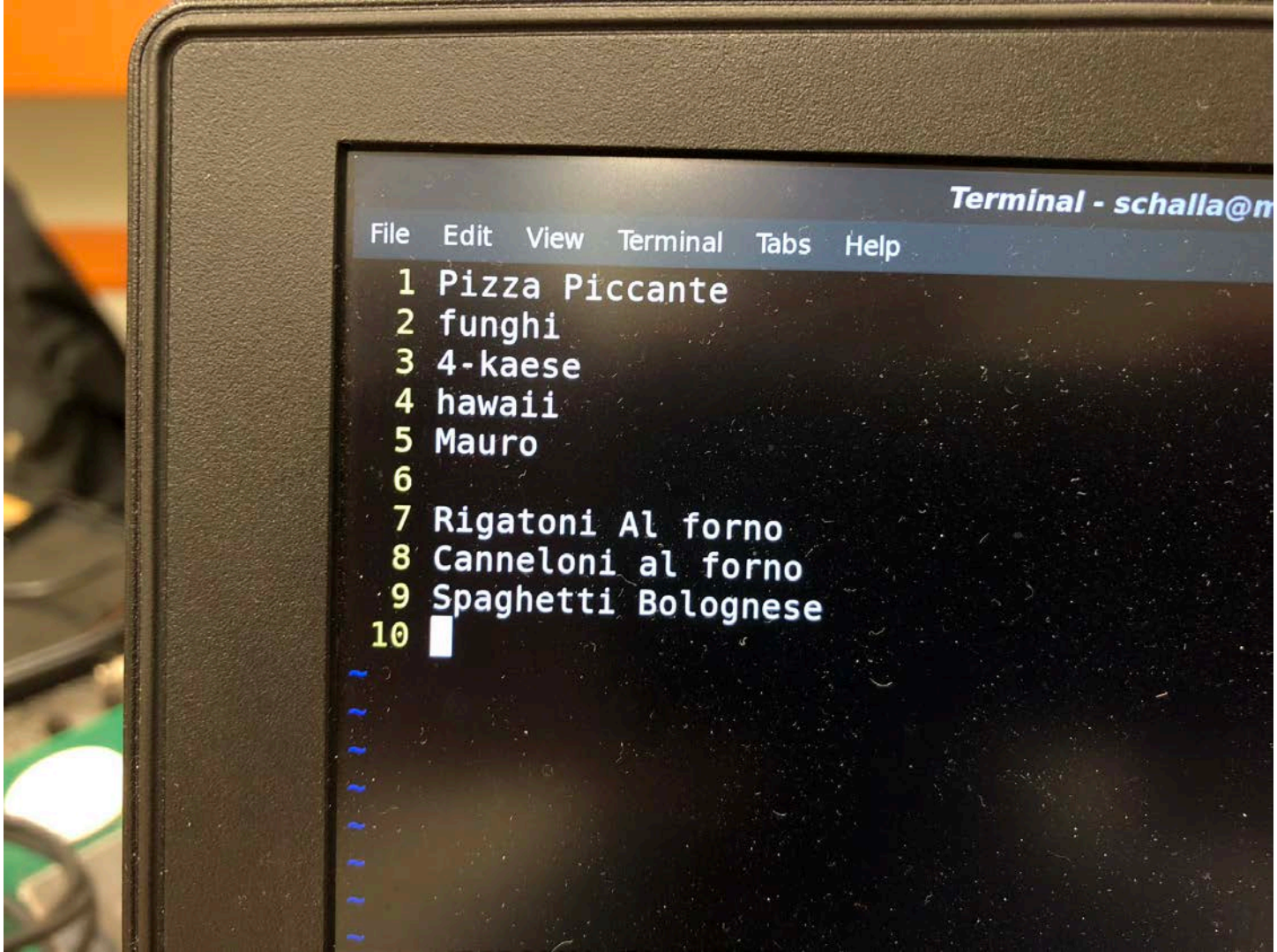
- Begin: ~ 11:30 AM – 1:00 PM
- End: ~ 12:00 AM - 2:00 AM

- Most findings were produced during the “night shift” ;-)

The Bug Hunters During the Intro Workshop


IN K 5819


CLUB-MATE


Terminal - schalla@m
File Edit View Terminal Tabs Help
1 Pizza Piccante
2 funghi
3 4-kaese
4 hawaii
5 Mauro
6
7 Rigatoni Al forno
8 Canneloni al forno
9 Spaghetti Bolognese
10

Workshops

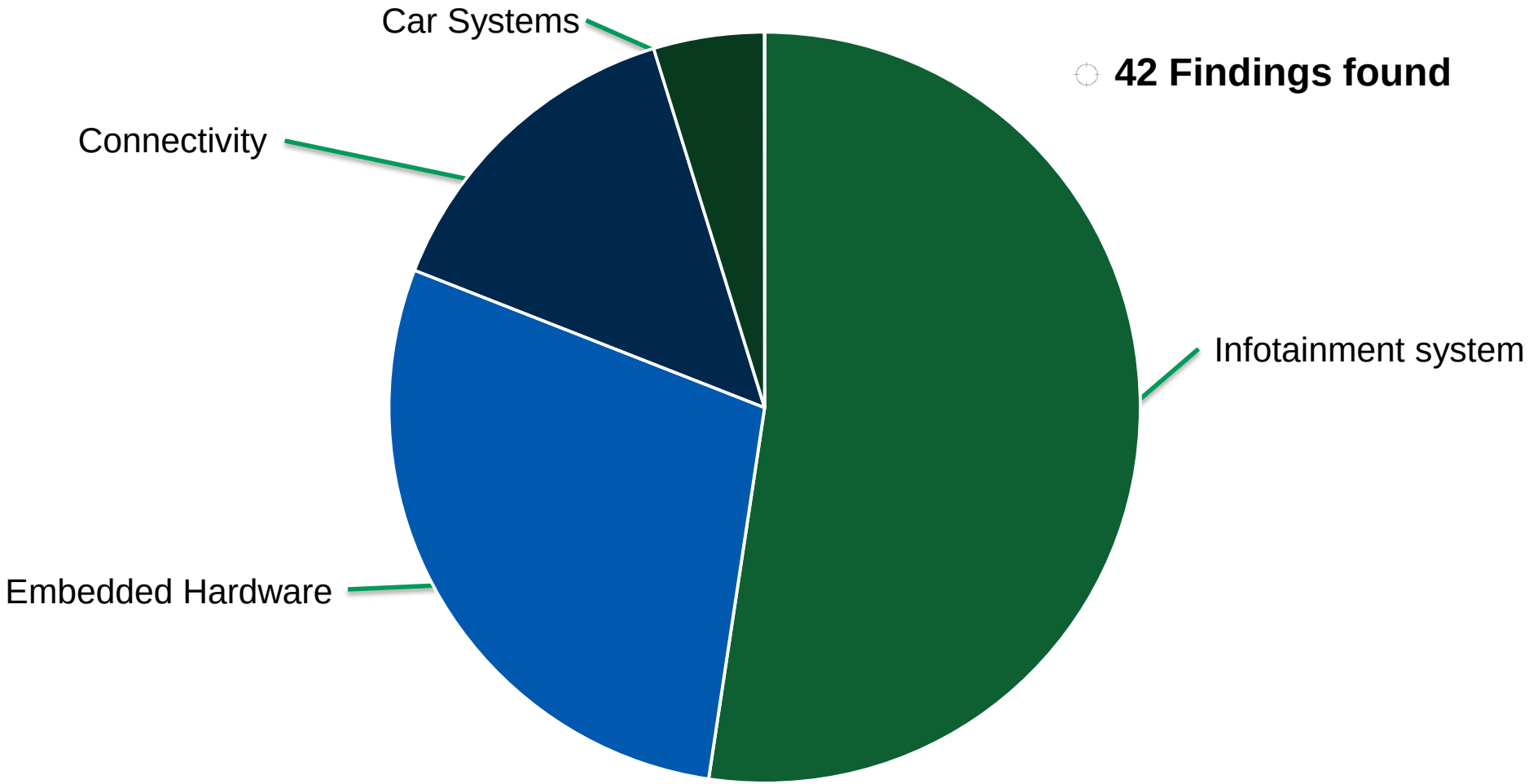
- Several times the Audi engineers presented their working field in order to give information on the targets of evaluation to the Bug Hunters
- In exchange the Bug Hunters explained how their testing approaches worked and which vulnerabilities they found – and how

Understanding the Automotive Domain


Fahrzeug: Audi drive select
lift / offroad
allroad
efficiency
comfort
auto
dynamic
individual
ENERGY DIGITAL

Conclusion & Takeaways

42


Car Systems
Connectivity
Embedded Hardware
Infotainment system
42 Findings found

Summary

- Security Testing itself is not sufficient for building secure cars
- The development of secure software and automotive systems must be understood as a process
- The phrase “testing is an integral part of development process” becomes even more important in the context of the development of secure automotive systems
- New testing approaches are needed

→To achieve this, close cooperation with security researchers is necessary

Thank You for Your Attention

Any Questions?

karsten.schmidt@audi.de
kschaller@ernw.de

@dg1vs
@p4nt3on

May I ask a Question?

I would like to discuss how we can improve such events?

- Does it make sense to start a public Bug Bounty?
  - My personal opinion → No.
- How to integrate such events into the development process?
- …