GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier

Byeongdo Hong, Sangwook Bae, Yongdae Kim
KAIST SysSec
Feb. 19, 2018
**Paging Area in Cellular Network**

**Tracking Area**
(radius < 10 km)

**Paging:**
A method to find specific subscriber

**How?**
By using subscriber’s **identifier**
Paging: A method to find specific subscriber

How?

By using subscriber’s **identifier**
Paging Area in Cellular Network

**Tracking Area**
(radius < 10 km)

**Paging:**
A method to find specific subscriber

**How?**
By using subscriber’s **identifier**

**Paging Request**

**Paging Response**

Yongdae
Identifiers in Cellular Networks

- **Permanent/Unique identifier**
  - IMSI (International Mobile Subscriber Identity)
    - Provisioned in the SIM card

- **Temporary identifier**
  - Used to **hide** subscriber
    - TMSI (Temporary Mobile Subscriber Identity)
      - Used in 2G/3G
    - GUTI (Globally Unique Temporary Identity)
      - Used in LTE
Location Tracking in Cellular Network

Location Area 1

Victim Yongdae
TMSI: 0xDEADBEEF

User B
0xDEADBEEF

User C
0xDEADBEEF

Location Area 2

Attacker

0xDEADBEEF = Yongdae?

Kune et al. NDSS 2012
Location Tracking in Cellular Network

Temporary ID Issue:
Unchanged Identifier
GSM: NDSS’12, LTE: NDSS’16

Location Area 1

Location Area 2

Repeat dialing

Victim A
TMSI: 0xff123456

User B

Attacker

0xff123456 = A I found A!!

0xff123456

0xff123456

0xff123456

0xff123456

0xff123456
Phone number-Temporary ID mapping

- Traffic analysis to find the same TMSI (Kune et al. NDSS’12)
  - Find intersects of identifier’s sets

- Using “Silent Call”
  - Terminating call before ringing

- Same vulnerability in LTE - unchanged GUTI (Shaik et al. NDSS’16)
Defense of Location Tracking

- Temporary Identifier Reallocation
  - \textit{GUTI Reallocation} in LTE
  - To prevent between subscriber and ID mapping

Q. Is \textit{GUTI Reallocation} the solution to existing attacks?

A. It is Yes

But \textit{simply changing} is not a solution!
Experiment Setup

Device Analysis

Diagnostic Monitor

Signaling Collection and Analysis Tool (SCAT) [1]

Broadcast Channel Analysis

srsLTE (Open source)

USRP B210

Antenna

Broadcast Channel Receiver

# Worldwide Data Collection

<table>
<thead>
<tr>
<th>Country</th>
<th># of OP.</th>
<th># of USIM</th>
<th># of signalings</th>
<th>Country</th>
<th># of OP.</th>
<th># of USIM</th>
<th># of signalings</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.A</td>
<td>3</td>
<td>22</td>
<td>763K</td>
<td>U.K.</td>
<td>1</td>
<td>1</td>
<td>41K</td>
</tr>
<tr>
<td>Austria</td>
<td>3</td>
<td>3</td>
<td>807K</td>
<td>Spain</td>
<td>2</td>
<td>2</td>
<td>51K</td>
</tr>
<tr>
<td>Belgium</td>
<td>3</td>
<td>3</td>
<td>372K</td>
<td>Netherlands</td>
<td>3</td>
<td>3</td>
<td>946K</td>
</tr>
<tr>
<td>Switzerland</td>
<td>3</td>
<td>3</td>
<td>559K</td>
<td>Japan</td>
<td>1</td>
<td>2</td>
<td>37K</td>
</tr>
<tr>
<td>Germany</td>
<td>4</td>
<td>19</td>
<td>841K</td>
<td>South Korea</td>
<td>3</td>
<td>14</td>
<td>1.7M</td>
</tr>
<tr>
<td>France</td>
<td>2</td>
<td>6</td>
<td>305K</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Data summary**

Collection Period: **2014. 11. ~ 2017. 7.**

- # of countries: **11**
- # of operators: **28**
- # of USIMs: **78**
- # of voice calls: **58K**
- # of signalings: **6.4M**

※ OP: operator, USIM: Universal Subscriber Identity Module, Signaling: control plane message
Same vs. Fingerprintable IDs

NDSS’12, ‘16: Same ID $\Rightarrow$ Location Tracking!!

This work: ID Fingerprinting $\Rightarrow$ Location Tracking!!
### Fixed Bytes in GUTI Reallocation

- 19 operators have fixed bytes

<table>
<thead>
<tr>
<th>Allocation Pattern</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning the same GUTI</td>
<td>BE-III, DE-II, FR-II, JP-I</td>
</tr>
<tr>
<td>Three bytes fixed</td>
<td>CH-II, DE-III, NL-I, NL-II</td>
</tr>
<tr>
<td>Two bytes fixed</td>
<td>BE-II, CH-I, CH-III, ES-I, FR-I, NL-III</td>
</tr>
<tr>
<td>One bytes fixed</td>
<td>AT-I, AT-II, AT-III, BE-I, DE-I</td>
</tr>
</tbody>
</table>

AT: Austria, BE: Belgium, CH: Switzerland, DE: Germany, ES: Spain, FR: France, JP: Japan, NL: Netherlands
Case I: Netherlands (NL-I)

(a) 1st byte
(b) 2nd byte
(c) 3rd byte
(d) 4th byte

# of call
Case I: Netherlands (NL-I)
Case II: Belgium (BE-II)

(a) 1st byte

(b) 2nd byte

(c) 3rd byte

(d) 4th byte
Case II: Belgium (BE-II)

- Fixed Two Bytes
- Monotone Increasing

Hexadecimal value vs. # of call for the 1st and 2nd bytes:

(a) 1st byte
(b) 2nd byte
Fixed Bytes in *GUTI Reallocation*

- 19 operators have fixed bytes

<table>
<thead>
<tr>
<th>Allocation Pattern</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning the same GUTI</td>
<td>BE-III, DE-II, FR-II, JP-I</td>
</tr>
<tr>
<td>Three bytes fixed</td>
<td>CH-II, DE-III, NL-I, NL-II</td>
</tr>
<tr>
<td>Two bytes fixed</td>
<td>BE-II, CH-I, CH-III, ES-I, FR-I, NL-III</td>
</tr>
<tr>
<td>One bytes fixed</td>
<td>AT-I, AT-II, AT-III, BE-I, DE-I</td>
</tr>
</tbody>
</table>

AT: Austria, BE: Belgium, CH: Switzerland, DE: Germany, ES: Spain, FR: France, JP: Japan, NL: Netherlands
Stress Testing

- No noticeable rule of *GUTI Reallocation* for some operators

- Invoking voice call continuously with a short time
  - Two types of test
    - Weak stress testing
    - Hard stress testing
      - Calls at shorter intervals than weak stress test
Stress Testing Result

- Force the network to skip the *GUTI reallocation*
  - Perform experiments on US and Korean operators
    - Two US and two Korean operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Weak Stress Testing</th>
<th>Hard Stress Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>KR-I</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>KR-II</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>US-I</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>US-II</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

O: Reuse *GUTI*
X: No noticeable change
Success Rate of our Attack

- Required number of calls covering 99% success rate

![Graph showing the success rate of attacks on 1, 2, and 3 bytes fixed with different paging rates: 5 paging/sec, 88 paging/sec, and 160 paging/sec.](image)
Location Tracking with GUTI

- Observation of broadcast channels after call invocation
  - Pattern matching (fixed bytes, assigning same GUTI)
  - Location tracking (Tracking Area, Cell)

---

Extended Service Request:
- SecurityHeader: 0
- ServiceType: 1 (mobile terminating CS fallback or 1xCS fallback)
- NASKeySetId: 2
- MTMSI: Identity:
  - IdentityDigit:
    - 01: 200 = 0xC8
    - 02: 22 = 0x16
    - 03: 66 = 0x42
    - 04: 93 = 0x5D

---

EXTENDED SERVICE REQUEST:
- SecurityHeader: 0
- ServiceType: 1 (mobile terminating CS fallback or 1xCS fallback)
- NASKeySetId: 2
- MTMSI: Identity:
  - IdentityDigit:
    - 01: 200 = 0xC8
    - 02: 22 = 0x16
    - 03: 66 = 0x42
    - 04: 93 = 0x5D

---

OpenSignal (at KAIST)
Defenses + Requirements

- **Frequent refreshing** of temporary identifier
  - Per service request

- **Unpredictable** identity allocation
  - Cryptographically secure pseudorandom number generation
    - Hash_DRBG can be used

- Collision avoidance
- Stress-testing resistance
- Low cost implementation
Conclusion

- Predictable reallocation logic
  - GUTI reallocation pattern
    - Fixed bytes (19 operators)
  - Same GUTI
    - By stress test (4 test cases)
    - Assigning same GUTI

- Location tracking is still possible in cellular network!
- Secure GUTI reallocation mechanism is required
Thank you
BACK UP SLIDES
GUTI Format

- MCC (12bits)
- MNC (12bits)
- MMEGI (16bits)
- MMEC (8bits)
- M-TMSI (32bits)

S-TMSI
Dataset Release?

- Our dataset includes somewhat sensitive information.
  - Name of telcos ➔ Vulnerabilities can be linked to telcos.
  - Some IMSIs

- Not clear if releasing this dataset may cause any legal issues.

  - Finding performance bugs by comparative analysis of call flows

- Should we build open-source dataset using crowdsourcing?
  - May help customers to push telcos to build secure and better cellular network!
Stress Testing Result: US-I

(a) Normal GUTI Reallocation with CSFB call

(b) GUTI Reallocation and CSFB call Collision
\[ P_r(\bigcap_{i=1}^{N-1} A_i \neq \emptyset) = P_r(\bigvee_{a=0}^{2^{8k}-1} (a \in \bigcap_{i=1}^{N-1} A_i)) \leq \sum_{a=0}^{2^{8k}-1} P_r(a \in \bigcap_{i=1}^{N-1} A_i) = 2^{8k} P_r(a \in \bigcap_{i=1}^{N-1} A_i) \text{ for some } a = 2^{8k} \prod_{i=1}^{N-1} P_r(a \in A_i) \text{ for some } a = 2^{8k} \prod_{i=1}^{N-1} (1 - P_r(a \notin A_i)) \text{ for some } a = 2^{8k} \prod_{i=1}^{N-1} (1 - (\frac{2^{8k}-1}{2^{8k}})^t) \text{ for some } a = 2^{8k} (1 - (\frac{2^{8k}-1}{2^{8k}})^t)^{N-1} \]
Obtain target information (Phone number, carrier)

Perform GUTI Reallocation?
Attack Flow

Perform GUTI Reallocation?

Yes

No

Find the target
(MME area, Tracking area, Cell)

Analysis of rules for ID reallocation

OpenSigna

Google Maps API
Attack Flow

- Analysis of rules for ID reallocation
  - Have fixed bytes?
    - Yes → Find the target (MME area, Tracking area, Cell)
    - No → Stress test

Tools:
- OpenSigna
- Google Maps API
Paging Distribution in Korea (KR-I)

Max: 88 pagings / sec

Min: 5 pagings / sec