Hacks & Case Studies: Cellular Devices

Brian Butterly bbutterly@ernw.de - @badgewizard

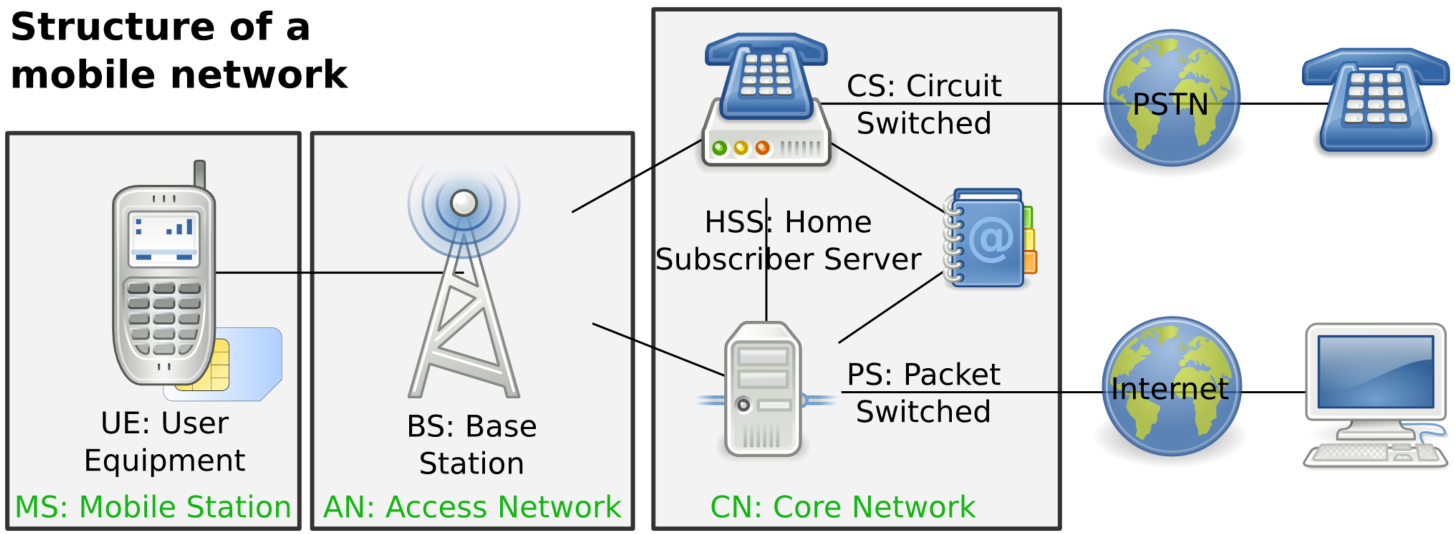
Hendrik Schmidt hschmidt@ernw.de - @hendrks_

This Talk is about...
Cellular Networks?

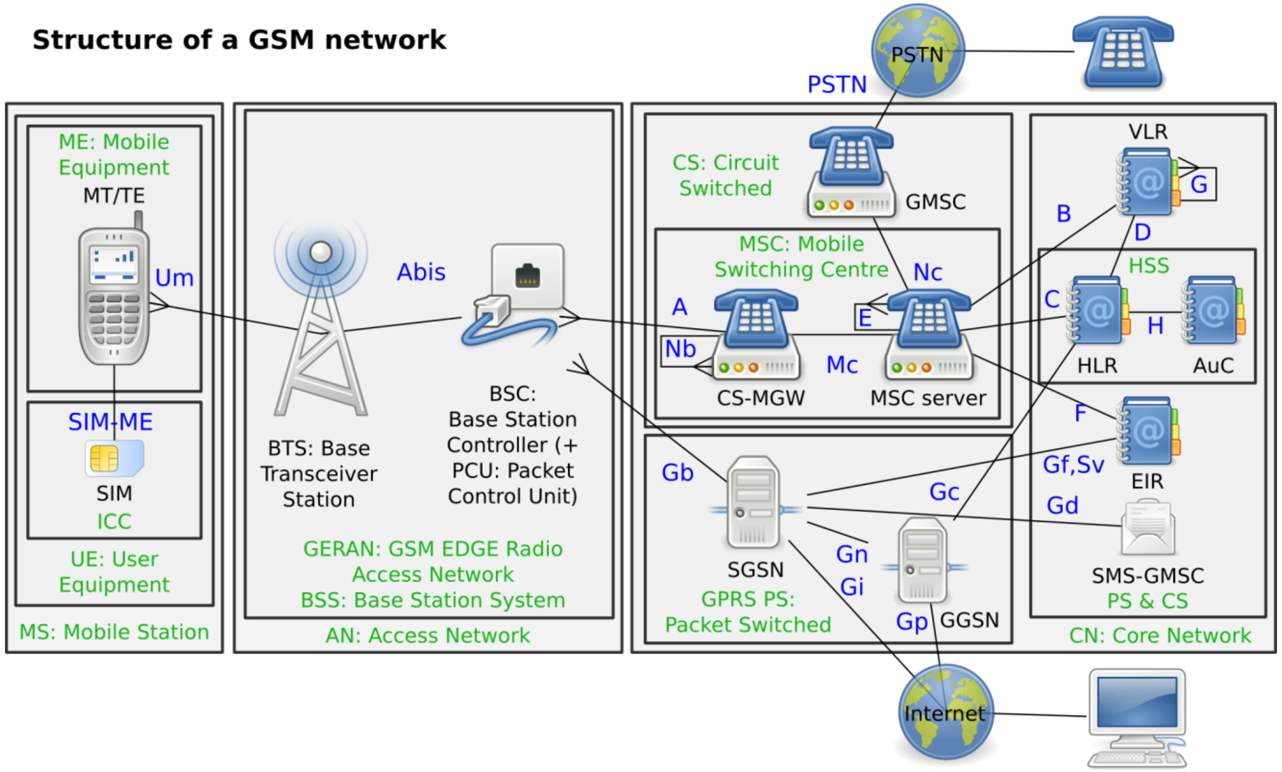
- Connecting $mobile_devices which each other
  - Internet of Things (GSM, EGSM, LTE, LTM-M)
  - Automotive Systems
  - Industry 4.0

- Using Services as
  - Voice
  - Data
  - Messaging
  - OTA Updates

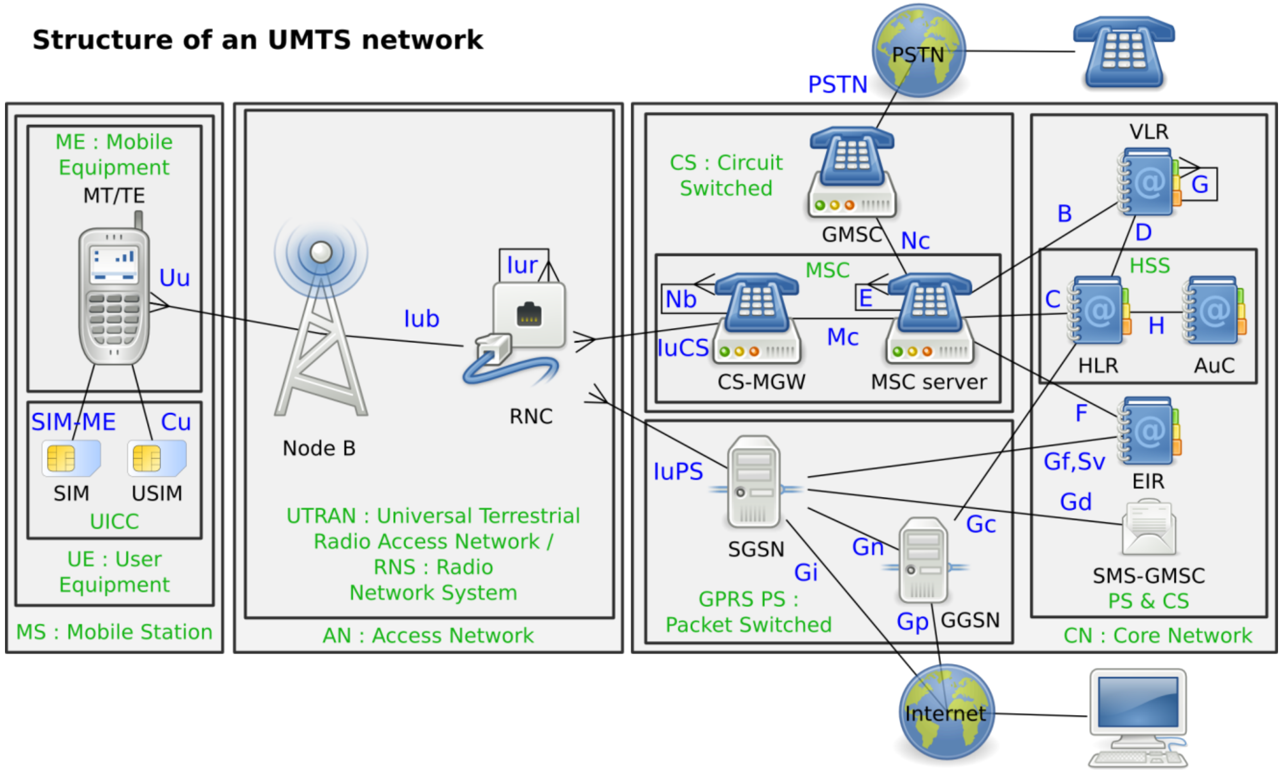
Common structure of mobile networks



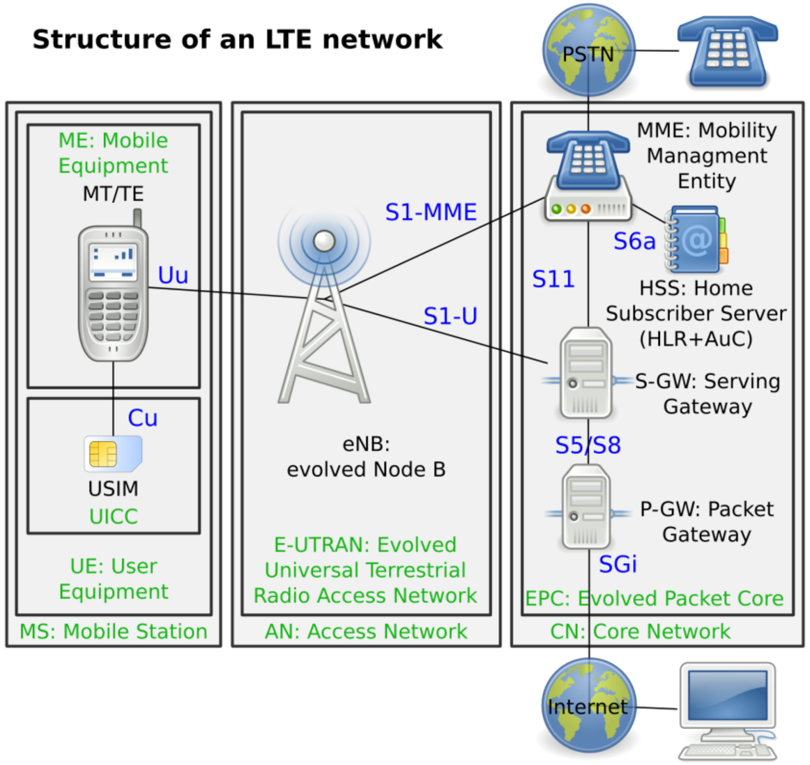
Structure of a GSM network



Structure of an UMTS network



Structure of an LTE network



The Goal?

- Simulating a real world environment / a provider
- Interception of mobile data

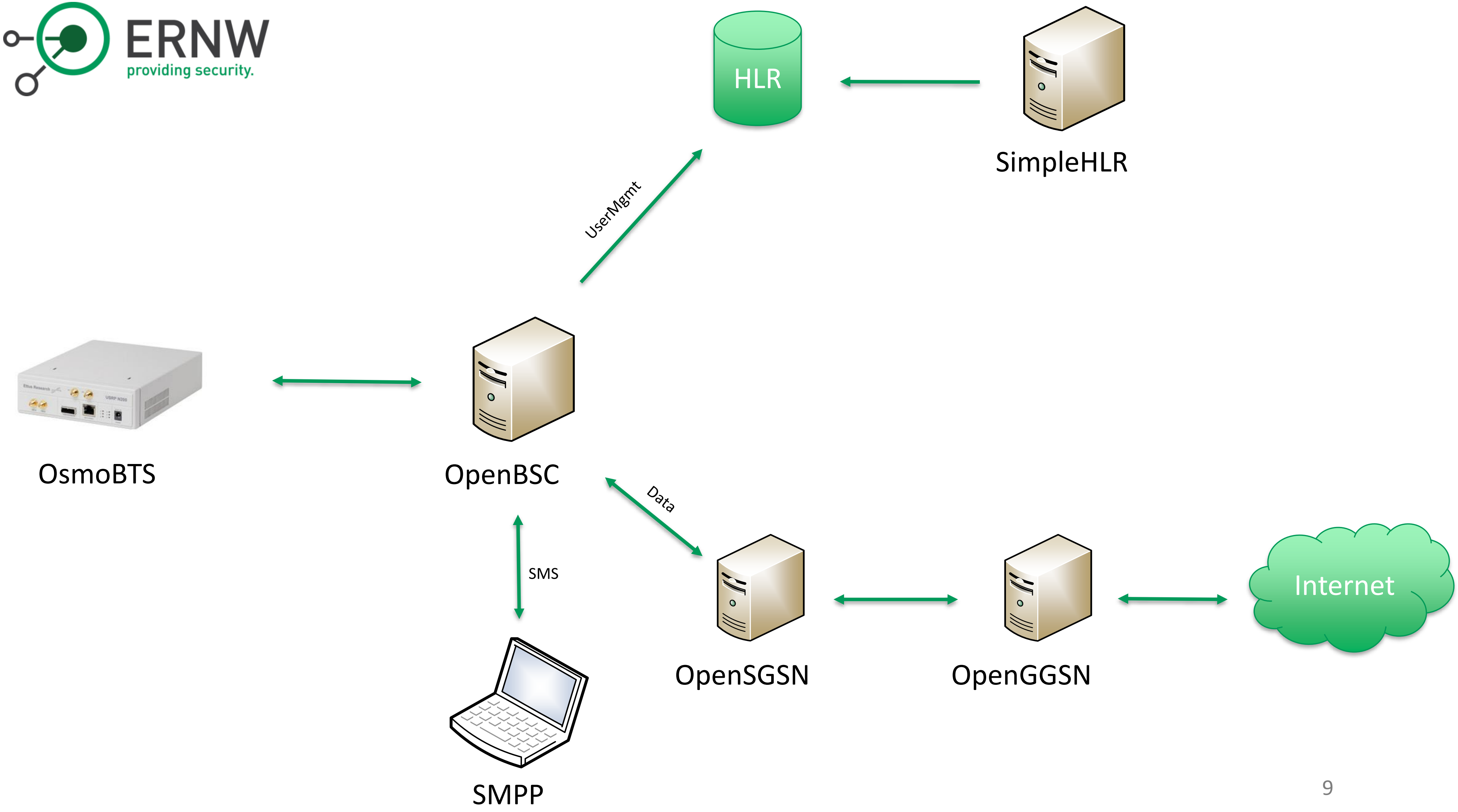
- Raw Data Access

  → Open Source?
- Portable
- Monitoring Capabilities
  - Wireshark?

→ What, we are building our own Stingray?

Tools

- GSM
  - phone: osmocomBB
  - network: openBSC, osmoBTS, openBTS, gr-gsm
- UMTS
  - phone: xgoldmon, gr-UMTS
  - network: openBTS-UMTS
- LTE
  - phone: Samsung Kalmia, SnoopSnitch
  - network: Aramisoft, openLTE, srsLTE, OpenAirInterface



HLR

SimpleHLR

UserMgmt

OsmoBTS

OpenBSC

Data

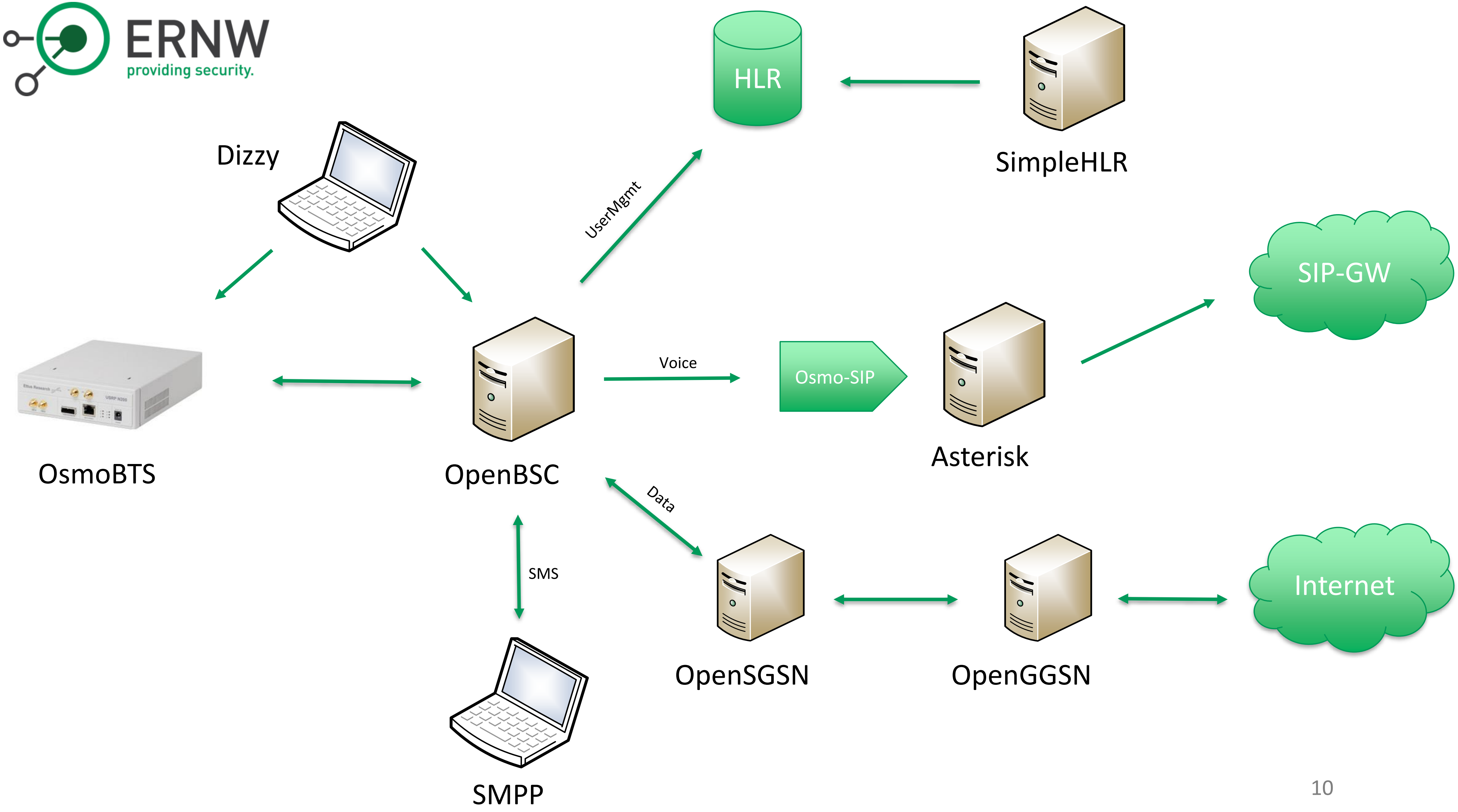
SMS

OpenSGSN

OpenGGSN

Internet

SMPP


HLR
SimpleHLR
Dizzy
UserMgmt
SIP-GW
Voice
Osmo-SIP
Asterisk
OsmoBTS
OpenBSC
Data
SMS
OpenSGSN
OpenGGSN
Internet
SMPP

IMSI-Catching –
Why is this Working?

- Mobile Connection depends on
  - MCC / MNC (Roaming SIM?)
  - Authentication/Encryption Keys
    → Can be ignored when using A5/0
  - APN
  - SMSC-Number

- Limitations
  - GPRS/EDGE/UMTS
  - Private/Restricted APNs

(Brief) Cell Selection

1. Build Cell Selection Table
2. Read Last Cell from SIM
3. Select Home Network (best/loudest)
4. Select Roaming Network (best/loudest)

Challenges:

- Cell Fixation
- Higher privileged networks (LTE)

→ Downgrade attacks

→ Jamming

ERNW
providing security.

Voice & Message Interception

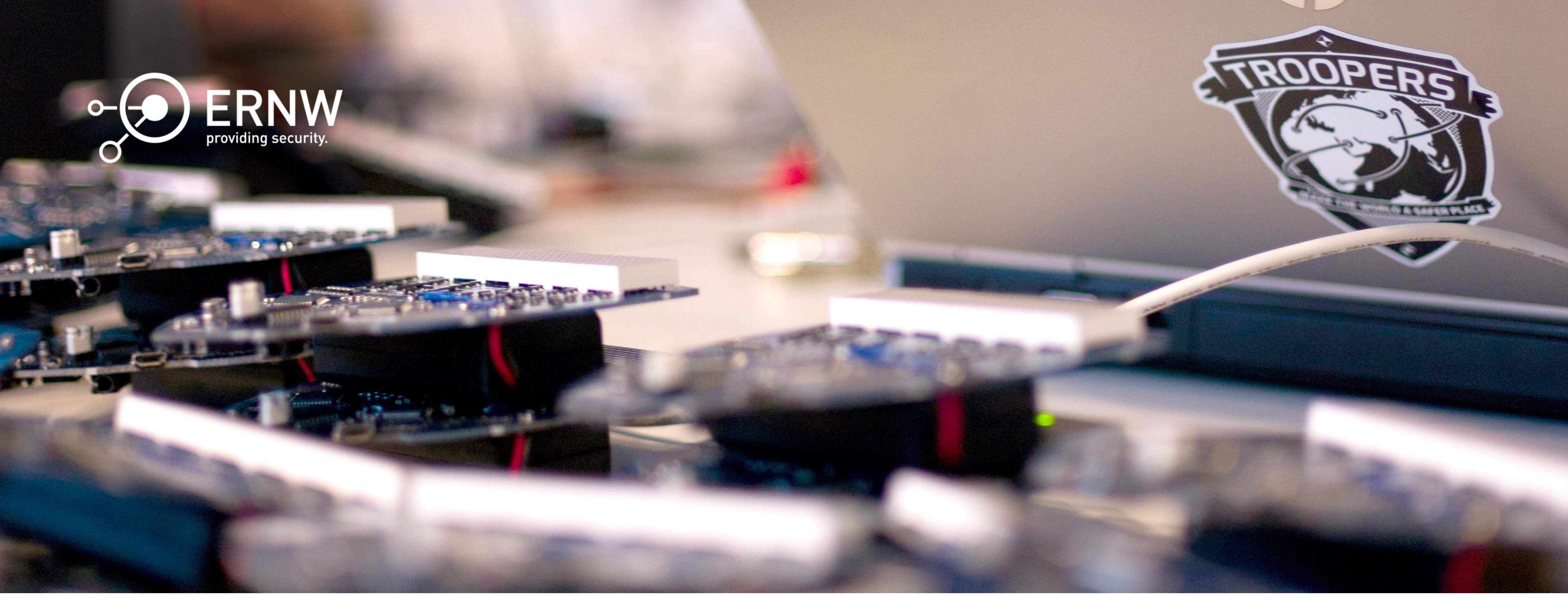
- Intercepting Calls & Messages like a Full-MitM-IMSI-Catcher
  - Testing implemented Security Measures (Authentication/Encryption)
  - Emergency Calls

- SIP based Uplink to PSTN

ERNW
providing security.

Data Interception (eliminating the magic)

- GPRS Data Access
- "Common" Pentest Methodology
  - Identification of running services
  - Eavesdropping & Encryption Tests
  - Man-in-the-Middle of Communication



Playing around with SMS

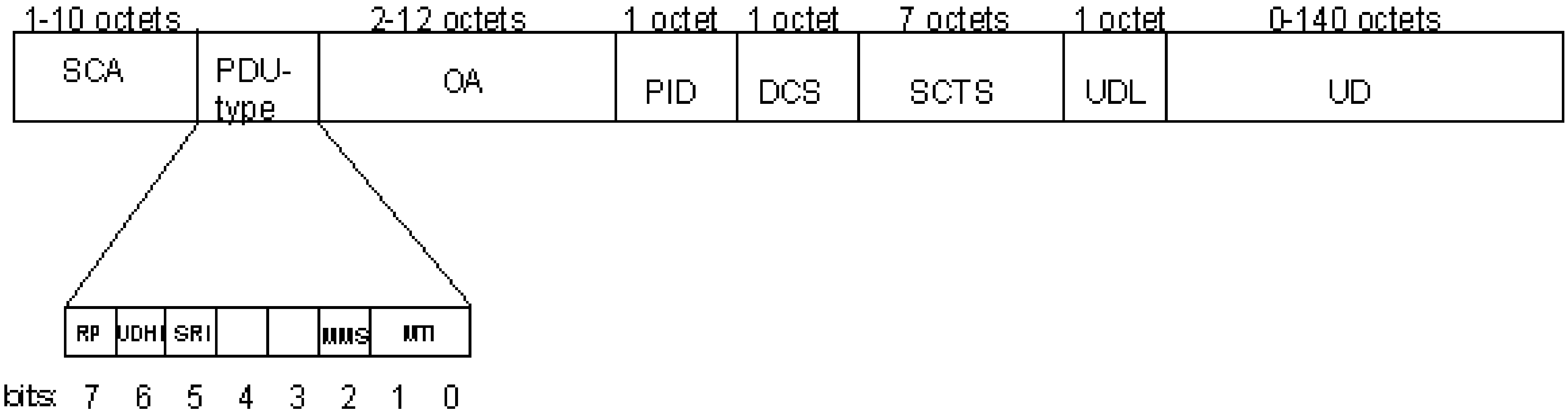
ERNW
providing security.

Definition MO/MT SMS

- The term MO message (mobile-originated message) is a message that a subscriber sent from a mobile device into the ExactTarget system. Setting up your system to respond to MO messages is similar to setting up a triggered email: you **create content and the system sends it out automatically** whenever anyone triggers the message. In the case of SMS, people trigger the message by sending you a keyword in a MO message.

- The term MT message (mobile-terminated message) refers to a message that goes out from the ExactTarget system and is received by the subscriber's mobile device. Setting up an MT message is similar to setting up a user-initiated email: you **choose the content and select the subscribers, and send the message at the time you choose**.

SMS Deliver (Mobile Terminated)



1-10 octets		2-12 octets	1 octet	1 octet	7 octets	1 octet	0-140 octets
SCA	PDU-type	OA	PID	DCS	SCTS	UDL	UD

RP	UDHI	SRI			MMS	MTI	
bits: 7	6	5	4	3	2	1	0

Source: http://www.activexperts.com/xmstoolkit/sms/technical/

Short Messaging Service

- SMS PDU Attacks
- SMS UDH Attacks
- Application access via SMS

- OTA Updates via (8-bit) binary Data
  - Depends on PID/DCS
- Data Forward to SIM

- Ever used a M2M SIM for free SMS?

The Python Code

```
def send_message(destaddr, dcs, pid, message):
        print 'Sending SMS "%s" to %s' % (string,dest)
        pdu = client.send_message(
                source_addr_ton=smpplib.consts.SMPP_TON_INTL,
                source_addr_npi=smpplib.consts.SMPP_NPI_ISDN,
                source_addr='1001',
                dest_addr_ton=smpplib.consts.SMPP_TON_INTL,
                dest_addr_npi=smpplib.consts.SMPP_NPI_ISDN,
                destination_addr=destaddr,
                data_coding=dcs,
                protocol_id=pid,
                esm_class=smpplib.consts.SMPP_GSMFEAT_UDHI,
                short_message=message,
                registered_delivery=False,
        )
        print(pdu.sequence)
```

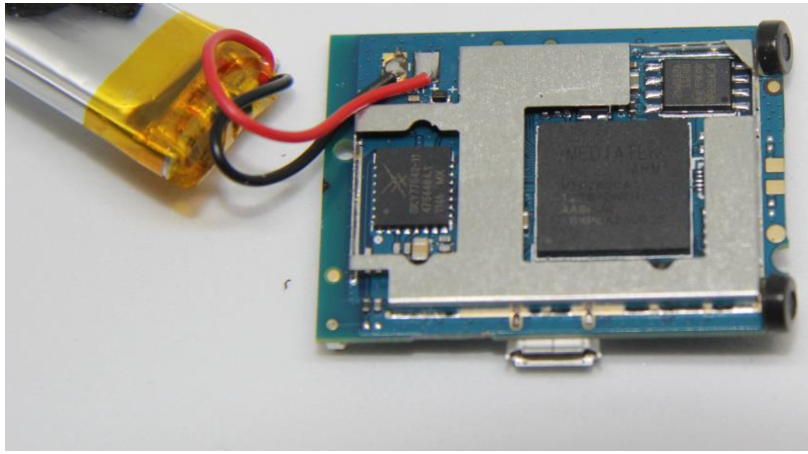
- TP-DCS:
  - GSM 7-Bit
  - 8-Bit Data
  - UCS-2
  - Message Class
- TP-PID
  - Forward SM
  - Data Download (125)
  - U(SIM) Data Download (127)
  - ... and more
- Furthermore
  - UDHI
  - Status-Reports
  - Tracing

Practical Use

Personal Tracker

- Remotely controlled via text message
- Send a text message containing "DW" to device
- Device responds with current "location"
  - "Loc:Please link: http://gpsui.net/smap.php?lac=1&cellid=2&c=262&n=23&v=6890 Battery:70%"

Security



- Solely based on knowledge of device's phone number

ERNW
providing security.

Gate Relay

- Control of relay for switch relay for (rolling) gates via text message or call
- Send text message containing xxxxCC to device to trigger relay
  - Here xxxx is a PIN

Triggering the Relay without the PIN

- 4 digits -> 10^4 -> 10000 combinations
  - Text message flat rate FTW
  - Or online services for sending text messages

- Simple bruteforce via text messages
  - 1111CC
  - 1234CC
  - 9999CC

RTU5024
Open Sliding/Swing/Garage Gate
Remote Switching ON/OFF
With a FREE Call from Authorized Numbers at Specified Time!
KKMOON
CE RoHS FC
Power
DC 9-15V
+
-
Relay Output
NO
COM
NC

ERNW
providing security.

Home Alarm System

- Arming, disarming and notifications via text message
- Send a text message with
- TEL:
- 1. 90900001
- 2.
- 3.
- 4.
- 5.
- Response with
- “Store phone numbers successfully.”

ERNW
providing security.

Security

- Security is based on having access to an authorized number
  - And of course knowing the device’s number

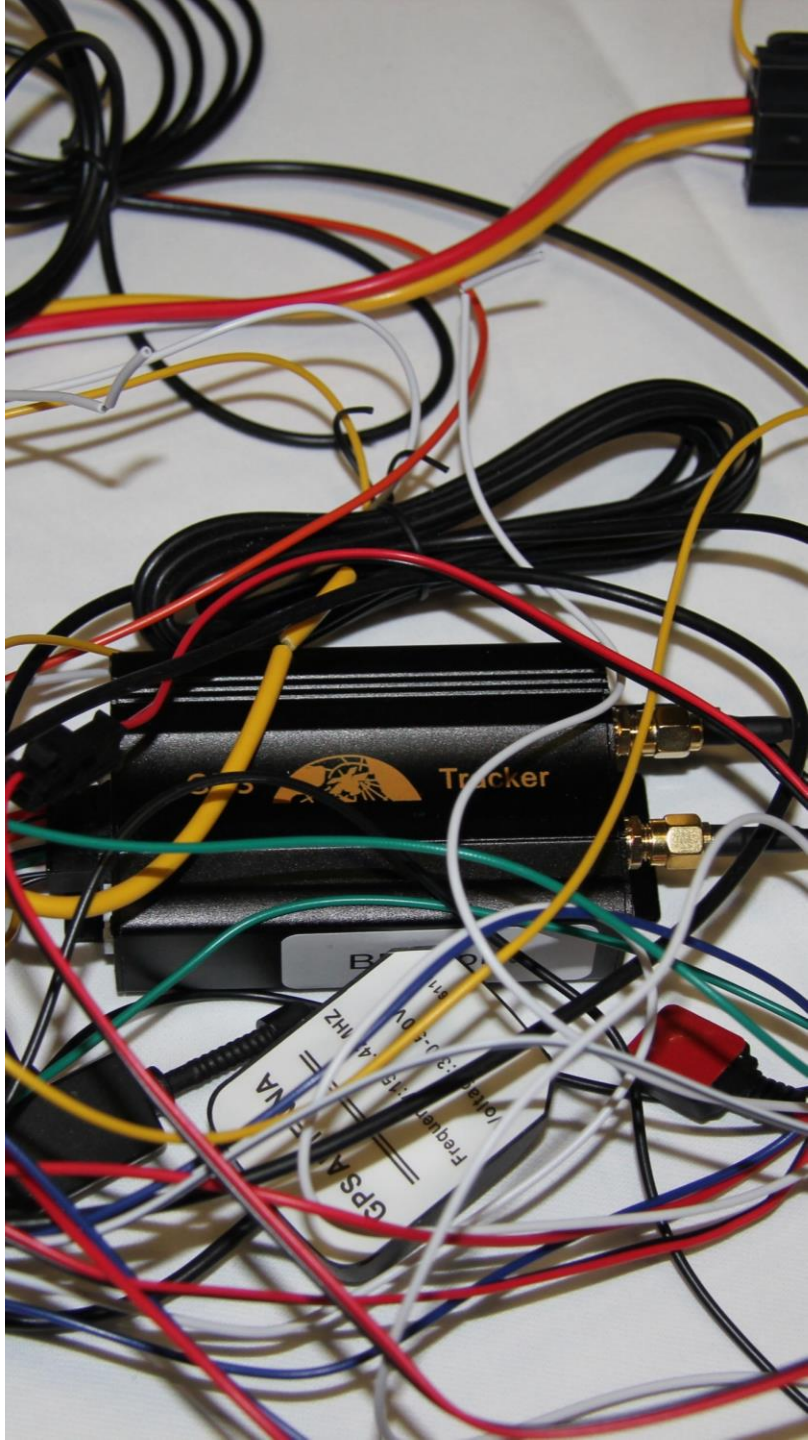
- Prior configuration everybody can remotely control the alarm system

GPS Tracker

- Simple GPS Tracker
- Regularly connects to backend and uploads its current position

GPS Tracker

- Data is transferred as plaintext
- An attacker in a man in the middle position can simply modify or spoof messages
  - In both directions



Security

- Security is based on credentials for management website

- Also solely based on cellular network’s encryption / security
  - Plaintext protocol can be intercepted when access to traffic is given

Custom APN

- The APN ("Access Point Name") is the first node a cellular devices with IP communication connects to
  - I.e. "internet.telekom"

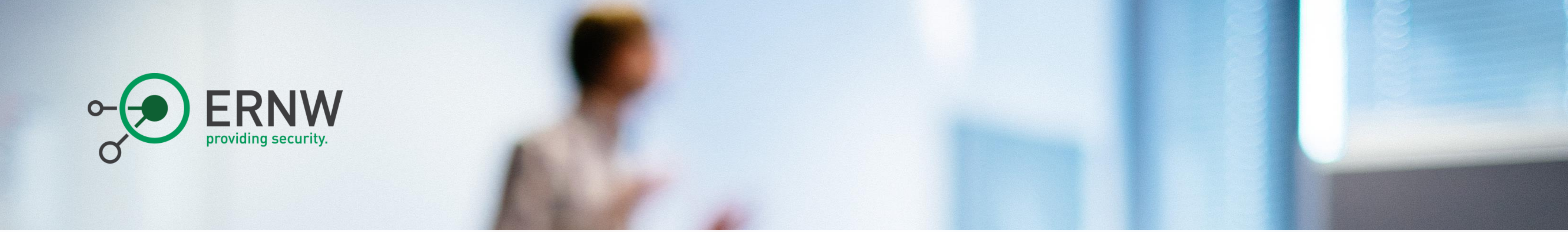
- They give the possibility to route traffic separated from the traffic of other cellular devices.

Custom APN

- Access to APN is generally open
  - Can be restricted based on SIM card or username and password
- Device has no way to identify validity on APN
  - And our setup accepts all APN names

Accessing APNs

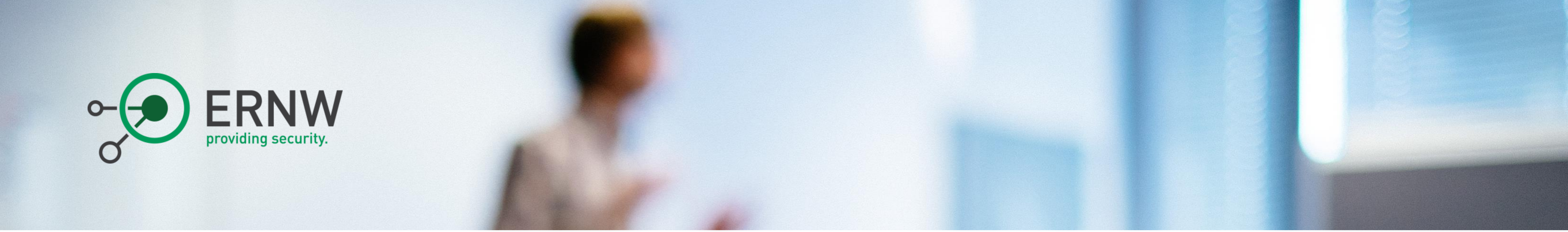
- Using a SIM card from a legit device an attacker can establish a connection to a custom APN
- And from there pipe custom traffic to all systems running behind the APN



Device Control via Text Message

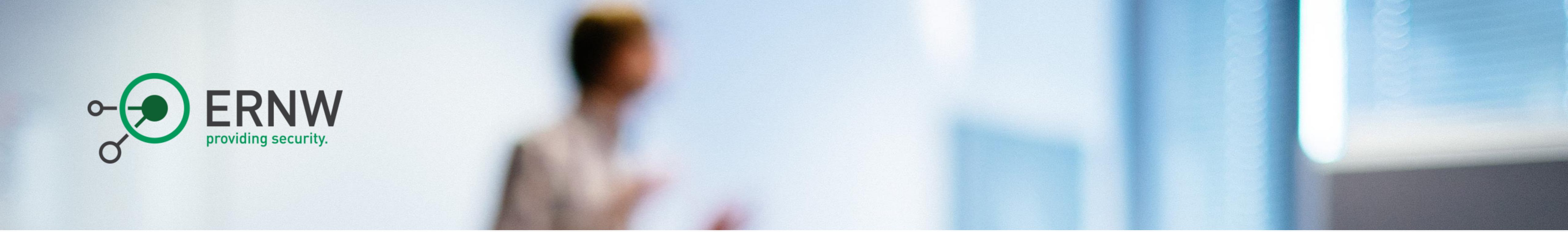
- Many different more or less “secure” solutions in use
  - Security WILL break usability

- All threatened by the use of fake basestations
  - Securing this approach properly would kill usability



Device Control via Voice Call

- Security always based on source number of phone call
  - Logical
- Also vulnerable to attacks using rogue basestations



ERNW providing security.

Device Control via IP

- Same issues as with “normal” IP communication
- You cannot rely on the network’s security. Own measures (encryption, HTTPs) must be applied
    - Can be very vulnerable to rogue basestations

Device Control via App

- Hard to say
  - They may use insecure text messages, or use something secure
- As apps offer usable interfaces, they enable to use of secure interfaces towards the devices

IoT Testing

- Running an own cellular network is key to properly testing IoT devices with cellular uplinks
- Many tasks can be automated by scripts
  - Or at least supported
- Also low level attacks become possible
  - SMS fuzzing
  - Attacks against OTA updates
  - Attacks based on hidden SMS

Summary

- Device security often relies on security of underlying network
- Networks are not as secure as often expected
- Tools for attackers are cheap, accessible and easy to use

- Specific hardening for cellular interfaces is necessary