(n+1)G - Security

IMI 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
  - Done a fair amount of research and security testing on cellular clients and backends

The Opening

- Option 1:
  - NanoBTS, 1800MHz, eBay, 100€-200€
  - 1800MHz Multiplexer, Sysmocom 120€
    - Cable setup
    - Because I currently do not have a license to actually transmit data over the air
  - Cheap vehicle immobilizer, Amazon <40€
  - Complete OpenBSC Backend, Osmocom Project, Free

- **Option 2:**
  - Motorola C118
  - Running OsmocomBB
    - Open source operating system for certain mobile phones
  - Sniffing on a frequency belonging to ???
    - Fully passive
    - Legally sniffing is a very very grey area
    - Obviously this was just for research & demonstration purposes
  - Otherwise said, you've just seen a 12€ IMSI Catcher in action

State of Cellular Security

- Black Magic! & Best explained with a simple example
- Text on the right is just there for afterwards, don't read it :)

Dialog with a customer from a while ago: "We've received your device and can't get it to work" - "What's the problem?" - "It doesn't connect" - "What does the debug output say?" - "Everything ok" - "So it works!" - "No it doesn't connect to the backend" - "But it says ok, so it's fine. You're doing something wrong" - "Here's the PCAP of the failed connections" - "How did you get that PCAP, we've never seen that kind of traces!?" - "Well we sniffed it!" - "What?" - "The traffic on the cellular interface" - "But...How? You can't just do that"

2G - 2007: The GSM Scanner Project

- THC Group

- Using gammu & debug mode on Nokia 3310 for sniffing GSM traffic

Hackers start buying Nokia 3310

2G - 03.2008: Intercepting GSM traffic

- Black Hat DC: THC Group

- Sniffing GSM traffic with a Nokia 3310
- Stating broken A5/0, A5/1, A5/2
  - Using Rainbow tables, unpublished
- Sniffing location data in plaintext
- Sniffing IMSI

Hackers buy even more 3310

2G - 12.2009: Using OpenBSC for fuzzing of GSM handset

- 26C3: Harald Welte

- Running an own 2G network and utilizing it for fuzzing and attacking mobile phones

libsmpp

```
git clone git://git.osmocom.org/libsmpp34.git
cd libsmpp34
autoreconf -fi
./configure
make
sudo make install
sudo ldconfig
```

osmo-ggsn

```
git clone git://git.osmocom.org/osmo-ggsn/
cd osmo-ggsn
autoreconf -fi
./configure
make
sudo make install
sudo ldconfig
```

osmo-sgsn

```
git clone git://git.osmocom.org/osmo-sgsn/
cd osmo-sgsn
autoreconf -fi
./configure
make
sudo make install
sudo ldconfig
```

osmo-sip-connector

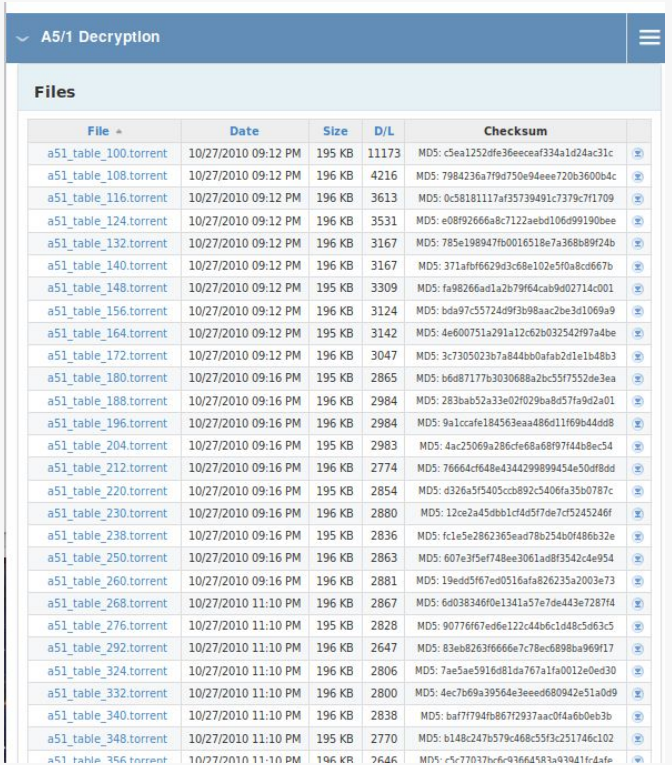
```
git clone git://git.osmocom.org/osmo-sip-connector
cd osmo-sip-connector
autoreconf -fi
./configure
make
sudo make install
```

:)

2G - 12.2009: GSM: SRSLY?

- 26C3: Chris Paget, Karsten Nohl

- Enabling cracking of A5/1 encryption with about 2TB of rainbow tables
- Published tools & rainbow tables for everyone to decrypt A5/1 encrypted communication



File	Date	Size	D/L	Checksum
a51_table_100.torrent	10/27/2010 09:12 PM	195 KB	11173	MD5: c5ea1252dfe36eeceaf334a1d24ac31c
a51_table_108.torrent	10/27/2010 09:12 PM	196 KB	4216	MD5: 7984236a7f9d750e94eee720b3600b4c
a51_table_116.torrent	10/27/2010 09:12 PM	196 KB	3613	MD5: 0c58181117af35739491c7379c7f1709
a51_table_124.torrent	10/27/2010 09:12 PM	196 KB	3531	MD5: e08f92666a8c7122aebd106d99190bee
a51_table_132.torrent	10/27/2010 09:12 PM	196 KB	3167	MD5: 785e198947fb0016518e7a368b89f24b
a51_table_140.torrent	10/27/2010 09:12 PM	196 KB	3167	MD5: 371afbf6629d3c68e102e5f0a8cd667b
a51_table_148.torrent	10/27/2010 09:12 PM	195 KB	3309	MD5: fa98266ad1a2b79f64cab9d02714c001
a51_table_156.torrent	10/27/2010 09:12 PM	196 KB	3124	MD5: bda97c55724d9f3b98aac2be3d1069a9
a51_table_164.torrent	10/27/2010 09:12 PM	195 KB	3142	MD5: 4e600751a291a12c62b032542f97a4be
a51_table_172.torrent	10/27/2010 09:12 PM	196 KB	3047	MD5: 3c7305023b7a844bb0afab2d1e1b48b3
a51_table_180.torrent	10/27/2010 09:16 PM	195 KB	2865	MD5: b6d87177b3030688a2bc55f7552de3ea
a51_table_188.torrent	10/27/2010 09:16 PM	196 KB	2984	MD5: 283bab52a33e02f029ba8d57fa9d2a01
a51_table_196.torrent	10/27/2010 09:16 PM	196 KB	2984	MD5: 9a1ccafe184563eaa486d11f69b44dd8
a51_table_204.torrent	10/27/2010 09:16 PM	195 KB	2983	MD5: 4ac25069a286cfe68a68f97f44b8ec54
a51_table_212.torrent	10/27/2010 09:16 PM	196 KB	2774	MD5: 76664cf648e43442998994 5e50df8dd
a51_table_220.torrent	10/27/2010 09:16 PM	195 KB	2854	MD5: d326a5f5405ccb892c5406fa35b0787c
a51_table_230.torrent	10/27/2010 09:16 PM	196 KB	2880	MD5: 12ce2a45dbb1cf4d5f7de7cf5245246f
a51_table_238.torrent	10/27/2010 09:16 PM	195 KB	2836	MD5: fc1e5e2862365ead78b254b0f486b32e
a51_table_250.torrent	10/27/2010 09:16 PM	196 KB	2863	MD5: 607e3f5ef748ee3061ad8f3542c4e954
a51_table_260.torrent	10/27/2010 09:16 PM	196 KB	2881	MD5: 19edd5f67ed0516afa826235a2003e73
a51_table_268.torrent	10/27/2010 11:10 PM	196 KB	2867	MD5: 6d038346f0e1341a57e7de443e7287f4
a51_table_276.torrent	10/27/2010 11:10 PM	195 KB	2828	MD5: 90776f67ed6e122c44b6c1d48c5d63c5
a51_table_292.torrent	10/27/2010 11:10 PM	196 KB	2647	MD5: 83eb8263f6666e7c78ec6898ba969f17
a51_table_324.torrent	10/27/2010 11:10 PM	196 KB	2806	MD5: 7ae5ae5916d81da767a1fa0012e0ed30
a51_table_332.torrent	10/27/2010 11:10 PM	196 KB	2800	MD5: 4ec7b69a39564e3eeed680942e51a0d9
a51_table_340.torrent	10/27/2010 11:10 PM	196 KB	2838	MD5: baf7f794fb867f2937aac0f4a6b0eb3b
a51_table_348.torrent	10/27/2010 11:10 PM	195 KB	2770	MD5: b148c247b579c468c55f3c2517 46c102
a51_table_356.torrent	10/27/2010 11:10 PM	196 KB	2646	MD5: c5c77037bc6c93664583a93941fc4afe

More and more networks enforce using A5/3

2G - 12.2010: SMS-o-Death

- 27C3: Nico Golde, Collin Mulliner

- Insight into SMS fuzzing
- DoS against various mobile phones by sending type 0 and other “funky” SMS

Mobile manufacturers start implementing measures

2G - 12.2010: Wideband GSM Sniffing

- 27C3: Karsten Nohl, Sylvain Munaut

- Using old Motorola phones and OsmocomBB to sniff 2G communication
- Direct output to wireshark

Hackers buy stacks of old Motorola phones

3G - 06.2011: Breaking into Vodafone UK 3G femto cells

- THC Group

- Access is possible via a serial interface on the device's PCB
- Allows tapping into phone calls of phones connected to the cell

Vodafone initially ignores the vulns, then decides to fix them
Researchers start buying the cells

2G - 03.2013: Let me answer that for you

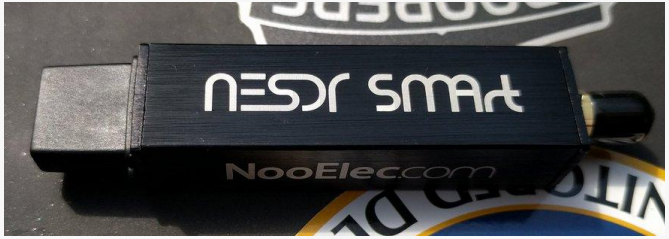
- TelcoSecDay: Nico Golde, Kevin Redon

- DoS attack against 2G networks by answering all paging requests in a certain area with a few mobile phones

:)

2G - 2014 GR-GSM

- Tool by Piotr Krysik

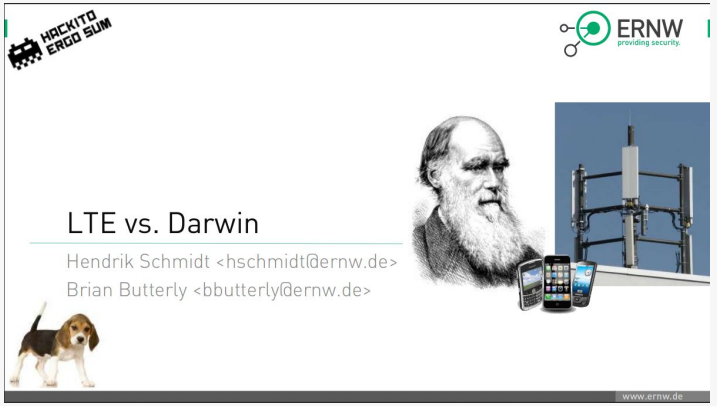


- Using software defined radio for sniffing GSM traffic
- Compatible with 20€ RTL SDR sticks
  - DVB-T Sticks that can be reused as a sniffer
- Direct output to wireshark

SDR sticks rise in price

4G - 01.2014: LTE vs. Darwin

- ShmooCon: Hendrik Schmidt, Brian Butterly



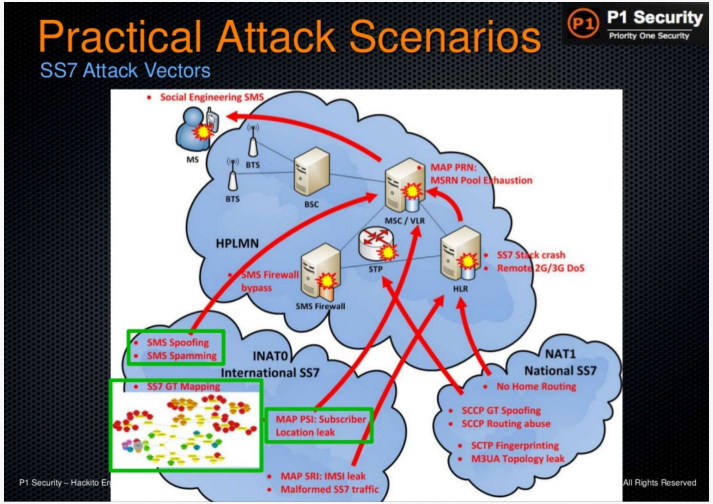
- Conceptual/design flaws and issues in 4G standards
- Theoretical attacks against LTE base stations

Invitation to share more details with GSMA

2G - 05.2014: Worldwide Attacks on SS7 Networks

- Hackito Ergo Sum: Pierre-Olivier Vauboin, Alexandre De Oliveira

- Rerouting calls and messages via direct access to the worldwide 2G backend network



Telcos start hardening SS7 infrastructure

2G - 05.2014: Hacking Telco equipment, The HLR/HSS

- Hackito Ergo Sum: Laurent Ghigonis

- Insight into security of cellular core networks
- Disclosure of various vulnerabilities and attack methods

:)

4G - 11.2015: LTE and IMSI catcher myths

- Black Hat EU: Ravishankar Borgaonkar, Altaf Shaik

- Flaws in authentication, convincing phone to connect to fake BTS, relying on vulns in device and network
- Downgrade attacks, force phone to leave “secure” 4G network and use 2G instead

4G - 05.2016 IMSecure - Attacking VoLTE and other Stuff

- Area 41: Hendrik Schmidt, Brian Butterly

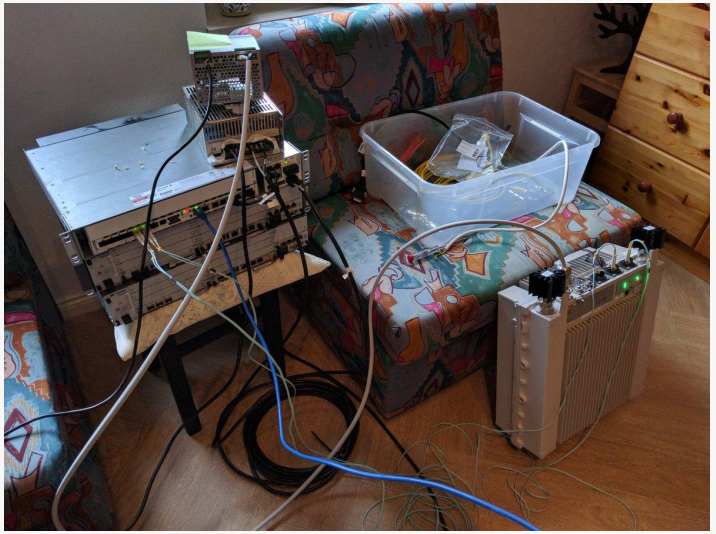
- Insight into security aspects of VoLTE
- Presentation of attack paths, vectors and flaws

Various VoIP security researchers also start looking at VoLTE

4G - 08.2016: Attacking BaseStations

- DefCon: Hendrik Schmidt, Brian Butterly

- Insight into the architecture and issues with 4G basestations
  - Also insight into how insecurely actual networks are configured
- Fully configure MetroPCS basestation acquired from eBay and taken to pieces
- Emulation of core backend components



Invitation to GSMA
Telcos understand the issues

4G - 07.2017: New Adventures in Spying 3G & 4G

- Black Hat: Ravishankar Borgaonkar

- Passively sniffing 3G & 4G networks to track phones
- Using fake SIM cards

:)

4G - 12.2017: Attacking NextGen Roaming Networks

- Black Hat EU: Hendrik Schmidt, Daniel Mende

- Insight into the 4G successor of SS7
- Transferring known vulnerabilities from SS7 to the new technology

Telcos started thinking about maybe changing things?

4G - 06.2019: Spoofing Emergency Alerts

- University of Colorado Boulder

- Project shows how easily Presidential Alert Messages can be spoofed
  - Partially motivated by the Hawaii missile alert
- Single transmitter sufficient to cover a complete football stadium

:)

Tracking, Sniffing, Spoofing

- Attack vectors have changed
- 4G has become more secure
- Still a lot of old issues have been re-implemented in 4G

5G - A New Hope

- Many features presented in 5G where actually concepted for 4G
  - But never implemented
- NB-IoT and LTE-M kind of failed during the 4G era
  - Consumer market was priority 1, protocols weren’t implemented in time, thus never used
- Security community has proposed many changes during 2G, 3G, 4G
  - Some have been accepted

5G - 08.2019: New Vulnerabilities in 5G Networks

- Black Hat: Altaf Shaik, Ravishankar Borgaonkar

- Tracking: Same protocol, same issues as in 4G
- Downgrade: Still possible
- NB IoT partially not encrypted
- Battery drain attacks by keeping IoT devices alive

Things are starting just as bad with 5G as with 4G
Issues are being addressed, but . .

Summary on a low budget

- Attackers can
  - Sniff 2G & crack, unless it's A5/3
  - Set up fake 2G basestations/networks and trick devices to connect
  - Force devices from 4G to downgrade to insecure 2G
- 2G Vulns still result in significant issues for 4G networks
  - And probably also 5G
- Also both 4G networks and clients are vulnerable to certain attacks

Not everything is bad

- 2G: A5/3 is still ok
- 4G is comparably secure
  - If there wasn't the downgrade
- 5G seems to be starting as "secure" as 4G

- The IoT protocols are new and thus will be flawed
  - Experience....

Outlook

- Companies have to learn to never solely rely on transport networks
  - And telkos should be more transparent about this
- Always use some kind of application layer encryption
  - TLS FTW
- Maybe think about dropping 2G all together
- Think twice whether you really need RF

Thanks for your time

Questions?

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