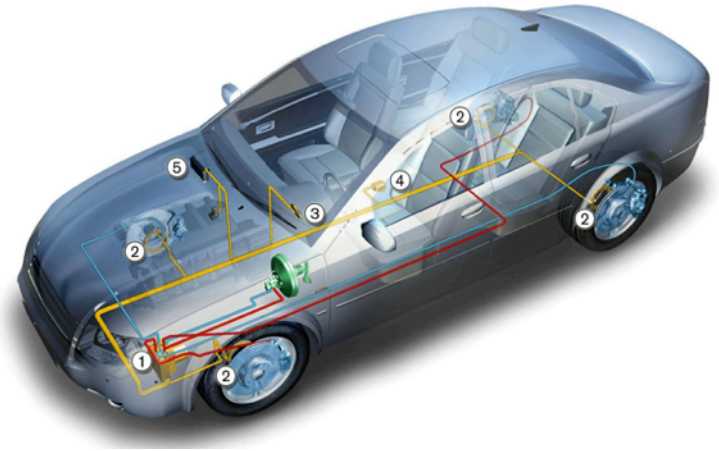
Car Security

A Pentester's Approach

Matthias Luft, mluft@ernw.de



ERNW

Providing Security.

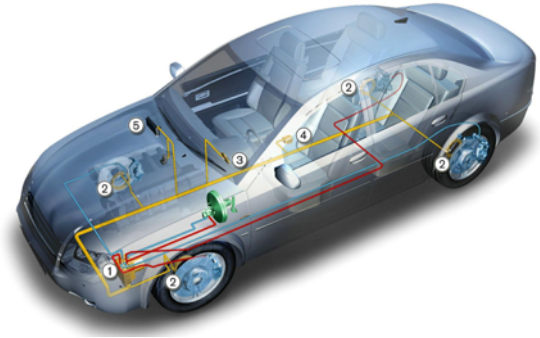
- Highly specialized security consulting & assessment services company, since 2001.
- Independent of vendors, financial obligations, share holders.
- Our customers are mainly very large, global enterprises.

- 50+ assessments/year

- #whoami
  - Team Lead Vulnerability Research and Information Security Management
  - Long-time-pentester-who-became-team-lead

Car/IoT Security

- Simply, in the future, there will be “network communications”, for many items.



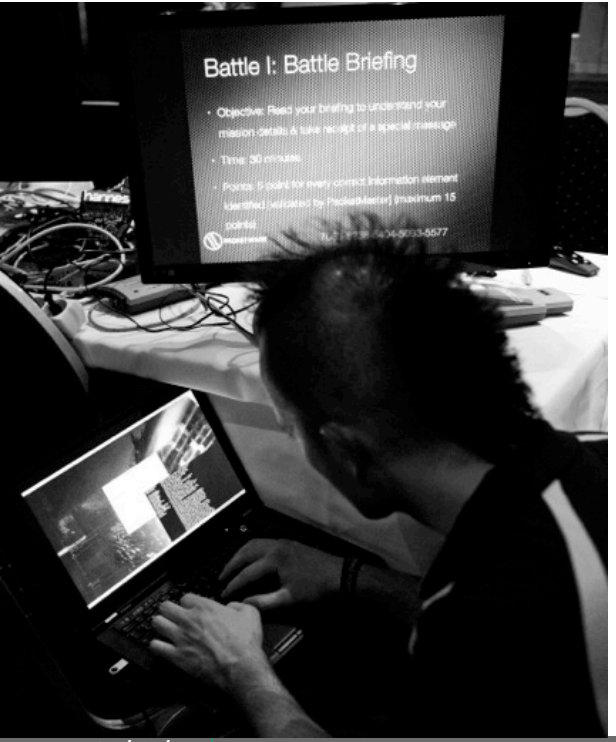
In the Old Days

ERNW
providing security.

The Future is Now

ERNW
providing security.

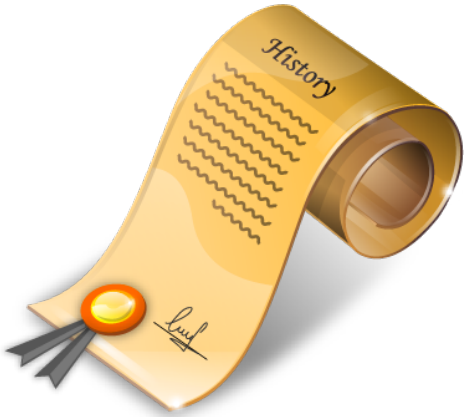
Pentesting & CarSec



- 90% of pentests cover traditional IT.
- How to approach car security?

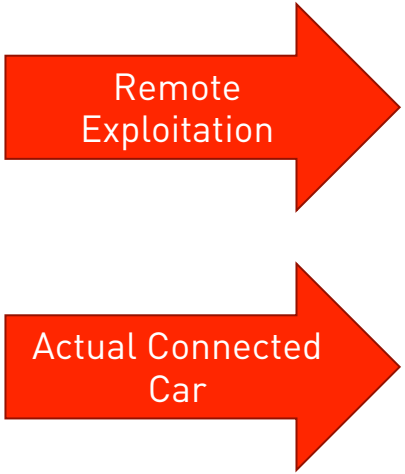
➔ What have we seen in the past?

CarSec History



- CAN Control
  - Various Researchers,
    e.g. Craig Smith or Charlie Miller
- Attacking the key fob
  - ETH Zurich
  - Cesare, BH 2014 [2000-2005]
- Externally accessible ODB ports
  - BMW, 2012

CarSec History



- Various Remote Compromises (e.g. FM, TPMS,
  - Autosec, UCSD/University of Washington
  - http://www.autosec.org/publications.html
- BMW Remote Unlock

Subject: system administrators guide to cracking
Date: 2 Dec 1993 03:36:16 GMT
From: zen@death.Sun.COM (d ... 415-336-0742)
Followup-To: comp.security.unix
Lines: 1106

Improving the Security of Your Site by Breaking Into it

Dan Farmer
Sun Microsystems
zen@sun.com

Wietse Venema
Eindhoven University of Technology
wietse@wzv.win.tue.nl

Introduction

Every day, all over the world, computer networks and hosts are being broken into. The level of sophistication of these attacks varies widely; while it is generally believed that most break-ins succeed due to weak passwords, there are still a large number of intrusions that use more advanced techniques to break in. Less is known about the latter types of break-ins, because by their very nature they are much harder to detect.

CERT. SRI. The Nic. NCSC. RSA. NASA. MIT. Uunet. Berkeley. Purdue. Sun. You name it, we've seen it broken into. Anything that is on the Internet (and many that isn't) seems to be fairly easy game. Are these targets unusual? What happened?

Pentesting

ERNW
providing security.

Pentest Steps

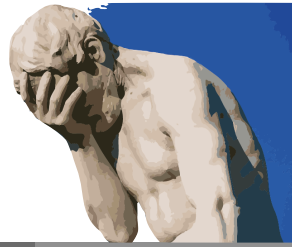
- Reconnaissance

- Enumeration

- Vulnerability Research

- Exploitation

- Documentation



One step back...

- Those were the phases of a properly defined pentest.
- What is necessary to properly define a pentest?

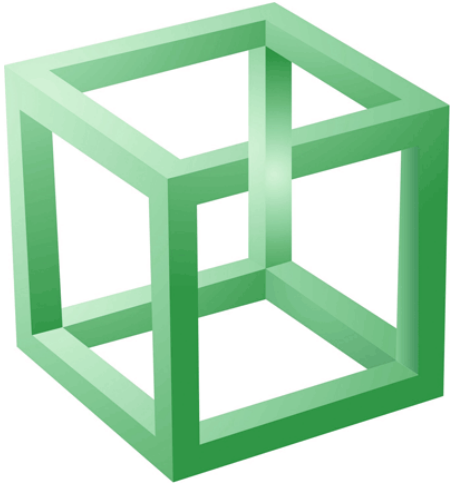
Security

"[...] security is the absence of unmitigatable surprise."

Dan Geer

Safety

ISO 26262 defines
Functional Safety as:

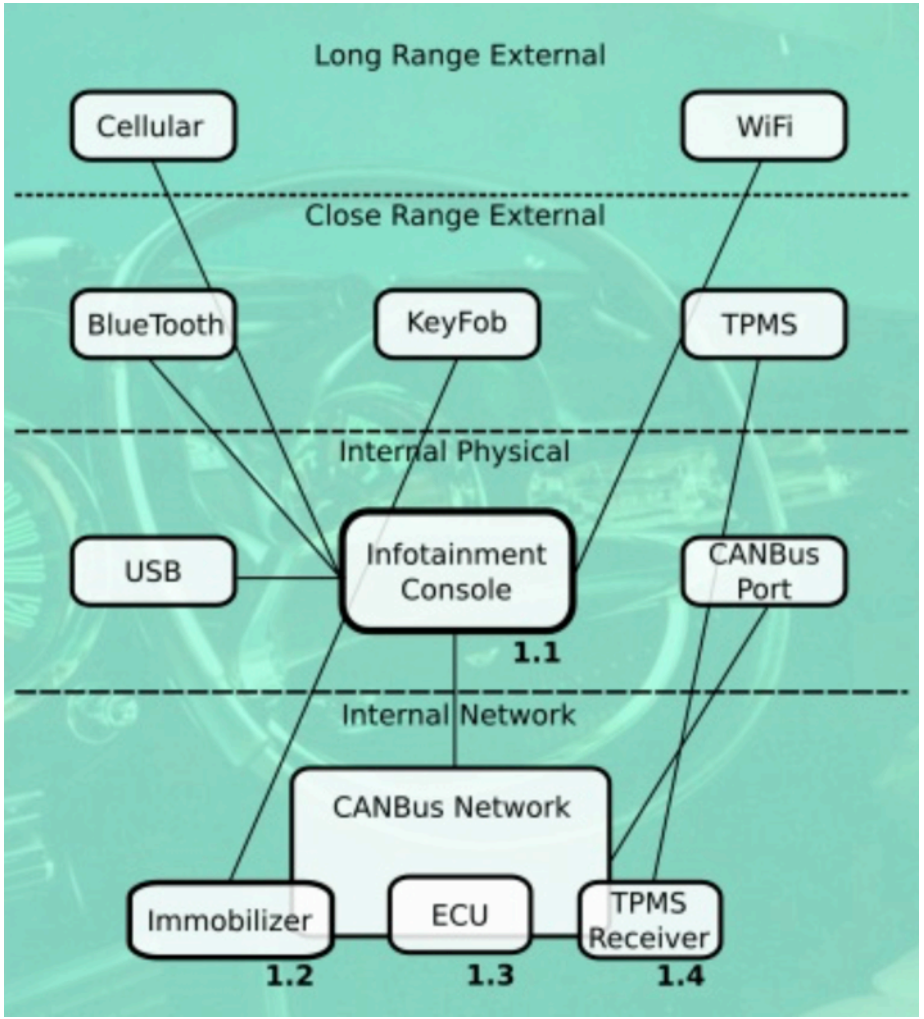


"[...] absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electrical and/or electronic systems [...]"

ISO 26262

So there might be common objectives of security and safety, at least for *systems*

- Given we're "security guys", I'll talk about security, in the following.
- Denial-of-Service scenarios might become way more relevant!



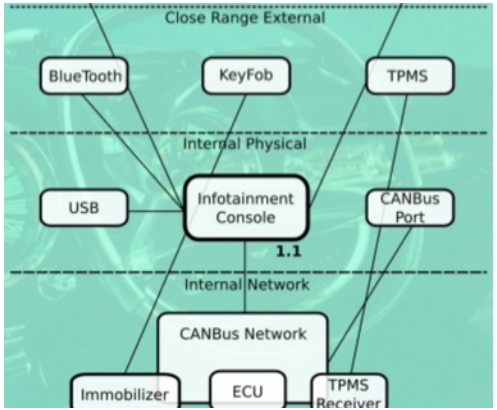
Checklist

Source: Car Hackers Handbook (2014)

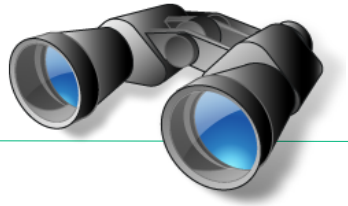
Different Views

- Threats:
  - Is it possible to remotely track the driver?

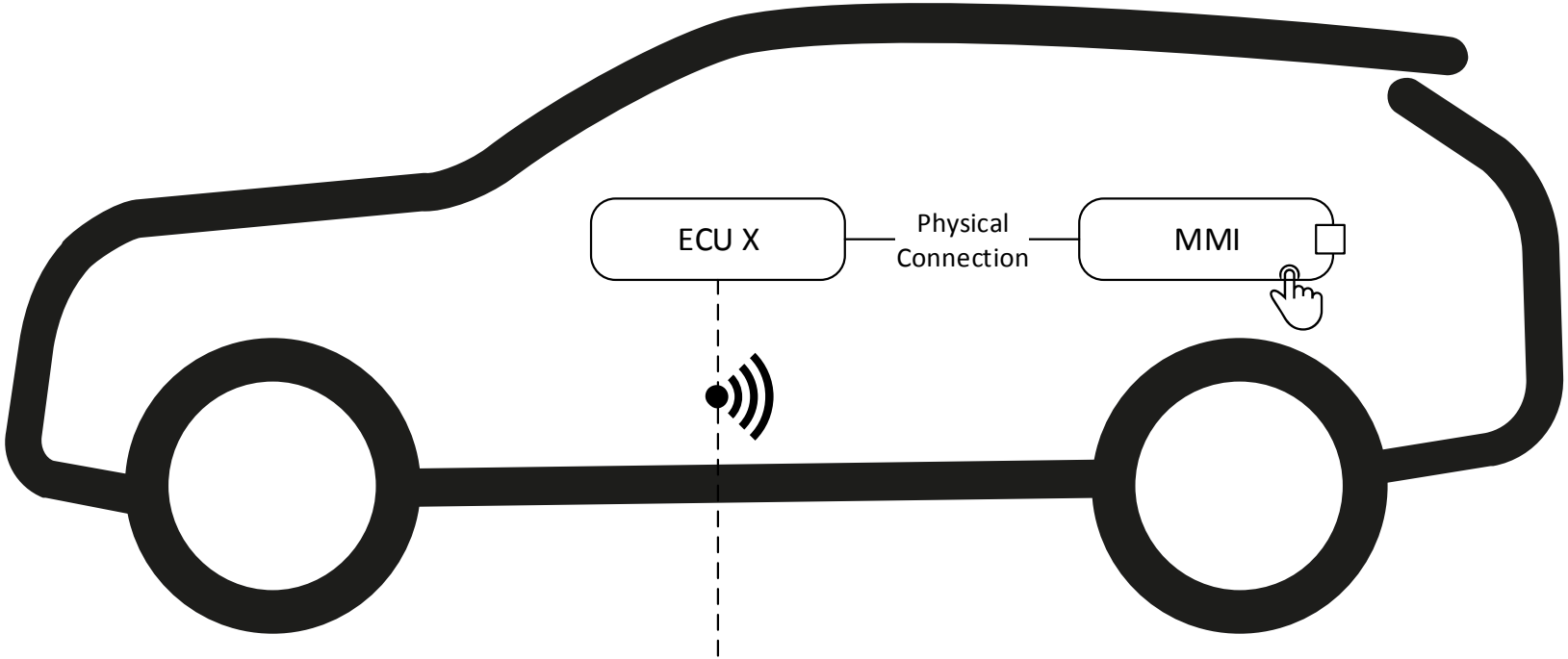
- Technical:
  - What interfaces can I interact with?

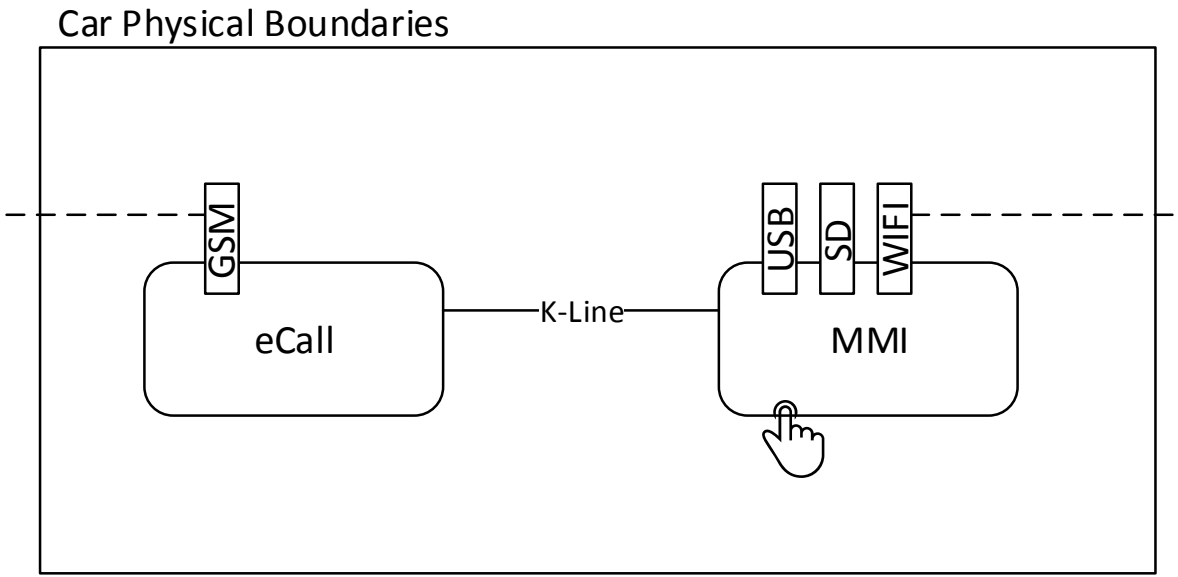


Reconnaissance



Overview





Overview

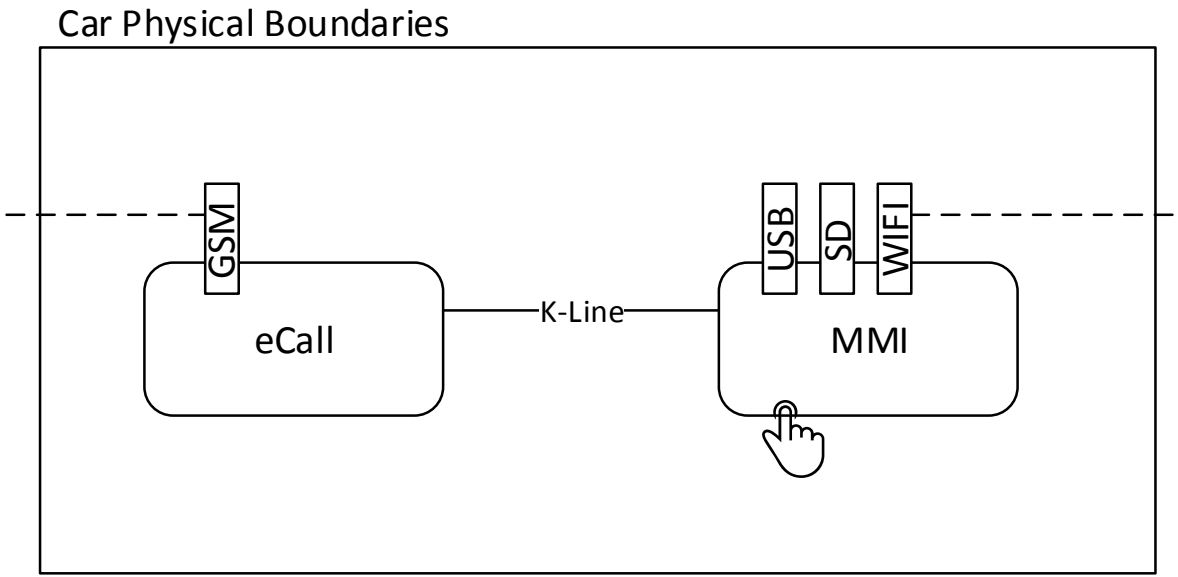
... in a more practical way.

Car vs. Regular IT?

First differences

- Different interfaces!
- Regular pentests rarely cover USB or SD access.

Enumeration



Overview

... in a more practical way.

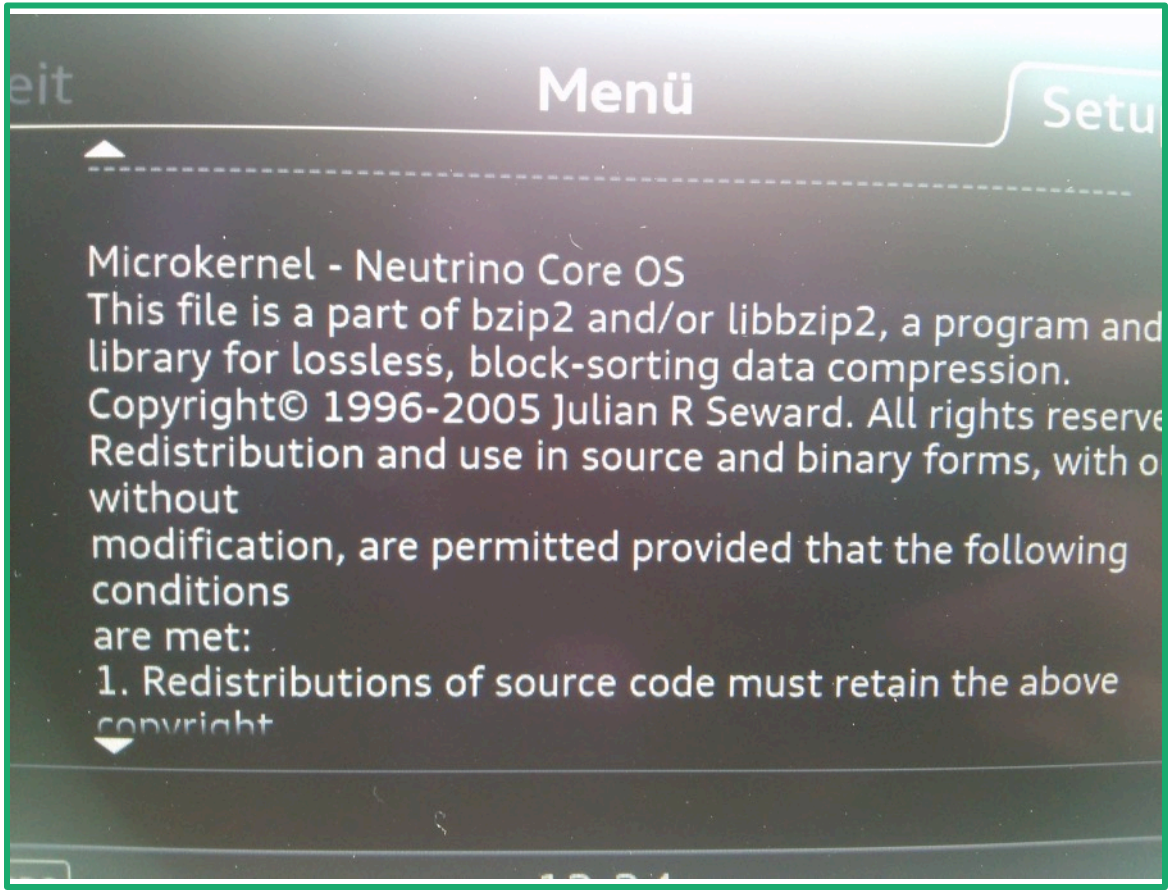
Enumeration

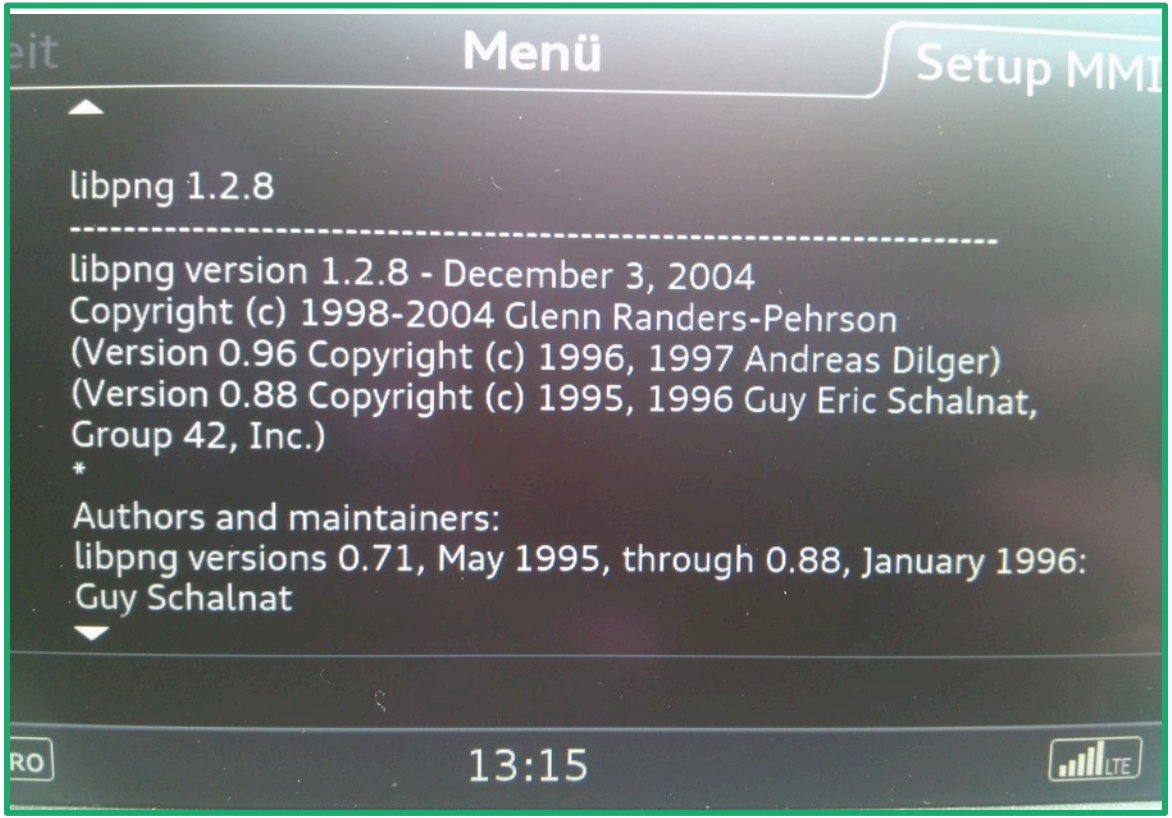
- Traditional pentest:
  - IP/TCP/App footprinting
- Car security:
  - Typically only limited IP access (e.g. for the wifi interfaces)
  - However, we typically have physical access!

Enumeration

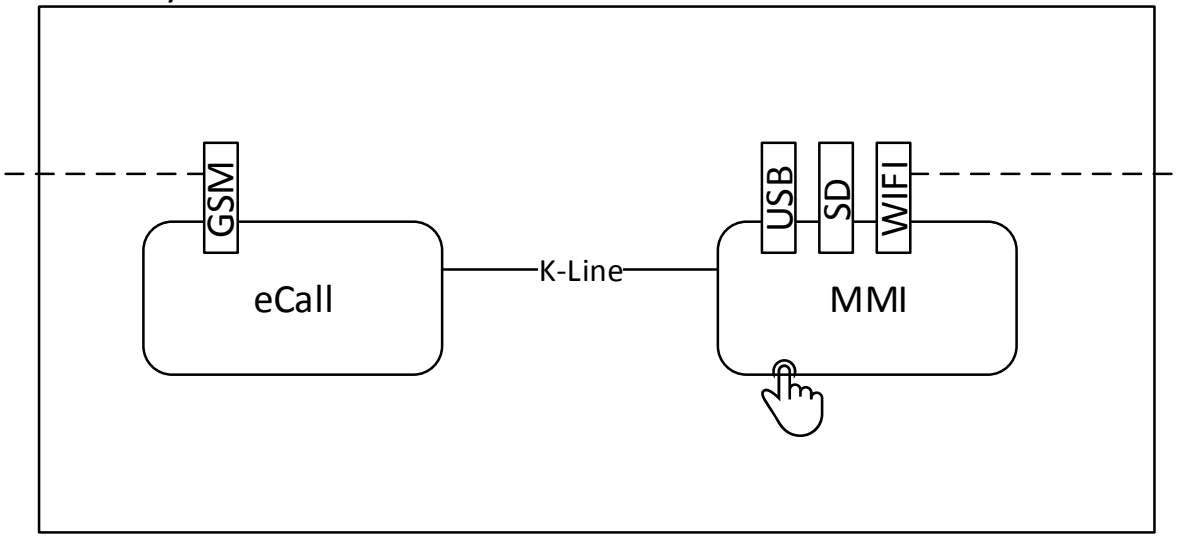
Physical Access

- Traditional embedded security
- Firmware extraction
  - Removing flash, soldering fuses, enumerating JTAG interfaces…
- Firmware analysis
  - MIPS/ARM knowledge becomes crucial.


eit
Menü
Setu
Microkernel - Neutrino Core OS
This file is a part of bzip2 and/or libbzip2, a program and
library for lossless, block-sorting data compression.
Copyright© 1996-2005 Julian R Seward. All rights reserve
Redistribution and use in source and binary forms, with o
without
modification, are permitted provided that the following
conditions
are met:
1. Redistributions of source code must retain the above


eit
Menü
Setup MMI
libpng 1.2.8
---
libpng version 1.2.8 - December 3, 2004
Copyright (c) 1998-2004 Glenn Randers-Pehrson
(Version 0.96 Copyright (c) 1996, 1997 Andreas Dilger)
(Version 0.88 Copyright (c) 1995, 1996 Guy Eric Schalnat,
Group 42, Inc.)
*
Authors and maintainers:
libpng versions 0.71, May 1995, through 0.88, January 1996:
Guy Schalnat
RO
13:15
LTE

Car Physical Boundaries



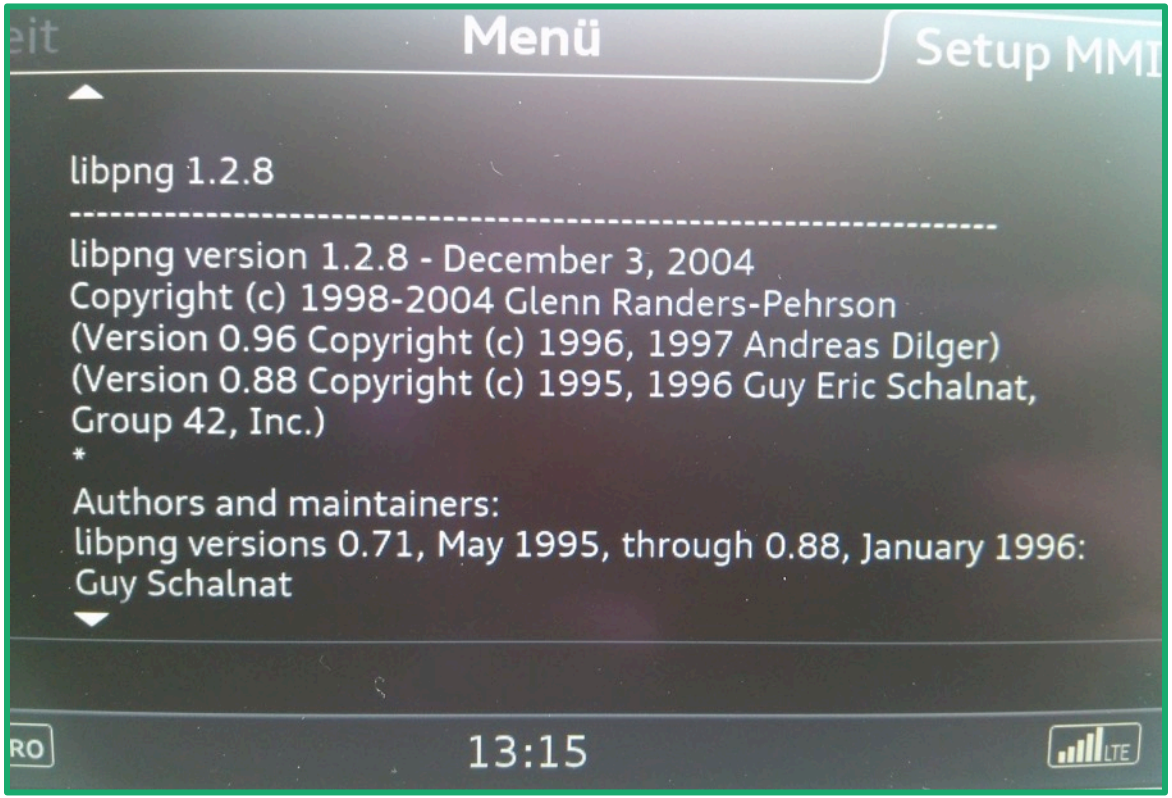
Component	Interface	Relevant Information
MMI		libraries: libpng, … Kernel: Neutrino
	USB	libusb-1.0.9
	Wifi	Offers AP, open ports: 53, 8080
eCall		Vendor: XYZ Version/Model: XYZ
	GSM	LTE support

Overview

Enumeration

ERNW
providing security.

Vulnerability Research


eit
Menü
Setup MMI
libpng 1.2.8
---
libpng version 1.2.8 - December 3, 2004
Copyright (c) 1998-2004 Glenn Randers-Pehrson
(Version 0.96 Copyright (c) 1996, 1997 Andreas Dilger)
(Version 0.88 Copyright (c) 1995, 1996 Guy Eric Schalnat,
Group 42, Inc.)
*
Authors and maintainers:
libpng versions 0.71, May 1995, through 0.88, January 1996:
Guy Schalnat
RO
13:15
LTE

ERNW
providing security.

http://www.libpng.org/pub/png/libpng.html

Vulnerability Warning

Versions up through 1.2.11 and 1.0.19 have a buffer-overrun vulnerability when a particular error message is triggered. The overrun is always by exactly two bytes ('k' and NULL) so it seems highly unlikely that it could be used for anything more nefarious than denial of service (e.g., crashing your browser when you visit a site displaying a specially crafted PNG). Nevertheless, it's worth fixing, and versions **libpng 1.2.12** and **libpng 1.0.20**, released 27 June 2006, do just that. (Note that 1.2.11 and 1.0.19 erroneously claimed to include the fix, but in fact it had been inadvertently omitted.) MITRE refers to this bug as CVE-2006-3334.

Fault Injection/Fuzzing

- Fault injection / Fuzzing
  - Given the number of network/ communication stacks/relationships, this should be a mandatory effort.

Somebody will do it someday.
Better be the first to try it.

Exploitation

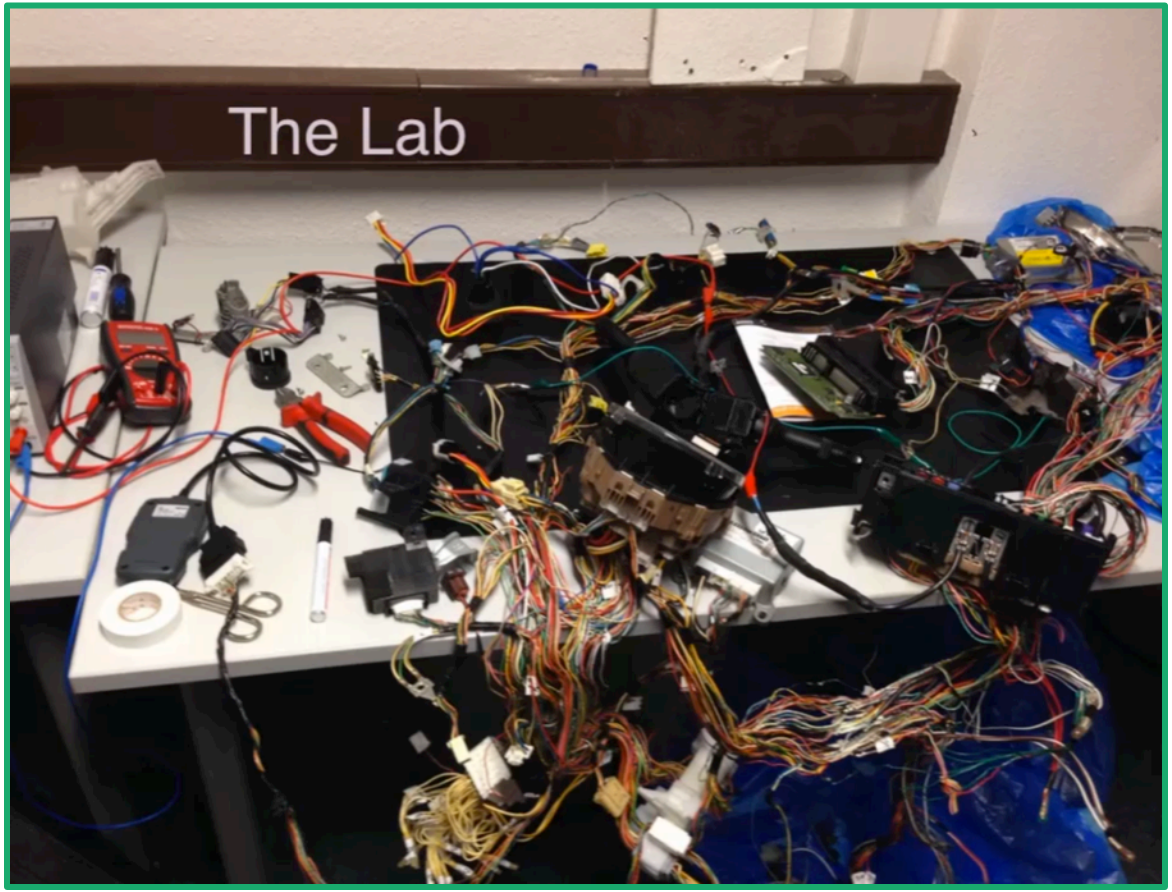
ERNW
providing security.

Exploitation

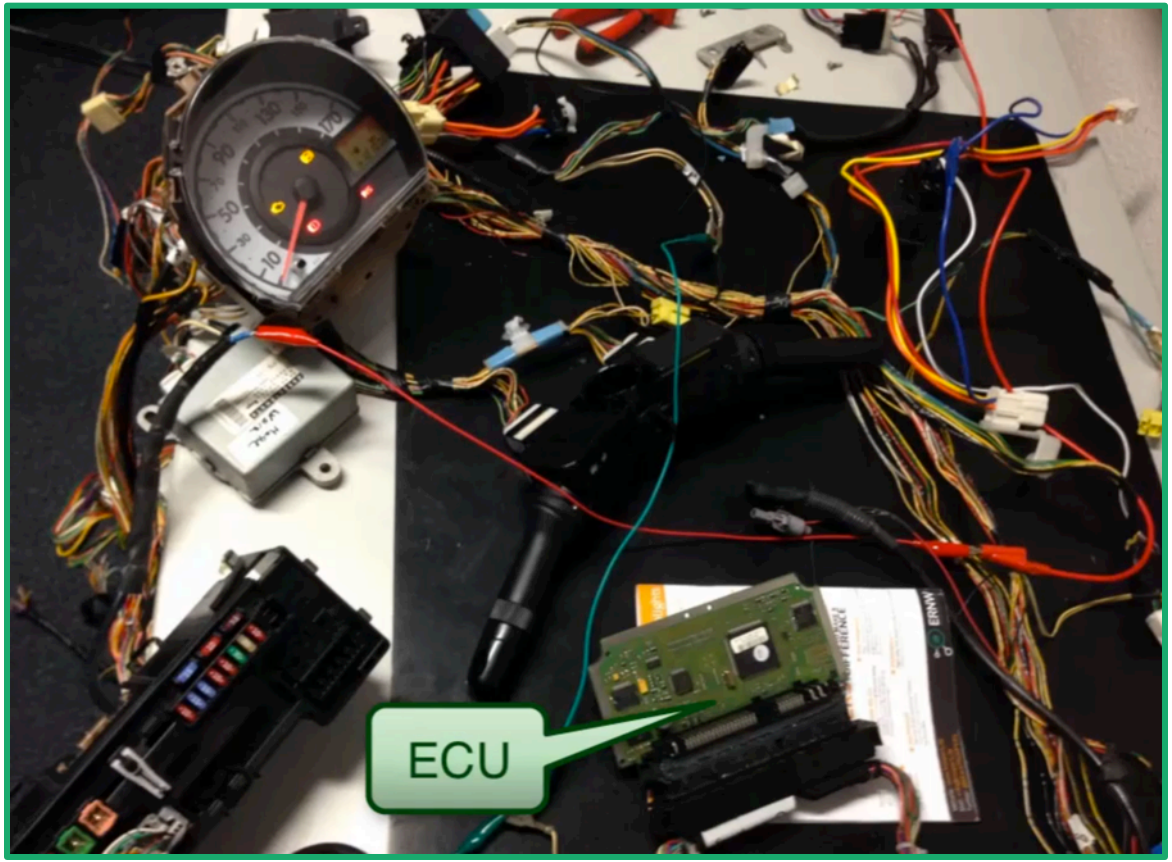
- Lab environment required!
- Traditional pentest:
  - Lots of virtual machines…
- Car Security?
  - …

Lab

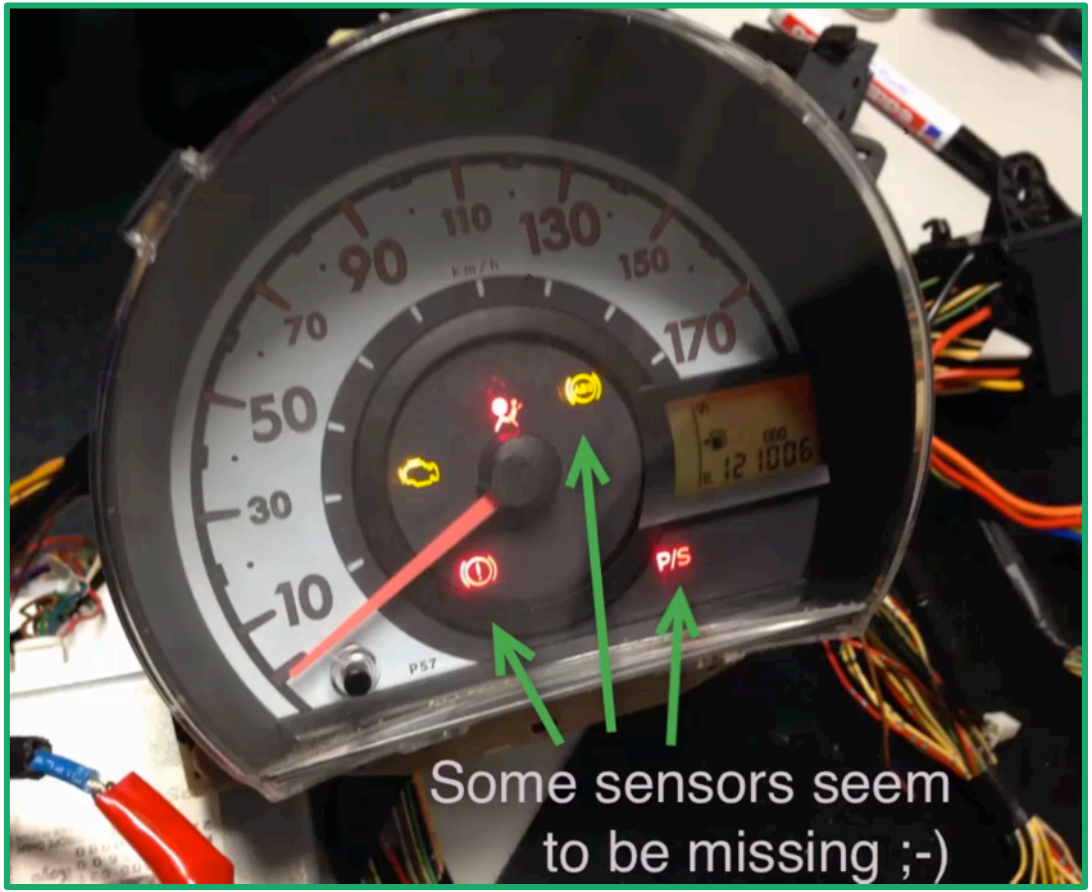
Lab



Lab



Lab



Lab

Lab

Finally

Cell Identification

- Choosing the wireless technology:
  - GSM
  - UMTS
  - LTE
  - (or others)

- Identification by cell scanning and frequency scanning:
  - Based on the used frequency the technology and provider can be identified.
  - Modems support cell scanning functions, showing available cells and provider.

Cell Sniffing

- Active sniffing
  - Open baseband implementations like OsmocomBB
  - For LTE: Samsung Kalmia USB Stick
- Passive sniffing
  - Sniffing via USRP, rtl-sdr or HackRF
  - Decoding with Gnuradio projects like gr-gsm
- Based on the gathered data further steps can be performed (e.g. A5/1 cracking).

pytacle

USRP

GSM1800

N: /root/record1_usrp

set: 725

e: /tmp/pytacle_record_dl_N

Record

: /root/record1_usrp

Crack

: /root/record1_usrp

1e f0 0b ab 3b ac 70 02

e: /tmp/pytacle_decode_HY

Decode

```
Found Immediate Assignment, ts 1
Decoding timeslot 1
Trying to find System Information Messages
Found System Information Type 5, fn 862245
Found Ciphering Mode Command, fn 862315
Trying to find suitable Ciphertext
Found suitable Ciphertext, fn 862347
Found suitable Ciphertext, fn 862449
Found suitable Ciphertext, fn 862551
Trying to find key via kraken
Testing SI, fn:862245 with cipher text fn:862347
Kraken: Cracking #31 0001110001110101000011100010100111010001101110
Kraken: crack #31 took 91602 msec
Kraken: Cracking #32 0100011001100100001000100111111010011011111100
Kraken: Found 934ef5e1e65087aa @ 4  #32  (table:412)
Found key ('934ef5e1e65087aa', '4')' for fn 862345
Trying to find KC... ...not found, sorry!
Kraken: Cracking #33 0100000111101111011001110101010110101101110010
Kraken: crack #33 took 174427 msec
Kraken: Cracking #34 0011100010110111101000111010100100011011000010
Kraken: crack #34 took 91729 msec
Testing SI, fn:862245 with cipher text fn:862449
Kraken: Cracking #35 0110101000111011111110100111100110100001100100
Kraken: crack #35 took 91783 msec
Kraken: Cracking #36 0111000011110111111111101111011010101010011011
Kraken: crack #36 took 91409 msec
Kraken: Cracking #37 0111101000111000111100000001011111000001001011
Kraken: crack #37 took 91395 msec
Kraken: Cracking #38 1011111111100100000010010011111001000011101000
Kraken: Found d5eb21665d2b8f25 @ 13  #38  (table:172)
Found key ('d5eb21665d2b8f25', '13')' for fn 862449
Trying to find KC... ...found! '1e f0 0b ab 3b ac 70 02'
```

Properties | Scan | Quit

ERNW providing security.

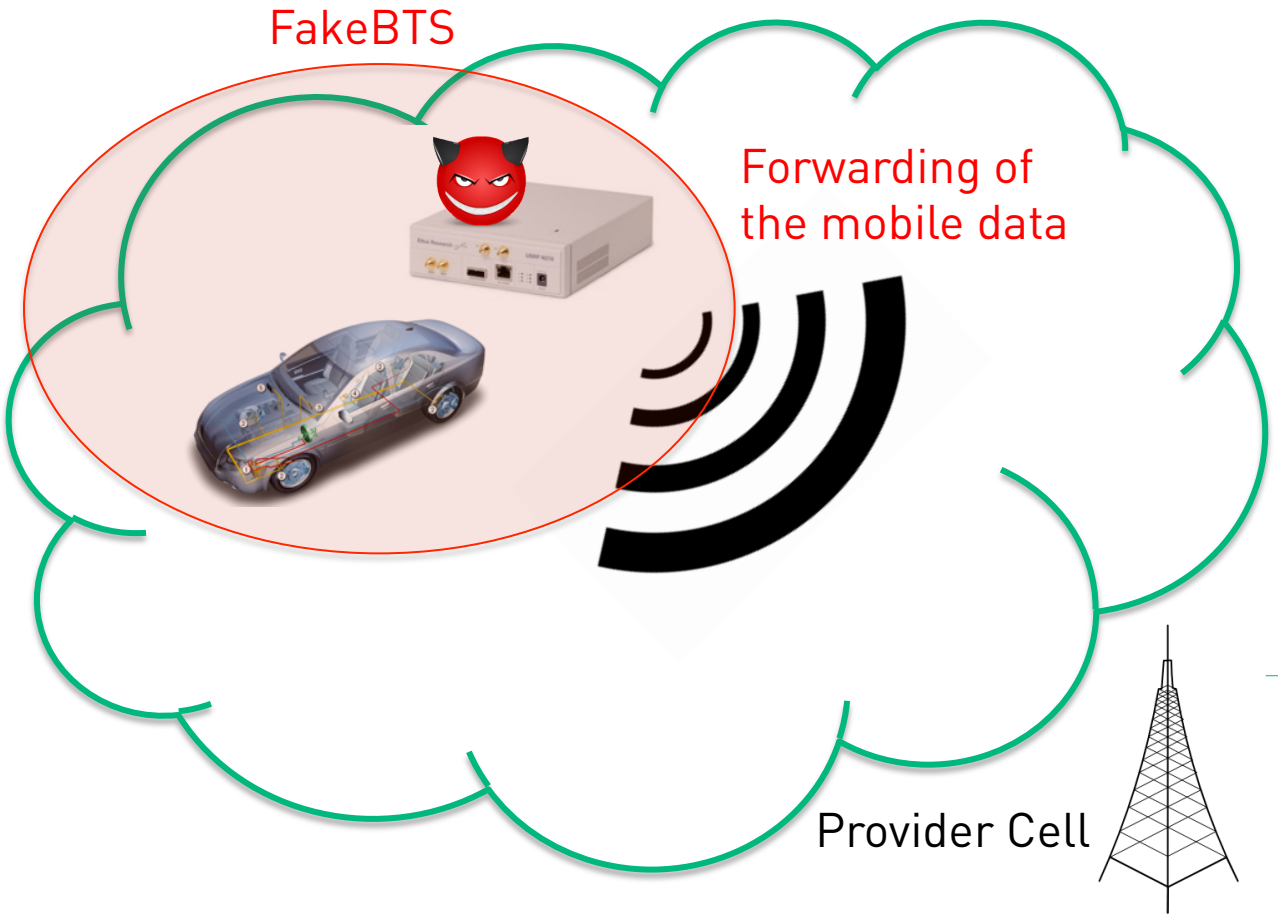
Cracking A5/1 w/ Pytacle

http://www.insinuator.net/2013/10/pytacle-alpha2/

The Cell in the Middle

- Fundamental tool is a FakeBTS
  - OsmoBTS with Ettus USRP
- Or even easier with a SysmoBTS
  - All-in-one implementation by Sysmocom, providing a GSM cell including voice, sms and data services.
- Things that can be configured
  - MNC, MCC, ShortName, LongName

→ And that's all we need; Encryption and authentication material will be forwarded (or disabled) by the FakeBTS.



A mobile will always choose the best cell available!

Actually, that's ours ;-)

Conclusions

- Reliability/safety/security of cars and connected services can be competitive advantage
  - And must be marketed as such.
- Typical pentesting approaches must be extended/complemented.
- HW assessment/various interfaces.
- Both the car and the backend services must be in scope.

There's never enough time...

Thank you...

@uchi_mata

mluft@ernw.de

...for yours!

Further information:
https://www.insinuator.net
(..soon)

Disclaimer

All products, company names, brand names, trademarks and logos are the property of their respective owners!

There are few things to know about TROOPERS:

ERNW
providing security.

DATE: March,14 -18. 2016
PLACE: Heidelberg, Germany
MISSION: Make the world a safer place.

REGISTRATION OPEN: www.troopers.de

ERNW providing security.

The Archive

Jeff Gough at TROOPERS13

- Feel the spirit – TROOPERS14 Trailer: https://www.youtube.com/watch?v=A9zWD7ZVAGI
- TROOPERS15 Talks:
  - Videos: https://www.youtube.com/playlist?list=PL1eoQr97VfJkfckz9nZFR7tZoBkjij23f
  - Slides: https://www.troopers.de/archives/
- We hope to see you in 2016!