Peeking over the Cellular Walled Gardens
A Method for Closed Network Diagnosis

Byeongdo Hong ¹, Shinjo Park ²
Hongil Kim ¹, Dongkwan Kim ¹
Hyunwook Hong ¹, Hyunwoo Choi ¹
Jean-Pierre Seifert ², Sung-Ju Lee ¹
Yongdae Kim ¹

¹KAIST
²TU Berlin & Telekom Innovation Labs

TSD '18, 2018. 3. 13.
Shinjo Park
Doctoral student at SecT, TU Berlin
Research interests
  - Cellular network system
  - Baseband security
  - Telco equipment security

Hongil Kim
Ph.D. student at System Security Lab. KAIST
Research interests
  - Cellular network system
  - Mobile device security
  - Internet of Things (IoT) security
Contents

- Problem definition: what do we want to see?
- Signaling data collection and analysis framework
- Dataset and problem overview
- Time-related misconfigurations
- Synchronization problems
- Security issues
- Conclusion
Cellular Walled Garden

- 3GPP standard allows interoperability between each different entities
- Several things hinder this in reality
  - Standard itself allows various optional procedures, which may collide with each other
  - Optimization is considered as an operator know-how and not shared between companies
  - Even multinational operators are not operating in the same principle in multiple regions due to regulation and interoperation issues
- Relationship between operators and equipment suppliers
  - Equipment suppliers makes whatever operator wants
  - Potentially insecure and inefficient decision
  - Operational outsourcing introduced a new set of problem
How to diagnose problems in mobile network?
- Large dataset of control plane
- Comparative study
- Root cause analysis

We propose a new diagnosis methodology:
Comparison of control plane implementation

Design goals
- Efficiently, easily and quickly: re-utilizing existing method to identify a problematic point
- How and where we should collect signaling messages?
Definition of Problem and Our Approach

- Even simple operation like voice call could be implemented differently between operators
- Only high-level key performance indicators (KPIs) are visible to the user, control plane interaction is abstracted by the OS
- We focus on the following aspects by studying signaling messages collected from UEs
  - How fast and when the messages are sent
  - What kind of optional procedures are performed
  - Why certain procedures are failing
  - Interaction between multiple layers: RRC, NAS (EMM, ESM, MM, SM, CM)
- We systematically collect traces from CSFB voice calls
  - Voice call is one of essential services
  - Details are explained in the following slides
Why CSFB?

- Yes, we know that CSFB will be eventually replaced by VoLTE or Vo5G
- Includes multiple procedures in 3G and 4G: RRC, NAS (E)MM, CM, (E)SM
- Both 3G and 4G procedures are independently implemented
- Still relevant in 5G, as it will also be bridged to 3G and 4G
CSFB Signaling Trace Collection Method

- One or more phone connected to the PC
- Implemented automatic dialer app for Android and Sailfish OS – an easy and efficient way to trigger CSFB multiple times
- RRC and NAS signaling messages are collected during experiment session
- Signaling messages are further analyzed within our framework
- VoLTE is also included when possible
Signaling Trace Data Collection

- Either baseband manufacturer’s tool (e.g. QXDM) or third-party tool (e.g. Accuver XCAL, QualiPoc) is required
- Baseband manufacturer tools are normally only available to their customers
- Third-party tools could be bought by anyone
- Free software tools were limited when we started the research (Only xgoldmon, SnoopSnitch was available then)
- Why not develop one by ourself?

- We are mostly focusing on the RRC and NAS signaling messages (L3 and above)
- Lower L1 and L2 are out of scope for us
Parsing Qualcomm DIAG Data for LTE: Free Software Way

- QXDM and other commercial solution excluded here
- An article by Dieter Spaar on August 2013, although the code was not available then\(^1\)
- SnoopSnitch (2014): IMSI catcher detection rule focused on 2G/3G, but also LTE DIAG messages are partially parsed
- MobileInsight from researchers of UCLA and OSU (2015)\(^2\)
- diag-parser from moiji-mobile (2016)\(^3\)
- osmo-qcdiag from Osmocom (2017)\(^4\)

- When I started this, there were no affordable free software tools. Now there are several.

---

\(^1\) [http://www.mirider.com/weblog/2013/08/index.html](http://www.mirider.com/weblog/2013/08/index.html)

\(^2\) [http://mobileinsight.net/index.html](http://mobileinsight.net/index.html)

\(^3\) [https://github.com/moiji-mobile/diag-parser](https://github.com/moiji-mobile/diag-parser)

\(^4\) [http://cgit.osmocom.org/osmo-qcdiag/](http://cgit.osmocom.org/osmo-qcdiag/)
P1 Security (2013): LTE monitoring on Samsung LTE USB stick, earlier revision of Samsung Exynos Modem (aka Shannon, Kalmia, CMC2xx)\(^5\)

UI-based RAM dumps\(^6\) are still existing in S8, and the method is used as a quasi-official way on baseband debugging!

On smartphones, diagnostic interfaces are needed to be enabled via hidden menu

But there were no further free software tools for parsing RAM dumps or USB stream from smartphones

\(^5\)https://github.com/P1sec/LTE_monitor_c2xx

\(^6\)Recon 2016, Breaking Band: reverse engineering and exploiting the shannon baseband (Nico Golde, Daniel Komaromy)
Parsing Samsung Baseband Trace Stream

- Certain sequences are sent to enable the diagnostic streaming
- The overall frame structure hadn’t been largely changed from what P1 Security analyzed

<table>
<thead>
<tr>
<th>7f</th>
<th>15 00</th>
<th>00</th>
<th>12 00</th>
<th>50 ff</th>
<th>a0 02 52</th>
<th>9a fd 34 a4</th>
<th>04</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>03 00</td>
<td>34 02</td>
<td>20 00</td>
<td>7e 00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Leading 7f and trailing 7e (strangely no HDLC)
- Yellow 15 00 and 12 00: length of the entire stream. Don’t know why repeated twice.
- Red a0 02 52: command ID. We observed minor differences between baseband models.
- Pink 9a fd 34 a4: looping timestamp. Incremented 1 by 1 µs.
- Blue values: Depending on the command. Listed here is LTE RRC DL DCCH message, SecurityModeCommand.
Dissecting LTE in Wireshark

- Usage of GSMTAP is also extended to baseband monitoring tools
- Maintained in libosmocore and Wireshark has dissector for GSMTAP

- Decoding only RRC is not enough, since NAS is ciphered inside RRC
- Basebands are providing RRC, plain NAS, ciphered NAS message all separately
- LTE RRC definition was added by libosmocore commit b0a3c2f1 (Jun 2014), NAS by libosmocore commit f9b1e555 (Nov 2017)
- However it was not properly included in Wireshark GSMTAP dissector
  - Initial attempt was made in Jan 2015 as Change 6680 but eventually abandoned
  - LTE RRC parsing support was included by Wireshark commit 551309a6 (Jul 2017)
  - LTE NAS parsing support is still yet to be added (Nov 2017, Change 24554)
  - Decision on how to differentiate ciphered and plain NAS message is pending, this is the major showstopper at this moment
SCAT: Signaling Collection and Analysis Tool

- Tool for collecting signaling messages (SCATm)
- Framework for analyzing performance issues systematically (SCATA)

- Data collected from 13 countries, 33 operators
- Collected from November 2014 to present
- We focused on the following:
  - Why certain procedure takes longer time in some operator
  - Why certain optional procedure are implemented only by certain operator
  - Why failure occurs in some operator where other operators are fine
Dataset Overview

- Europe: Austria, Belgium, France, Germany, Iceland, Latvia, The Netherlands, Spain, Swiss, UK
- Asia: Japan, South Korea
- Americas: USA (Atlanta, AZ, Las Vegas, San Diego)
- Mostly used prepaid SIM cards for each countries
### Data Analysis Framework Overview

#### Phase 1. Time threshold
- RRC Connection
- Security Mode Setup
- 3G/LTE Attach
- Call Setup time
- MM (TAU/LAU etc.)
- 3G Detach time
- Operator I > Operator II
  - Operator I: $\varepsilon = 0.5$ (sec)
  - Operator II: $\varepsilon = 1$ (%) 
  - Normal Group
  - Suspect Group

#### Phase 2. Control flow sequence
- 3G Call Disconnect
- 3G MM Procedures
- 3G RRC Release
- LTE Attach
- 3G RRC Setup
- 3G MM Procedures
- 3G RRC Release
- LTE Attach

- Suspect Group = \{Operator I, Operator V\}
- Normal Group = \{Operator II, Operator III, Operator IV, ...\}

#### Phase 3. Signaling failure
- LAU Reject
- Radio Link Failure
- Service Reject
- Authentication Failure
- Random Access Failure
- TAU Reject
- Operator I > Operator II
  - Operator I: $\varepsilon = 1$ (%) 
  - Operator II: $\varepsilon = 0.5$ (sec)
  - Normal Group
  - Suspect Group

#### Decision Phase
- Is it a problem? Yes
  - Suspect Event $\in$ Problem Set
  - Cause Analysis

#### Phase 1
Time comparison by procedure

#### Phase 2
Comparison of signaling procedure sequence

#### Phase 3
Comparison of signaling failure occurrence probability
Data Analysis Framework

- **Time threshold-based detection**
  - Measuring time of each control procedure based on baseband/PC timestamp
  - Comparing time taken by procedure between each operators
  - Define a standard time range

- **Control sequence based detection**
  - Record control procedure sequence for the same high level action
  - Calculate probability of failure per action
  - Define a threshold per operator

- **Signaling failure based detection**
  - Calculate probability of failure per action
  - Compare between operators for each service
  - Find suspect group by outliers of each category
## Analysis Results

<table>
<thead>
<tr>
<th>Problem</th>
<th>Effects</th>
<th>Observed In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implicit Detach on LTE</td>
<td>Delayed LTE attach</td>
<td>2 operators</td>
</tr>
<tr>
<td>Inefficient RRC and NAS coordination</td>
<td>Delayed mobility procedure</td>
<td>5 operators</td>
</tr>
<tr>
<td>Incorrect LTE network specification</td>
<td>Unavailability of LTE</td>
<td>1 operator</td>
</tr>
<tr>
<td>Unnecessary mobility management procedure after CSFB call</td>
<td>Delayed 3G detach and LTE attach</td>
<td>4 operators</td>
</tr>
<tr>
<td>Security context sharing error</td>
<td>Delayed LTE attach</td>
<td>1 operator</td>
</tr>
<tr>
<td>Redundant AKA procedure</td>
<td>Delayed 3G attach</td>
<td>5 operators</td>
</tr>
<tr>
<td>Fallback to 2G during voice call even with good 3G availability</td>
<td>Degraded call performance</td>
<td>2 operators</td>
</tr>
<tr>
<td>Insufficient security</td>
<td></td>
<td>Several</td>
</tr>
</tbody>
</table>
Problem Overview

- We found following set of CSFB problems affecting network switch performance
- Additionally, security level provided by the network was also evaluated

- Time-related misconfiguration
  - MME handover and TA Update
  - RRC and NAS coordination (5 operators)

- Synchronization problem
  - Misconfigured cell reselection
  - Redundant location update (4 operators)

- Security issues
  - Security context sharing problem
  - Dropping to 2G?
  - Improper security algorithm (in year 2017!)
For one operator
- TAU failed with “Implicitly Detached” while moving back to 4G
- It took 10 seconds for re-attach

Possible cause: MME conflict
- UE is assigned to the different MME after TAU failure
- Serving MME might conflict for some error
- To recover MME conflict, MME configures Guard timer
- The guard timer might cause such a long delay to attach
Time Misconfiguration: RRC and NAS Coordination

- Timing mismatch between RRC and NAS can cause unnecessary delay
- Example: If a UE is about to move from 3G to LTE but 3G NAS procedure is remaining, one of the following is possible

1. \(3G\text{ RRC }\) Release \(\rightarrow\) LTE Attach
2. 3G MM Procedures \(\rightarrow\) 3G RRC Release \(\rightarrow\) LTE Attach
3. 3G RRC Release \(\rightarrow\) 3G RRC Connect \(\rightarrow\) 3G MM Procedures \(\rightarrow\) 3G RRC Release \(\rightarrow\) LTE Attach

- For case (3), additional delay between 0.5 – 1.5s had been observed for 5 operators
Following operator acquisition in Germany in 2014, they only allowed 3G roaming between each other but excluded 2G and 4G.

However, 3G SIB 19 of merged network included both network’s EARFCN.

As a result...

- Operator A user could successfully move from combined 3G to operator A’s LTE network.
- **Operator B user could not move from combined 3G to operator B’s LTE network!**

Operator B’s user could **stuck in 3G for up to 100 sec** if operator A’s LTE cell was selected to camp on.

Roaming status ended around 2016-2017 when two networks were finally consolidated.
Synchronization Problem: Redundant Location Update

- The standard allows operators to conduct 3G LAU in LTE TAU
- No need to do again when the UE falls back to 3G
- Two redundant updates (in stationary environment)
  - 3G LAU after the CSFB call before LTE attach
  - 3G LAU as soon as the UE falls back to 3G
Security Issues: Context Sharing

- Although 3G and LTE have different security contexts, the standard allows security context mapping between them.
- During LTE TAU, it is possible to use 3G-mapped security context ($KSI_{SGSN}$) or native one ($KSI_{ASME}$).
- LTE TAU with $KSI_{SGSN}$ always failed in one operator, causing 1.2-1.5 sec extra delay.
  - About 1/3 of total TAUs were failing.
- We assume that security context is not shared between each generation.
- Signaling traces of the same operator in 2017 imply that the problem had been addressed.
Security Issues: Repeated AKA Procedure

- How often AKA will be performed during CSFB in both 3G and LTE is up to operator implementation
  - Seldom (<10%): 7 operators
  - Frequently (20<x<90%): 3 operators
  - Always (100%): 3 operators
- Various factors can affect time for authentication
  - USIM card itself, baseband processor, others
  - Authentication time ranges between 10 ms to 500 ms
- Always performing authentication may lead to usage monitoring attack\(^7\)

Security Issues: Dropping to 2G?

- CSFB voice call sends user from LTE to 3G in most cases
- Sending explicitly from LTE to 2G is also possible, when there is no 3G coverage or 3G network is overloaded
- Two operators showed interesting pattern
  - Signaling messages were collected at the same place
  - Even though 3G was functional, the network sent the UE from 3G to 2G using HandoverFromUTRANCommand after call setup in 3G
  - Even worse, the operator in question used A5/1
- 2016: 4G → 3G → 2G → 4G
- 2017: 4G → 3G → 4G
Security Issues: Improper Security Algorithm

- Even though GSMMap was announced during 28C3\(^8\) some operators are still caring less on security
- 2G: A5/1 is still alive even in 2017
- LTE
  - If NAS is unciphered it still can be protected over-the-air by RRC ciphering
  - **RRC** should be ciphered unless emergency service, but some operators are applying **EEA0** as RRC encryption algorithm
- Operators might left network unciphered after testing, but both RRC and NAS should be ciphered as soon as possible

\(^8\)Karsten Nohl, Luca Melette. Defending mobile phones. 28C3 (2011)
Communicating With Operators

- We had a good relationship with some operators
  - Some provided us the rationale of configuration decision
  - Some addressed security problems more or less later
- Some operators did not replied to some of our findings
- Hope that they addressed the problem silently
Limitation

- Only end devices were monitored
- We don’t know what is really inside core network
  - Only a result of core network operation is visible as signaling messages by end device
  - Non-standardized, operator-specific operations
  - Interaction of multiple layers were hard to track
  - Operator’s SLA may different; this also includes operation timeouts
- Mobility was not considered during the experiment
  - Mobility management itself is another big topic
  - Systematically performing mobility related experiment is possible in not everywhere
  - Interaction with L1 and L2 is relatively harder than L3
Conclusion

- To diagnose network problems, studying a single network is not enough
  - Comparative measurement study with as much as possible data is required
  - Operators can implement different policies, implementation, optimization
  - By cross-checking data from multiple networks, we can gain a wider view on problem solving and performance optimization

- Operator awareness is also important to solve network problems
  - Not every network operation center is aware of the issues
  - We were well positioned to discuss the mentioned problems with network operators

- There are some remaining issues for opening up our dataset
  - Every patch needs to be merged in libosmocore/Wireshark
  - Privacy issues: which part of signaling messages should be anonymized? What kind of problem can arise when we build crowdsourced systems?

Title:
https://www.flickr.com/photos/88869697@N05/8533841120/in/photostream
https://imgflip.com/i/10ofaw
https://commons.wikimedia.org/wiki/File:S-Bahn-Ring_Berlin.svg
Qualcomm still plays the major role
MediaTek follows Qualcomm fiercely
Samsung and Hisilicon plays minor role as a vertically integrated player
Intel’s market shared collapsed, the only major user is Apple
xgoldmon won’t work on Intel XMM 7000 series (7160 and 7260 tested)
So where are tools supporting LTE?
Why not develop it by ourself?

---

9Global Information Inc., Baseband/Modem & Smartphones Market ‘17
Getting Into Samsung Baseband

- Recon 2016, Breaking Band: reverse engineering and exploiting the shannon baseband (Nico Golde, Daniel Komaromy)
- UI-based RAM dumps are still existing in S8, and the method is used as a quasi-official way on baseband debugging!
- The trace contains “full baseband↔apps IPC traces, including your seen networks, called numbers, etc”
- Diagnostics interfaces are also exposed as USB