09. – 12.12.2019
Frankfurt am Main

```
MDkuIOKAkyAxMi4xM
i4yMDE5CkZyYW5rZn
VydCBhbSBNYWlu
```

#ittage

Christopher Scheuring
Brian Butterly

Von echten Hackern & Security-Researchern

Hackers and Security Researchers

IT-Tage 2019

Christopher Scheuring -- Brian Butterly

About Us

Christopher

- Security Researcher & Analyst
  - Officially Incident Response
  - More on the offensive side…
- Mainly focused on IoT / OT&ICS / HW / Multi-Tier-Environments
  - Also having a look at automotive and other embedded systems

@0x4045494650
chris@aucmail.de

Brian

- Security Researcher
  - Officially Incident Response
  - Probably break more stuff on the side…
- Mainly focused on Embedded / HW / Cellular
  - Which also includes stuff like mobiles and automotive

@BadgeWizard
brian@security-bits.de

“Nobody would ever do that!”

- #1 excuse for not applying proper hardening or applying other security measures
- Attacks / insights / research are always rated as being really hard or too expensive
- We’re here today to change your mind

The good, the bad and the nosey

- Why do people do research?
  - It’s fun
  - It’s interesting
  - It’s new
- Why do people do security research?
  - Idealists
  - Doing the right thing
  - Protecting others
  - Bad experience
  - And some for fame and fortune

Bad Experience

- Past and present have shown that there was and still is a lack of security in many products
- Modern IoT is re-implementing old IT vulnerabilities
- Security costs money & is in the way of quick product releases
- Entanglement of safety and security is often not understood

- A shop sells a product
- The customer trusts the shop
- Product has to be secure, because otherwise the shop wouldn’t have sold it
- Shop doesn’t understand security
- Manufacturer doesn’t focus on security

- The customer is lost . . .

Equipment & Stuff

Equipment

- Both the Open Source and the Maker community have made tools really cheap
  - And available
- Components and solutions, which might have costs thousands of Euros a few years back, now only cost a few hundred Euro
- They also provide vast amount of documentation, instructions and ideas

Community

- Hackers and researchers are not individuals
  - They’re part of an open community, which helps each other and shares
- Well, those are the people going to Hacker Conferences

- Next to talking and sharing knowledge, they regularly also share parts, tools and components

Work vs. Freetime

- Many people in security turned a hobby into a job
- Thus work and freetime often fuse together
  - Or they do extra jobs on the side
- Many researchers have a lot of private equipment, that they use for their hobby

Private Labs

- Electronics
  - Oscilloscope
  - Power supplies
  - Isolation Transformer
  - Function generator
  - Logic analyzer
  - Programmers
  - Various dev boards with different controllers etc.
  - Soldering iron, heat gun
- RF
  - SDR receivers & transmitters
  - Specific dongles (subGHz, attack specific)
  - NFC reader, writer, emulator
- Cellular
  - Basestations
- Making
  - 3D printer
  - Laser cutter engraver
  - PCB etching equipment
- Classic IT
  - Servers. switches, cables, WiFi
- Victims & PoCs
  - Stuff that looks interesting
  - Equipment others used
  - Etc. etc. etc. etc. etc.
- Documentation
  - Camera
  - Microscope

EDC

- Screwdrivers, knife, Leatherman
- 3..4 USB NICs
- Long range WiFi NIC
- WiFi AP
- HackRF/USRP
- YardStick One
- Ubertooth
- Bluetooth Dongles
- CrazyRadio
- RavenStick
- Some bus adapters for
  - CAN
  - RS485, RS23 etc.
- LoraWAN PI-HAT with GPS
- Buspirate
- JTAGulator
- Logic Analyzer
  - Various Wires
- Small soldering iron
  - + consumable
- NFC Reader/Writer
- Magstripe Reader
- USB Serial Adapter
- Several Level-Converters
- Dev board (ESP, Arduino etc.)
- Lockpicks

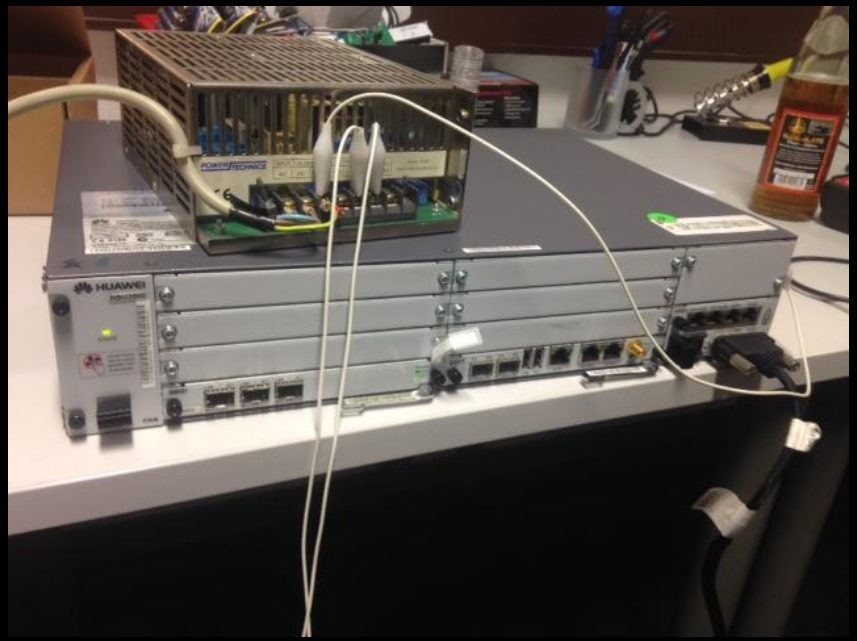
Fun Projects

eBay :)

- The approach of buying random stuff on eBay has been around for a long time
  - Harddisks, memory cards, networking equipment
- People often forget to delete old data before selling things
  - Companies make exactly the same mistakes
- Sometimes the devices simply don’t correctly delete the data and it can still be extracted
- The missing reset/factory default function…

- Budget: Whatever
  - Buying whatever one finds interesting
- Benefits:
  - Credentials
  - Insight into typical configurations
  - Equipment

Cellular Network Components



- Budget: 100€++
  - Random components from actual cellular networks
- Benefits:
  - Credentials
  - Certificates / Private Keys
  - Backend access
  - Insight into security configuration
  - An own network, if you got all necessary components

Running Your Own Cellular Network

- Cellular interfaces still run on a fair amount of black magic
  - Few manufacturers look closely at them
- Osomocom project offers us a whole software stack for running our own 2G / GSM network
  - Alternatively a 3G network

Budget: ~250€-1500€

- nanoBTS: eBay, 100-200€
- BladeRF: ~400€
- USRP: ~1200€
- Duplexer: 130€
- Cables: 20€

Benefits:

- SMS Fuzzing
- Direct access to IP communication
- Rerouting phone calls

Vehicle Immobilizer

- Connected to internet via GSM / GPRS
- Raw TCP data stream to centralized service
  - Server in some cloud in asia
  - Webinterface can be used to disable car or track location
- No encryption between immobilizer and backend
  - Attacker with MitM position (own cellular network) has full control over all of the devices functionality

Victim: 30-50€ vehicle immobilizer from Amazon (one of many very similar ones)

Intended to be placed in a car, with a relay on the power supply of the fuel pump

Also has a GPS tracker and microphone

Fun With RF

- SDR - Software Defined Radio
  - Programmable RF receivers / transmitters
  - Controllable via i.e. GRC or GQRX
- Dedicated dongles
  - Attacks against wireless mice & keyboards & presenters (2.4GHz)
  - LoRA
  - ZigBee

Budget: 20€-2000€++

- RTL-SDR-Dongle (SDR Receiver): 20€
- HackRF (SDR Transceiver): ~300€
- USRP (SDR Transceiver): ~1200€
- Specific dongles: 10€-200€
- YARDSSTICK ONE

Benefits:

- Sniffing
- Spoofing
- Injecting
- Often full control of victim

“Hacking” Around DVB Streams

Using Gnu Radio (SDR) and HackRF for DVB broadcasts:

- Broadcast webcam stream via DVB-T
- Broadcast existing TS
- Capture and replay TS
- MitM of live TS
- Capture and decode MHEG/MHP
- Mux own MHEG/MHP data stream with Audio/Video stream

Budget: 20€-2000€++

- RTL-SDR-Dongle (SDR Receiver): 20€ (only for receiving DVB-T)
- HackRF (SDR Transceiver): ~300€

Benefits:

- Sniffing
- Spoofing
- Injecting
- Or just doing your own local DVB-T webcam broadcast e.g ;-)

Alarm System

- Alarm sensors only send a signal when they’re triggered
- No replay protection
  - Alarm trigger can be recorded and replayed
- No keep-alive signal
  - Trigger can easily be jammed

Victim: ~80€ home alarm system

- With movement sensors, PIN pad and window switches
- Sensors connected with proprietary protocol and 868MHz

Benefit:

- Full disable of alarm system

Tracking Planes

- Modern planes are equipped with an Automatic Dependent Surveillance - Broadcast transmitter
  - Which broadcasts call sign, position, direction and speed
- Transmissions are neither signed nor encrypted
  - Anybody can receive or spoof them

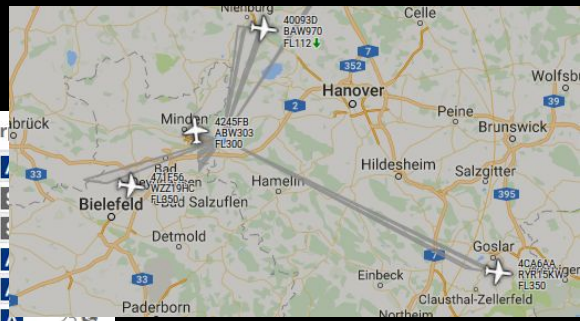
Budget: 30€

- RTL-SDR-Dongle: 25€
- Custom Antenna: 10€

Benefits:

- Tracking planes
- Fun PoC

ICAO	Callsign	Reg	Silhouette	Type	Sqwk	Track	Alt, ft	Speed, kt	V/S, fpm	Lat	Lon	Status	Azm	Dist, nmi	Msgs	Duration	Tr
3C6608						7.1°	36000	411	0	51.8237°	9.3203°		164.1°	30.0	87	00:29	A
4245FA	ABW303				0136		29975								20	00:43	
471F57	WZZ19HC				3454		35000								75	01:14	
4407CC	TAY186M				3525	157.4°	9675	328	-1664	52.7088°	9.8827°		49.7°	37.5	336	02:09	A
40093D	BAW970				2041	97.7°	9550	293	-1536	52.5900°	9.3945°		33.3°	20.5	190	02:15	A
471F56	WZZ19HC				3454	98.1°	34975	520	0	52.1024°	8.8765°		213.4°	14.6	1224	02:16	A
4245FB	ABW303				0132	353.6°	29975	440	0	52.4195°	8.9275°		317.9°	9.2	1512	02:17	A



Receiving Satellite Weather Images

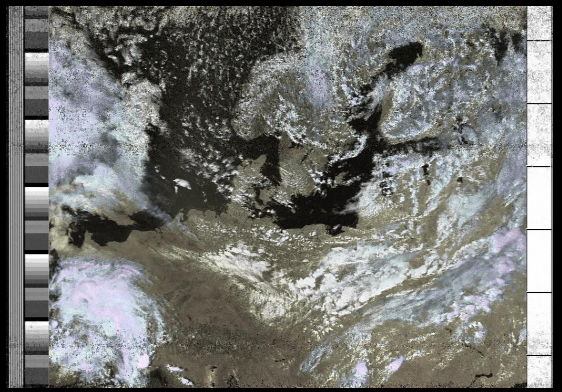
- National Oceanic and Atmospheric Administration Weather satellites
- Circle around earth, constantly transmitting images
- Transmission can be recorded using GQRX
  - Open Source SDR Software
- Decoding possible using WXtoIMG

Budget: 35€

- RTL-SDR-Dongle: 25€
- Custom Antenna: 10€

Benefits:

- A beautiful PoC



GPS Spoofing

- Open Source tool: gps-sdr-sim
- Uses SDR to spoof valid GPS signals
  - GPS is very weak, thus it’s easy to be stronger than the actual satellites
- Enables us to emulate static location or actual movement along a defined path at a given speed

Budget: >300€

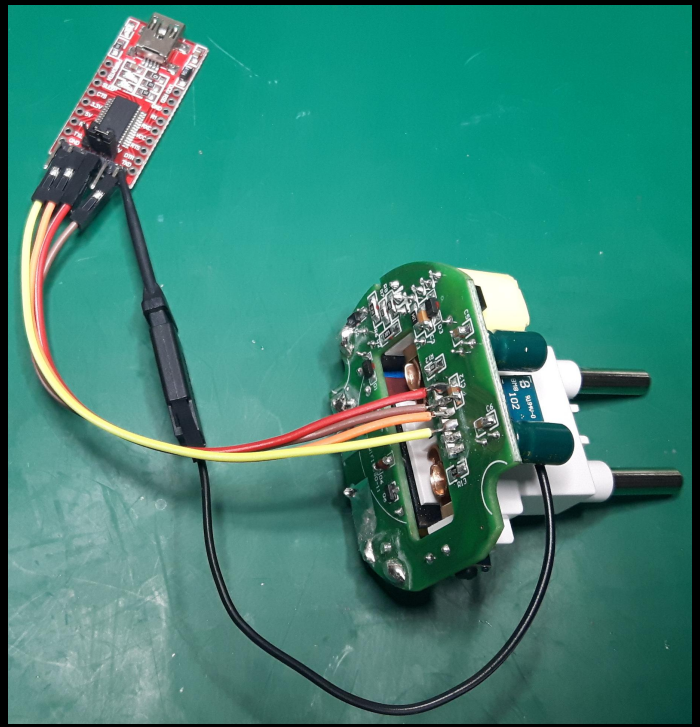
- HackRF One: ~300€
- BladeRF: ~500€
- USRP: ~1200€

Benefits:

- Circumventing GeoFencing
- HAVOC

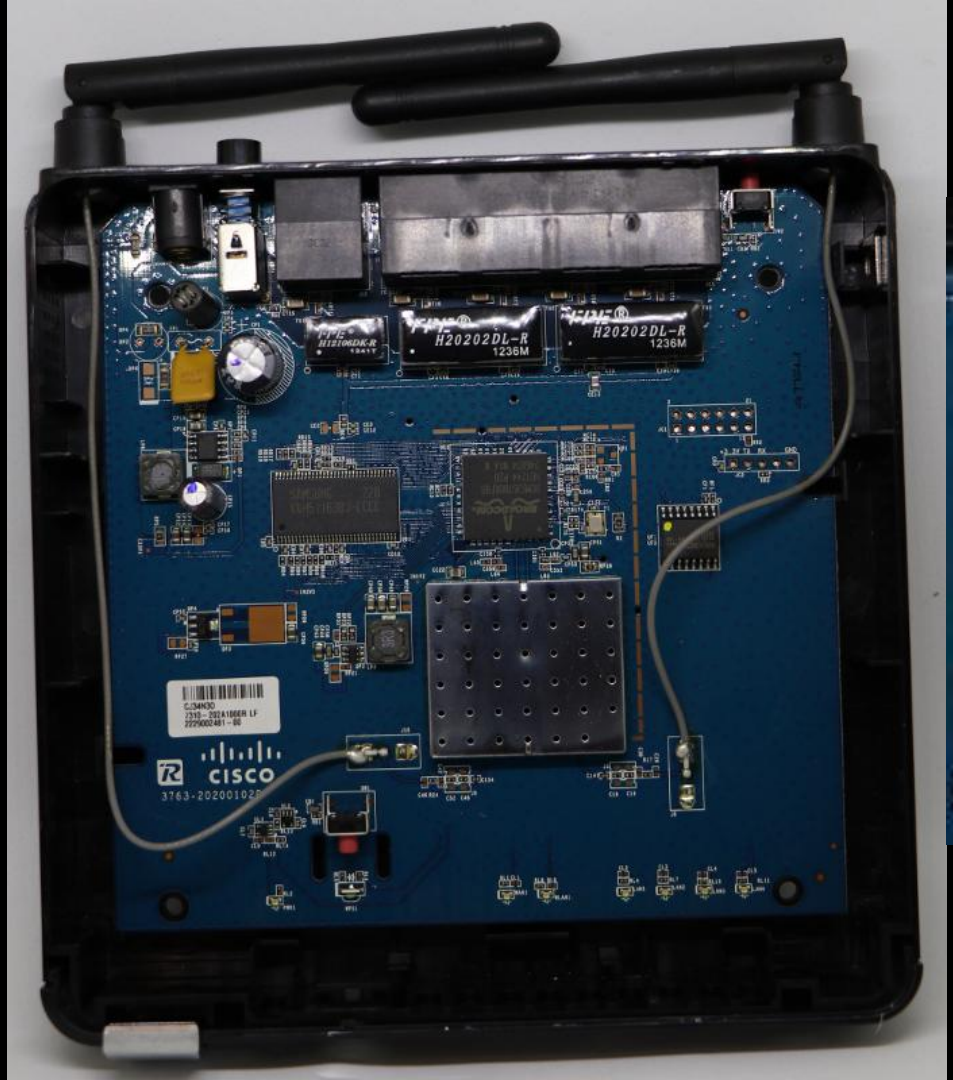
Embedded Security

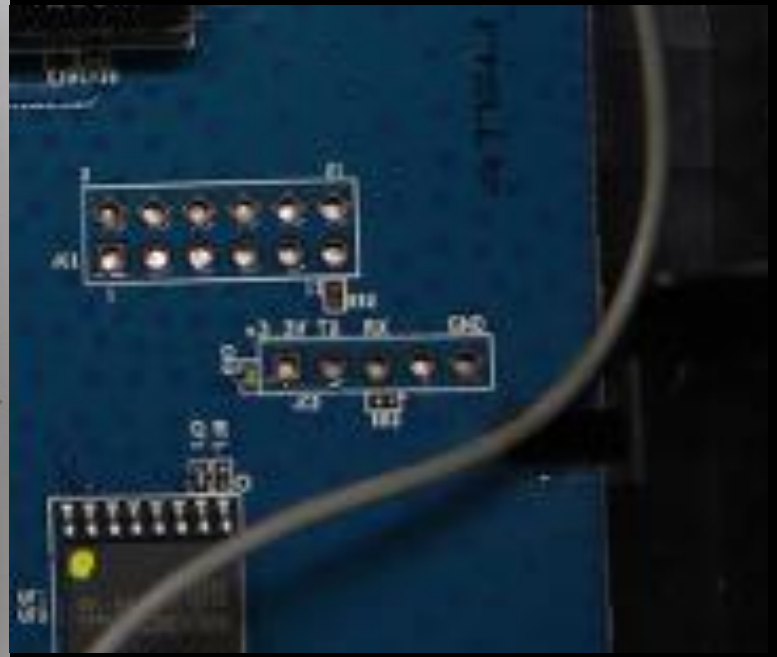
- Typical IoT / Smart Device:
  WiFi switchable Plug
- Most powered with cheap microcontroller or SOCs
  - E.g. TYWE26/ESP8266
  - Detailed documentation available
  - In most cases only UART to TTL converter needed
- Only challenge:
  NO galvanically isolation to AC 230V!
  - Sometimes soldering necessary if power/uart header missing



Cisco RV110W and RV215W

- SOHO routers by Cisco
  - Configuration limited to webinterface
  - Need to configure something that was not possible…
- Open the device
  - Identify UART
- Shell :)
- Sadly, although the device had gone through a factory reset, the backup of the configuration file was still there…
  - With the previous owner’s WiFi creds
- Budget: 10€
  - USB - TTL Cable: 10€
- Benefits:
  - Root on many many many devices
  - If not root, at least a way to get root
  - Possibly credentials of the previous owner


H20202DL-R
1236M
H20202DL-R
1236M
cisco



Dbox2 Debugging Mode

- Currently obsolete, but one of the old public Hard- and Software Hacks
  - Needs some soldering/steady hand and electronic skills
- Typical glitching attack
- Race-Condition at startup used to reset flash and break the bootloader startup
  - Reset flash (RP to GND) at startup
  - Disable write protect of flash (WP to HIGH)
  - Have fun flashing alternative bootloader and firmware

Extracting Secrets

Most common problem on IoT / Smart Devices:

- Stored Secrets on Device for WiFi, Cloud, File etc. Access
  - Mostly stored in cleartext
  - Sometimes obfusticated or stored encrypted with “known key”
  - Mostly unlikely but best solution: using of HSM/TPM
- Hacking tools more like:
  - strings and grep...

The very simple way:

```
$ strings smartplug_test_org.bin | grep -i mySSID
```

```
ESP.ty_ws_mod.wf_nw_rec_key={"ssid":"mySSID","passwd":"X9xxxxxxxxxxxxxxxxxxxxxxxxBb","wk_mode":0,"mode":0,"type":2,"source":3,"path":1,"time":5,"random":0}
```

NFC / RFID Attacks

- NFC cards can be very secure or very insecure
  - Depending on their age and use
- Many environments just use the UID of a dongle/card/tag
  - Which is burned into the tags memory
  - And can be read by anybody
  - And spoofed by anybody who tries
- Other environments still use (old implementations of) MiFare Classic cards
  - Which were declared insecure quite a few years ago

Budget: 30€-300€

- Proxmark (reader, writer, emulator): 300€
- Proxmark mini (china clone): 100€
- SCL3711 (reader, writer): 35€
- Chameleon mini (reader, writer, emulator): 60€

Benefits:

- Cloned access cards
- Emulated cards

Typical Access Cards

- Using older MiFare Classic card
  - From when the system were taken online
- Contains encrypted / authenticated access token
  - With permissions and user / holder ID
  - Usually one key for entire environment
- Initial attack takes about 3-10 minutes
  - Cracking of key
- Cloning of card then takes just a few seconds

- Budget: 101€
  - Proxmark Mini: 100€
  - Blank card: 1€
- Benefits:
  - Possibility to copy access cards within seconds
  - Own access cards

Easy Cloning HID Access Card

What you need:

- Original card (e.g. HID H10301)
- Proxmark3
- Compatible card (e.g. HID or T55xx)
- Round about 2-3 seconds
- Only two commands needed:
  - > lf search
    remember <TAG ID>
    Change the card ;-)
  - > lf hid clone <TAG ID>
  - Enjoy your cloned Card

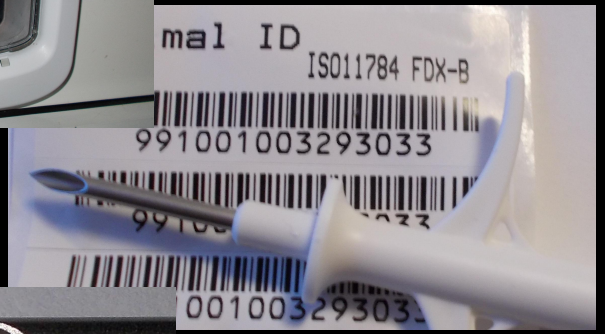
```
proxmark3> lf search
Checking for known tags:

HID Prox TAG ID: 2006ffffff
--------------------------------
Format: H10301 (HID H10301 26-bit)
Facility Code: 127
Card Number: 65535
Parity: Valid
--------------------------------
Valid HID Prox ID Found

proxmark3> lf hid clone 2006FFFFFF
#db# DONE!
```

Challenge: Programming a Cat Flap :-)

Cat initial doesn’t likes to go through the flap for programming!

Solution: Clone the pet’s ID (FDX-B ISO11784/85) :-)

- Use the proxmark3 nearby your cat - could become difficult…
- Use the known ID from pets vaccination certificate or ID injection (this “very” long no)
- Simulate ID using proxmark3 and hold into flap :-)
  proxmark 3> lf fdx sim 991001003293033



Automotive Security

- Breaking / attacking cars has been very popular over the past few years
- The community has produced various adapters, that allow access to CAN packets via Wireshark
  - Thus not requiring a lot of new skills to start
- Also: cars contain computers, that have USB and WiFi

Budget: 100€

- USB to CAN adapter: ~25€
- USB2.0 NIC: ~15€

Benefits:

- Full CAN BUS access
- Some car manufacturers expose Body Can Bus via ODB2
- Direct access to infotainment system (usually a root/admin shell)

CAN BUS

- CAN is the “backbone” BUS used in cars
  - Usually more than one
- There currently are only few security measures on the BUS
  - Spoofing and injection are easily possible, after identifying the correct signals
- Access is possible via the OBD2 socket in the cabin
  - Due to there being more than one BUS, one might have to be creative to reach the others

The Classics

- Spoof a low speed, then activate the parking assistant
  - Which will jolt the steering wheel
- Spoof a low distance warning from the collision sensors
  - And, well, BRAKE
- Spoof a lower speed, so that the pilot assists also works at higher speeds
- Send random packets and see what happens :)
- Custom build screens for detailed car status informations via ODB2

USB Ethernet Attacks

- Many modern cars have USB on the infotainment system
  - Play music from a USB stick
  - Connect Phone
- They don’t run magic, but simple Linux flavours, vxWorks or Windows
  - And thus support a lot of features via USB

- A broadly used entry vector is connecting a USB NIC
  - And receiving an IP address via DHCP or giving the car one
  - Many vehicles only work with specific chipsets
- ...portscan...
  - Telnet...ssh...
- ...firmware update image...
  - As source for the credentials...
- ...shell...

Fun with USB

- USB is very Universal
  - Keyboards, mice, printers, joysticks, phones, storage, cigarets
- Modern OS comes with drivers for A LOT of devices, both current and old ones
- USB device is identified by vendor & device ID
  - Facedancer can be used to emulate all possible IDs and show whether it would work on a target
- Budget: 50€ ++++
  - Facedancer: 30€
  - USB NIC 10€
  - USB keyboard: 10€
- Benefits:
  - Root, Admin
  - Havoc
  - A lot of fun in boring situations

Fun with USB

- Fuzzing via USB usually always results in a crash
  - Some joystick driver from the beginning of USB is bound to have vulnerability in it
- Attaching keyboards / mice often does the job
  - They give you access to OS specific shortcuts, i.e. Win+R

Devices with USB

- Cars
- Planes (entertainment system & cockpit)
- Oscilloscoes
- Printers
- Various medical devices in hospitals
  - Like the patient monitors in the rooms

DSL

- Most DSL contracts are being switched over to All-IP connections
  - No analog phone lines, just VoIP
- Routers are often automatically configured from the backend
- Simple setup allows full access to the connection between the router and the backend

Budget: ~150€

- Allnet ALL126AM2 DSLAM: ~100€
- A few DSL routers: ~50€

Benefits:

- Full MitM between DSL router and operator's backend
- Access to configuration data
- Access to configuration interfaces

Software

- Talk so far has given an insight into hacks and research that require some kind of hardware
- Obviously there are many topics out there, that require skills, but can be completely performed using Open Source software
- When doing “expensive” hardware attacks, one also always looks at the software components
  - Firmware, apps, backends
- Thus also software is in focus

Thanks! :)

Any Questions?