09. – 12.12.2019
Frankfurt am Main

Brian Butterly

Praktische Angriffe auf Mobilfunkschnittstellen

#ittage

Practical Attacks against Cellular Interfaces

IT-Tage 2019

brian@security-bits.de ~~ www.security-bits.de ~~ @BadgeWizard

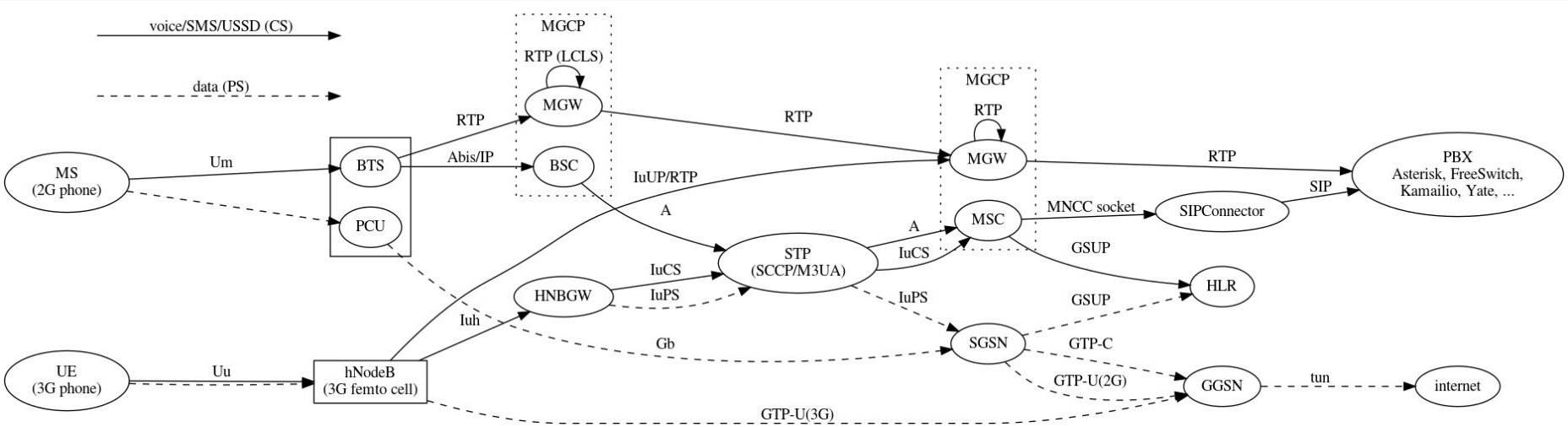
About Me

- Brian
  - @BadgeWizard
  - brian@security-bits.de
- Security Researcher / Hacker
  - Officially: “Incident Response”
- Hardware-, Embedded-, a bit of Telko-Security

Introduction

- Usage of cellular networks is still growing
- Evermore devices are planned to be using 5G in some way
- There a still a lot of “myths” concerning cellular security
- The content is this a quick reminder, that cellular is easy! :)

Network Structure Overview



Source: https://osmocom.org/projects/cellular-infrastructure/wiki/Osmocom_Network_In_The_Box

Equipment

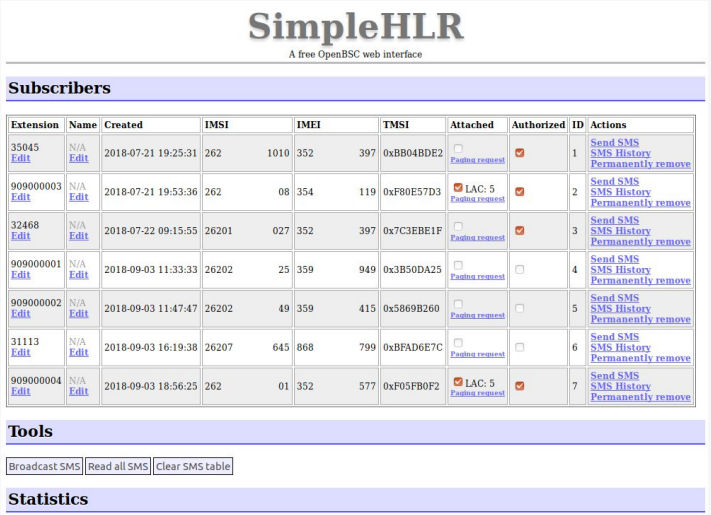
- BTS
  - SDR based with USRP (~1200€) or bladeRF (~400 €)
  - Actual BTS i.e. nanoBTS (~150€ from eBay)
  - More professional: SysmoBTS by Sysmocom
- Laptop / Virtual Machine
  - Linux box

Cable Setup

- Just playing with RF signals is against the law in most countries
  - In Germany the Bundesnetzagentur looks after the topic
- Thus direct cable connections can be used to not actually work with RF
  - The BTS has an RX and a TX antenna
  - The duplexer brings them onto a single cable
  - And also contains an attenuator

Software Setup

- Follow instructions for OpenBSC, OsmoSGSN, OsmoGGSN
  - Free Open Source software by Osmocom project
- Install osmo-SIP connector and Asterix
- Write a bunch of configuration
- Setup simpleHLR
- Start it all up



- A few hours following instructions

Calling

- Calls from client to client on network work natively
- External calling can be enabled by using osmoSIP-connector and Asterix
- Asterix can then be expanded using a SIP uplink

```
[incoming]
exten => abcdefe0,1,Log(Notice, "Incoming call via sipgate from
${CALLERID(num)}. exten is currentl$
exten => abcdefe0,2,Answer(),
exten => abcdefe0,n,Background(welcome)
exten => abcdefe0,n,Background(silence/9)
exten => abcdefe0,n,Hangup()
exten => _1337,1,Playback(tt-weasels)
exten => _1337,n,Hangup()
exten => _9090XXXXX,1,Log(Notice, "Incoming call for ${EXTEN}
from ${CALLERID(num)}.")
exten => _9090XXXXX,2,DIAL(SIP/${EXTEN}@192.168.1.20:5069)
exten => _9090XXXXX,n,Hangup()

include = Dialing-Errors

[internal]
exten => 1337,1,Answer
exten => 1337,2,Playback(tt-weasels)
exten => 1337,3,Hangup
exten => _9090XXXXX,1,DIAL(SIP/${EXTEN}@192.168.1.20:5069)
exten => 2222,1,DIAL(SIP/${EXTEN}@192.168.1.20:5069)
exten => _0!X.,1,Set(CALLERID(num)=SIPID)
exten => _0!X.,2,Dial(SIP/*31${EXTEN}@sipgate,30,trg)
exten => _0!X.,3,Hangup
include = Dialing-Errors
```

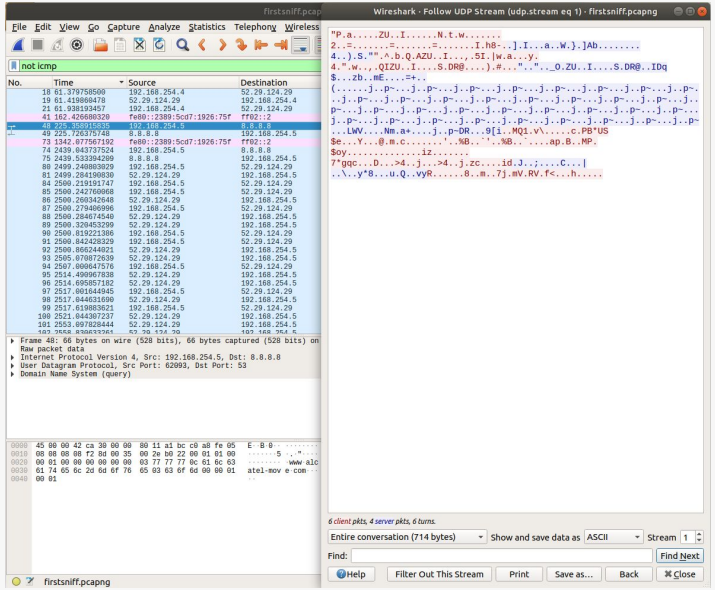
SMS

- Natively supported by the backend
- Can be sent via
  - SimpleHLR webinterface
  - Control socket
    - Optionally automated by a python script
  - Via SMPP interface

```
import telnetlib
import time

Host="127.0.0.1"
Port="4242"

tn = telnetlib.Telnet(Host,Port)

tn.write("subscriber id 1 sms sender id 1 send Hello there!\n")

tn.write("exit")
tn.write("exit")
```

IP Connectivity

- IP connectivity is possible by using OsmoSGSN and OsmoGGSN
- Supports custom APNs, authentication etc.
- Full IP traffic can then be forwarded to the internet
  - Or intercepted...

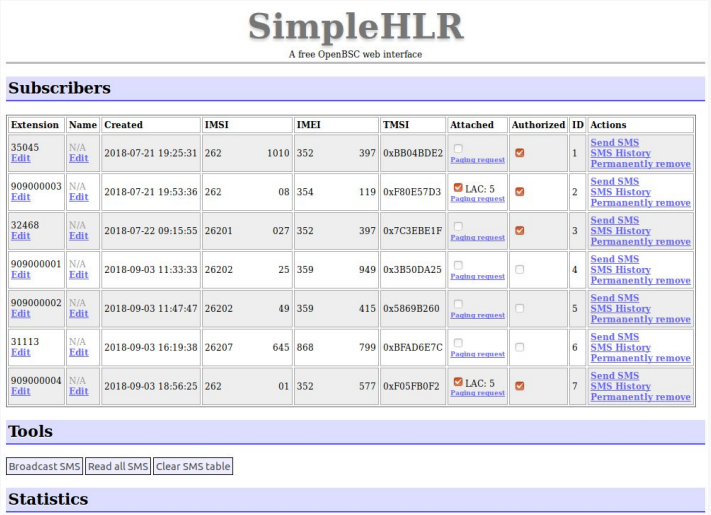


Addresses & IDs & Numbers

- IMEI
  - International Mobile Equipment Identity
  - “Unique” device ID
- IMSI
  - International mobile subscriber identity
  - Unique SIM card ID
- Phone Number
  - Allocated by cellular network
    - Usually allocated by IMSI
- IP Address
  - Allocated by the network (GGSN)

Phone Number

- Within our own network the number / extension is set depending on the IMSI
- It is configured in the HLR
  - Can be edited via console or directly in the table
- Thus, when a device joins our network we can call it, send it SMS
  - But we do not know it's normal phone number



SimpleHLR

A free OpenBSC web interface

Subscribers

Extension	Name	Created	IMSI	IMEI	TMSI	Attached	Authorized	ID	Actions
35045 Edit	N/A Edit	2018-07-21 19:25:31	262 1010	352 397	0xBB04BDE2	Paging request	☑	1	Send SMS SMS History Permanently remove
909000003 Edit	N/A Edit	2018-07-21 19:53:36	262 08	354 119	0xF80E57D3	☑ LAC: 5 Paging request	☑	2	Send SMS SMS History Permanently remove
32468 Edit	N/A Edit	2018-07-22 09:15:55	26201 027	352 397	0x7C3EBE1F	Paging request	☑	3	Send SMS SMS History Permanently remove
909000001 Edit	N/A Edit	2018-09-03 11:33:33	26202 25	359 949	0x3B50DA25	Paging request	☐	4	Send SMS SMS History Permanently remove
909000002 Edit	N/A Edit	2018-09-03 11:47:47	26202 49	359 415	0x5869B260	Paging request	☐	5	Send SMS SMS History Permanently remove
31113 Edit	N/A Edit	2018-09-03 16:19:38	26207 645	868 799	0xBFAD6E7C	Paging request	☐	6	Send SMS SMS History Permanently remove
909000004 Edit	N/A Edit	2018-09-03 18:56:25	262 01	352 577	0xF05FB0F2	☑ LAC: 5 Paging request	☑	7	Send SMS SMS History Permanently remove

Tools

Broadcast SMS | Read all SMS | Clear SMS table

Statistics

Availability

- While a device is in our network it can only receive SMS and calls from within our network
  - As we usually do not have an uplink (i.e. via SS7)
- Using a SIP uplink we can enable outgoing calls
  - But the the source number is the number of our SIP uplink
- IP connectivity works perfectly
  - Unless it is limited to certain APN

Access Point Name

- The APN is the name of the first gateway a cellular client uses to connect to the internet
  - I.e. internet.telekom.de, web.vodafone.de
- Thus kind of a virtual network
- Operators sell custom APNs to customers
  - Which are then separated from other mobile clients and have custom IP address spaces
  - And terminate at a different point

Custom APNs

- Access to an APN can be enforced by classical credentials, by IMSI or by IMEI
- Various companies use custom APNs to ensure that certain services are only exposed to certain clients
  - I.e. backend systems for the uplinks in cars

Coping with Custom APNs

- Our network can use custom APNs or just let every device connect to the same one
  - Simply accept all authentication
- If we need to allow traffic to a certain backend, we might need some magic
  - We can extract the SIM card from the victim, place it in a phone, let the phone dial into the network, with the correct SIM and IMSI and then forward traffic through there

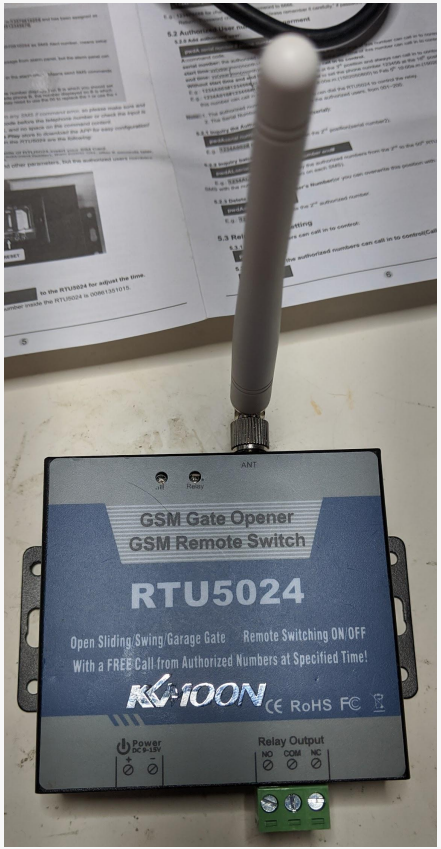
Real World Attacks

- By default a cellular client will not leave it’s network, when it has proper service
- To force it to connect to the attacker’s network, it has to be the only one or the strongest one after a disconnected
  - For a moving vehicle or a device on a person, attacking it in a building or in a tunnel can be very efficient
- This can either be triggered by protocol based attacks or by aggressively jamming away other signals

A Few Examples

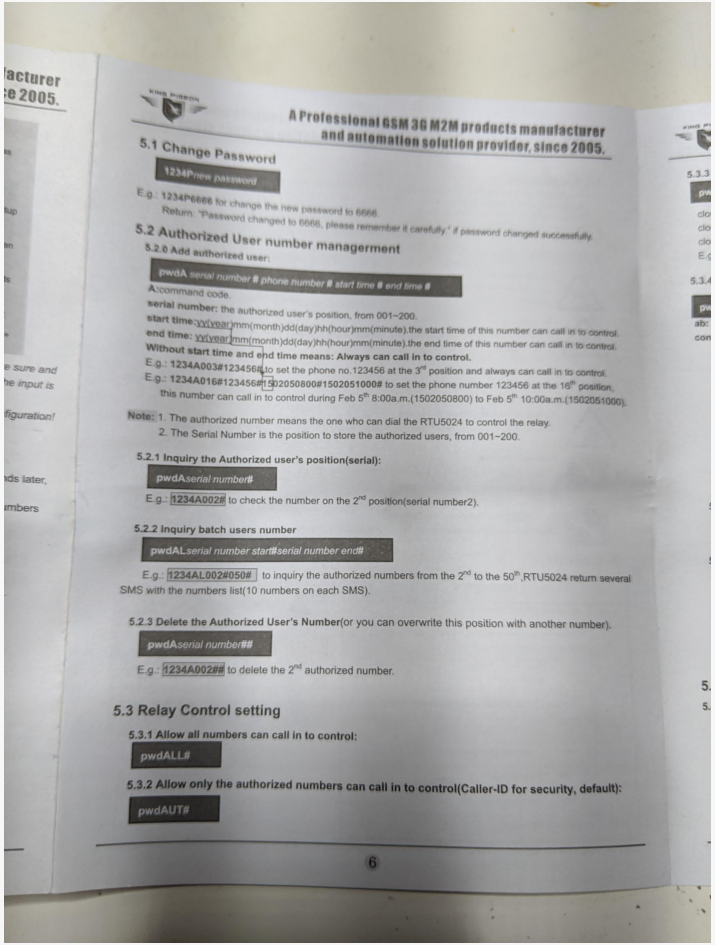
Gate / Garage Opener

- Rtu5024
  - ~25€ @Amazon
- Remote switch / relay with SMS and call control
  - For gates / garage doors
- For call control a list of numbers can be configured
  - When there is an incoming call, the relay is triggered



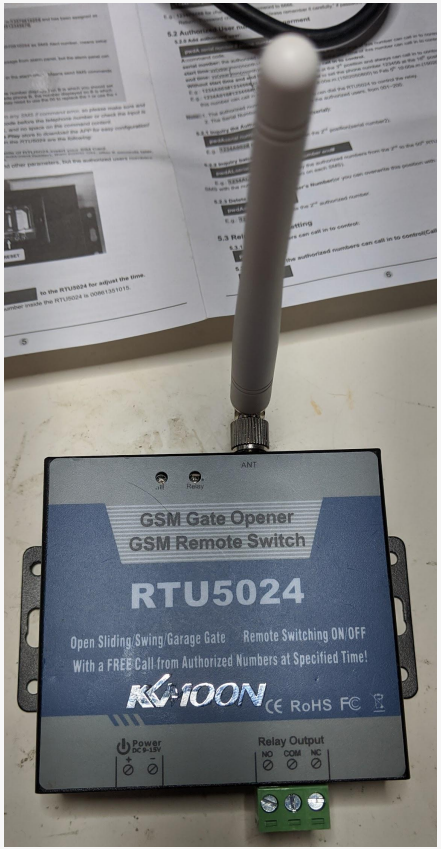
SMS Control

- An SMS with “xxxxCC” will enable the relay, “xxxxDD” will disable it
  - Here xxxx is a 4 digit PIN
- The PIN can be set by sending “xxxxPyyyy”
  - Where yyyy is the new 4 digit PIN



SMS Control

- So all we need to do, is send 10k SMS



Sending 10k SMS

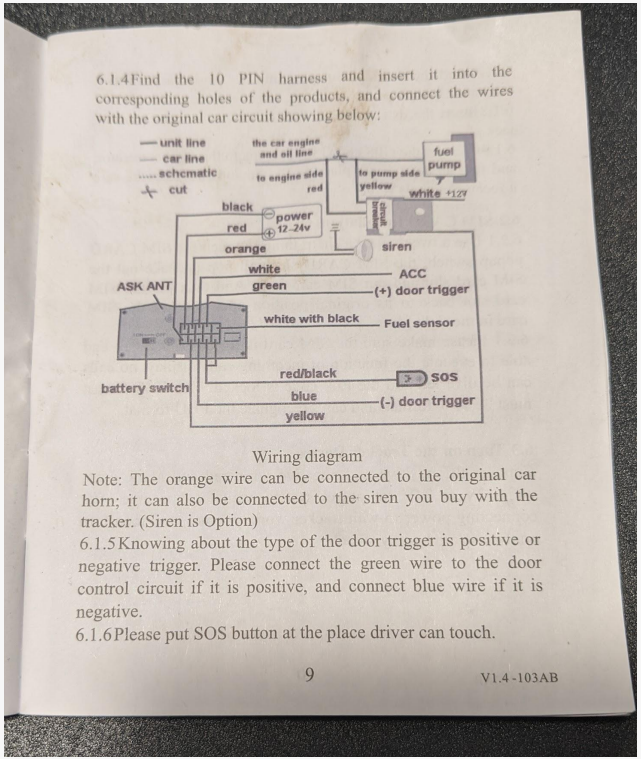
```
import telnetlib
import time

Host="127.0.0.1"
Port="4242"

tn = telnetlib.Telnet(Host,Port)

tn.write("subscriber id 1 sms sender id 1 send starting test\n")

pins=["%04d" % x for x in range(10000)]
for pin in pins:
  cmd = "subscriber id 2 sms sender id 1 send " + pin + "\n"
  print cmd
  tn.write(cmd)
  time.sleep(1)
tn.write("exit")
tn.write("exit")
```

Vehicle Immobilizer

- Cheap device from Amazon,
  - One of many
- Includes a GSM modem, GPS receiver, microphone & speaker and a relay to be connected to power supply of the fuel pump
- Can be controlled via app or webinterface
  - Some asian cloud service

Vehicle Immobilizer

- Initial setup is performed by entering IMEI into webinterface
  - IMEIs seem to iterated (as so often)
  - Some people seem to have provisioned their tracker into the demon account . . .
- Web/App can then be used to locate the vehicle, configure alarms based on speed / geo fencing, tap into the car (microphone)



6.1.4 Find the 10 PIN harness and insert it into the corresponding holes of the products, and connect the wires with the original car circuit showing below:

Wiring diagram

Note: The orange wire can be connected to the original car horn; it can also be connected to the siren you buy with the tracker. (Siren is Option)

6.1.5 Knowing about the type of the door trigger is positive or negative trigger. Please connect the green wire to the door control circuit if it is positive, and connect blue wire if it is negative.

6.1.6 Please put SOS button at the place driver can touch.

Vehicle Immobilizer

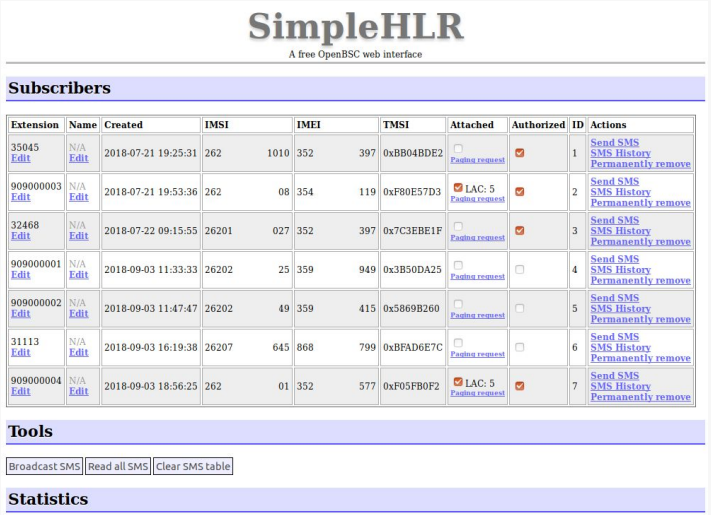
- Communication is done via a raw TCP stream
  - Different characters for different different commands
- No encryption / authentication except for the IMEI
- Thus vehicle location can easily be spoofed
- And..., the immobilizing feature. . .

Home Alarm System

- 100€ Home Alarm System from an electronics store
  - Comes with remote control, movement sensors, window switches
- Can be controlled via SMS and also sends out alerts via SMS
- Authentication is performed based on the source phone number

Home Alarm System

- While it's hard to spoof a call on a public network, it's easy to do so on a private one
- Simply change the Extension in the HLR
  - Or configure applicable phone in the SIP config
- Only open question is:
  - If an attacker goes for a specific target and alarm system, is the victim's phone number a secret?



SimpleHLR

A free OpenBSC web interface

Subscribers

Extension	Name	Created	IMSI	IMEI	TMSI	Attached	Authorized	ID	Actions
35045 Edit	N/A Edit	2018-07-21 19:25:31	262 1010	352 397	0xBB04BDE2	Paging request	☑	1	Send SMS SMS History Permanently remove
909000003 Edit	N/A Edit	2018-07-21 19:53:36	262 08	354 119	0xF80E57D3	☑ LAC: 5 Paging request	☑	2	Send SMS SMS History Permanently remove
32468 Edit	N/A Edit	2018-07-22 09:15:55	26201 027	352 397	0x7C3EBE1F	Paging request	☑	3	Send SMS SMS History Permanently remove
909000001 Edit	N/A Edit	2018-09-03 11:33:33	26202 25	359 949	0x3B50DA25	Paging request	☐	4	Send SMS SMS History Permanently remove
909000002 Edit	N/A Edit	2018-09-03 11:47:47	26202 49	359 415	0x5869B260	Paging request	☐	5	Send SMS SMS History Permanently remove
31113 Edit	N/A Edit	2018-09-03 16:19:38	26207 645	868 799	0xBFAD6E7C	Paging request	☐	6	Send SMS SMS History Permanently remove
909000004 Edit	N/A Edit	2018-09-03 18:56:25	262 01	352 577	0xF05FB0F2	☑ LAC: 5 Paging request	☑	7	Send SMS SMS History Permanently remove

Tools

Broadcast SMS | Read all SMS | Clear SMS table

Statistics

Solar Power Control Box

- Device for uploading usage statistics of a home solar system
  - And also doing some configuration and debugging
- Nicely running Windows CE
  - Old, but still in use
- Transmits data to a cloud backend
- Also allows remote access

Solar Power Control Box

- Remote access is....TELNET
- Device simply exposes a local telnet port via the cellular network
  - Which can sometimes receive a public IP address
  - Or is often at least reachable by other clients in the same APN
- Some of these devices have default passwords
  - Which often have large similarities to the device’s manufacturer

Now what?

Are we all lost?
What can be done better?

Cellular Network Security

- In 2G there is no way for the client to authenticate the network
  - Only the other way round
- Thus the client will connect to any network it finds suitable
  - A bit like a public WiFi, just MCC + MNC instead of the SSID
- In 3G and 4G, the client can authenticate the network
  - But there are a few flaws
- 5G is currently being researched

2G, 2G, 2G!

- Most cellular modems are able to fallback to 2G
  - I.e. when there is no other connectivity
- There also are various network and modem / baseband based vulnerabilities which can be used to trigger a downgrade to 2G
- Thus attacker will always be able to exploit the weaknesses of 2G networks

IP, IP & IP

- IP is IP, no matter whether it comes via cable, WiFi or cellular
- As long the cellular interface can be attacked, the client has to be able to protect itself
  - I.e. Application layer encryption
- Still many IoT devices don’t use SSL

- Modern developers should understand IP
  - Even though many player on the IoT market are re-implementing 15 year old vulns

Convenience

- Most simple and small products are developed with convenience in mind
  - Send a simple SMS to open a gate
  - Just perform a call to open a gate
- Sometimes security and convenience can be incompatible
  - You could transmit proper authentication via DTMF
  - Use some signed and encrypted token in the SMS
- It’s just not viable

Default Configuration

- Many products work out off the box
  - Insert SIM card, send SMS, done
- This yet again makes life easier for the user, but also implies a lack of proper security
- While a pairing / provisioning procedure might not be very nice, it ensures that the user applies a baseline of security measures

App Control

- While creating an app might be overhead, it allows the manufacturer the implementation of extra security measures
  - This doesn’t mean you can rely on an app. There are some that just send the insecure SMS
- One could i.e. still use SMS, but sign the payload
  - Or encrypt it

Not Everything is Bad

- There obviously are some very secure and nicely implemented solutions
  - With proper encryption and authentication
- Some commercial solutions simply wrap everything into a VPN tunnel
  - Problem solved

Cellular Pentesting

- When testing a new device, it is crucial, to also verify the security of the cellular interface
  - Especially when working with proprietary protocols
  - Don’t rely on self implemented measures, have them tested
- Ensure that your partner/supplier is actually able to test these interfaces
  - It’s sadly still a rather rare set of skills

Thanks for your time

Questions?

brian@security-bits.de ~~ www.security-bits.de ~~ @BadgeWizard