Ghost Telephonist

Link Hijack Exploitations in 4G LTE CS Fallback

Yuwei ZHENG, Lin HUANG, Qing YANG, Haoqi SHAN, Jun LI

UnicornTeam, 360 Technology
July 27, 2017
Who We Are?

• 360 Technology is a leading Internet security company in China. Our core products are anti-virus security software on PC and cellphones.

• UnicornTeam (https://unicorn.360.com/) was founded in 2014. This is a team that focuses on the security issues in many kinds of telecommunication systems.

• Highlighted works of UnicornTeam include:
  • Low-cost GPS spoofing research (DEFCON 23)
  • LTE redirection attack (DEFCON 24)
  • Attack on power line communication (BlackHat USA 2016)
• Demo video
• A story about this vulnerability
• Hijack random target
• The principle of this vulnerability
• Advanced exploitation (targeted attack)
• Attack internet accounts
• Countermeasures
A flower does not grow sometimes when you purposely plant it whereas a willow grows and offers a shade sometimes when you purposelessly transplant it.

When we used OsmocomBB as cellphone to access GSM network, we met a difficulty. During debugging the problem, we occasionally found a fake paging response can build the connection to network.
Hijack random target
Experiment Setting

C118
OsmocomBB L1

OsmocomBB L2/3
Random Attack Steps

Attack Steps

• 1) Listen on PCH channel
• 2) Extract TMSI/IMSI in paging
• 3) Forging a paging response with the TMSI/IMSI
• 4) Check whether MSC accepts the paging response
Hijack Result

• C118 has no SIM card.
• C118 successfully hijacked one call from 139****920.
What can attacker do in further?

• If attacker answers the incoming call
  • The caller will recognize the callee’s voice is abnormal.

• What does attacker know now
  • Victim’s TMSI or IMSI
  • Caller’s phone number
Get Victim’s Phone Number

• During an ongoing call, sending ‘CM Service Request’ does not trigger authentication, and the network will directly response a ‘CM Service Accept’.

• So attacker can make a call to another in-hand phone to know the victim’s ISDN number.
Get Victim’s Phone Number

Attack Signaling Flow

1) Send ‘hold’
2) Send ‘CM Service Request’
PCAP Records

Here are the records captured by Wireshark on the laptop that Osmocom is running on.

It confirmed that attackers can build a MO call connection with the network.
Why do some attacks succeed, but some not?

• Until now, our vision keeps in the 2G field…from the view of OsmocomBB.

• Is it introduced by the vulnerable GSM network?

• NO. We found if we set cellphone to be ‘2G-only’. Every call requires authentication.
Normal 2G Call vs. CSFB Call

In normal 2G call, Authentication does exist for every call.

When we analyze the signaling flow of CSFB, we were surprised to find that there is no authentication step.
Voice Solutions in LTE Network

• VoLTE
  • Voice over LTE, based on IP Multimedia Subsystem (IMS)
  • Final target of network evolution

• CSFB
  • Circuit Switched Fallback: switch from 4G to 3G or 2G when taking voice call

• SV-LTE
  • Simultaneous Voice and LTE
  • Higher price and rapid power consumption on terminal
• Combined attach / Combined Track area update
Vulnerability in CSFB

Signaling flow of CSFB MT call
• The principle is like someone comes out from the door of LTE, then enters the door of GSM. He shouts, ‘I must be as quick as possible!’ Then he is permitted to enter, without the badge of GSM.
• Basic idea
  • Because CSFB has no authentication procedure, attackers can send Paging Response on 2G network, impersonating the victim, thus hijack the call link.
The Ghost Telephonist gets control from here.
Why Network Sends Paging on 2G

• Cellphone stays in 4G
  • Network sends paging message in 4G LTE PCH. But this paging message uses 4G’s S-TMSI, not 2G’s TMSI.
  • S-TMSI and TMSI are generated during combined attach or location update procedure.

• C118 really hear paging messages
  • In some cases, network sends paging message both on 4G and 2G.
  • So using the TMSI captured on 2G can response the CSFB call on 4G.
  • Usually the network sends TMSIs, but sometimes it sends IMSI.
Targeted Persistent Attack

• Previous discussion is about random attack. Here we introduce targeted persistent attack to hijack the victim’s link.

• Use TMSI
  • Once attacker knows one TMSI, he can persistently send Paging Response with this TMSI, no matter whether there is paging coming.

• Use IMSI
  • If attacker knows one victim’s IMSI and know where he is, the attacker can go to the same paging area, and continuously send paging response with the IMSI to hijack the victim’s link.

• Use ISDN number
  • If the attacker knows victim’s phone number, the attacker can firstly call the victim then capture the TMSI of the victim. After that, use TMSI to launch the attack.
Attack with TMSI

• Condition
  • Attacker knows victim’s TMSI

• Attack Steps
  • 1) Persistently sending Paging Response with this TMSI
  • 2) Once victim has a Paging procedure existing, attacker can quickly control the link.
Attack with IMSI

- **Condition**
  - Attacker knows victim’s IMSI

- **Attack Steps**
  - 1) Persistently sending Paging Response with this IMSI
  - 2) Once victim has a Paging procedure existing, attacker can control the link.

- **Disadvantage**
  - When network side receives Paging Response with IMSI, it has to find out the corresponding TMSI, so this method will increase the link building latency then consequently results in low ratio of successful attack.
**Condition**
- Attacker knows victim’s ISDN number

**Attack Steps**
1) Make a call to victim with an anonymous cellphone, to trigger a CSFB; Use one C118 to sniff TMSI
2) Use another C118 to continuously send Paging Response with the TMSI and use anonymous cellphone to make second call to trigger CSFB again.
3) Hijack and hold the victim’s link.
• The victim cellphone keeps online in 4G network and doesn’t sense the attack.

• Attacker only needs fake 2G UE and doesn’t need fake 4G base station.
Different Cellphone Behaviors

- We found some cellphones are easily hijacked but some are not.

<table>
<thead>
<tr>
<th>Victim Cellphone</th>
<th>Chipset</th>
<th>Chipset Vendor</th>
<th>Fake Callee</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>msm8992</td>
<td>Qualcomm</td>
<td>✓</td>
</tr>
<tr>
<td>B</td>
<td>msm8994</td>
<td>Qualcomm</td>
<td>✓</td>
</tr>
<tr>
<td>C</td>
<td>mdm9615m</td>
<td>Qualcomm</td>
<td>✓*</td>
</tr>
<tr>
<td>D</td>
<td>mdm9625m</td>
<td>Qualcomm</td>
<td>✓*</td>
</tr>
<tr>
<td>E</td>
<td>mdm9635m</td>
<td>Qualcomm</td>
<td>✓</td>
</tr>
<tr>
<td>F</td>
<td>mt6753</td>
<td>MTK</td>
<td>✓*</td>
</tr>
<tr>
<td>G</td>
<td>kirin960</td>
<td>Hisilicon</td>
<td>✓*</td>
</tr>
</tbody>
</table>

[*] means jamming is needed in the attack.

Cellphones with [*] have better defense against this attack. Jamming is needed to cut off the connection between victim cellphones and the network.
Failure Analysis

• What ‘successful hijack’ means
  • After the attacker sends Paging Response, he receives the call. This means a successful hijack.

• Whether can hold the link
  • When the attacker receives the call, the call may be interrupted after a short time.
  • The reason is: the victim cellphone didn’t receive the call and it wants to ‘Fast Return’ back to 4G, so it will launch a Location Area Update procedure in 2G. This LAU results in the break of attacker’s link.
Failure Analysis

Fast Return Case 1 – Cellphone A, Qualcomm Chipset

Paging Response failure
Location Update not completed

<table>
<thead>
<tr>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCCH / Paging</td>
<td></td>
</tr>
<tr>
<td>LTE NAS EMM Plain OTA OUTGOING Message</td>
<td>Radio Bearer ID: 0, Freq: 39148, SFN: 224</td>
</tr>
<tr>
<td>UL_CCCH / RRCConnectionRequest</td>
<td>Radio Bearer ID: 0, Freq: 39148, SFN: 352</td>
</tr>
<tr>
<td>DL_CCCH / RRCConnectionSetup</td>
<td>Extended service request Msg</td>
</tr>
<tr>
<td>UL_DCCH / RRCConnectionSetupComplete</td>
<td>Radio Bearer ID: 0, Freq: 39148, SFN: 0</td>
</tr>
<tr>
<td>DL_DCCH / securityModecommand</td>
<td>Radio Bearer ID: 0, Freq: 39148, SFN: 359</td>
</tr>
<tr>
<td>UL_DCCH / SecurityModeComplete</td>
<td>Radio Bearer ID: 1, Freq: 39148, SFN: 0</td>
</tr>
<tr>
<td>DL_DCCH / RRCConnectionReconfiguration</td>
<td>Radio Bearer ID: 1, Freq: 39148, SFN: 362</td>
</tr>
<tr>
<td>UL_DCCH / RRCConnectionReconfigurationComplete</td>
<td>Radio Bearer ID: 1, Freq: 39148, SFN: 0</td>
</tr>
<tr>
<td>RR/Paging Response</td>
<td>Radio Bearer ID: 1, Freq: 39148, SFN: 0</td>
</tr>
<tr>
<td>MM/Location Update Request</td>
<td>Radio Bearer ID: 1, Freq: 39148, SFN: 0</td>
</tr>
<tr>
<td>LTE NAS EMM Plain OTA OUTGOING Message</td>
<td>Radio Bearer ID: 1, Freq: 39148, SFN: 371</td>
</tr>
<tr>
<td>Tracking area update request Msg</td>
<td>Direction: MS To NetworkLength: 13</td>
</tr>
<tr>
<td>Tracking area update accept Msg</td>
<td>Length: 0022</td>
</tr>
<tr>
<td>Tracking area update complete Msg</td>
<td>Direction: MS To NetworkLength: 15</td>
</tr>
</tbody>
</table>
Failure Analysis

Fast Return Case 2 – Cellphone F, MTK Chipset

Paging Response failure

Location Update completed
Supplemented by Jamming

• Break victim’s LAU
  • If the attacker sends jamming signal to the victim, this will break the link between victim and network, so that the attacker can keep holding the fake link.
  • This will increase the success ratio of the attack.
  • Disadvantage is the victim may sense the attack.
Attacking Internet Accounts

- **Login with verification SMS**
  - Some applications permit login with cellphone number + verification SMS. Don’t require inputting password.

- **Reset login password with verification SMS**
  - A lot of Internet application accounts use verification SMS to reset the login password. Attacker can use the cellphone number to start a password reset procedure then hijack the verification SMS.
Attack Steps

1. Get phone number
2. Reset password request with phone number
3. Receive authentication SMS
4. Reset password according to SMS
C118 Log shows it received the SMS sent from Facebook to the victim.
• We investigated the password reset routine of many popular websites and applications, including global and Chinese ones, for example SNS website, payment website, and IM App etc.

<table>
<thead>
<tr>
<th>Website/App</th>
<th>Inbound or Outbound SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>Inbound</td>
</tr>
<tr>
<td>Google account</td>
<td>Inbound</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>Inbound</td>
</tr>
<tr>
<td>Alipay (Chinese PayPal)</td>
<td>Inbound</td>
</tr>
<tr>
<td>WeChat (Chinese WhatsApp)</td>
<td>Outbound</td>
</tr>
<tr>
<td>DiDi (Chinese Uber)</td>
<td>Inbound</td>
</tr>
<tr>
<td>Sina Weibo (Chinese Twitter)</td>
<td>Outbound</td>
</tr>
</tbody>
</table>
• Telephonist and the victim should be in the same paging area (several base stations’ coverage)
• The attack is feasible only when 2G network is in use and uses A5/1 or A5/0 encryption.

• Telephonist attack doesn’t need to access SS7 core network.
• Telephonist attack doesn’t need fake base station.
• The victim keeps online in 4G network and is not aware of the attack.
Countermeasures

• To operators
  • Enable authentication in the CSFB procedure. The added latency is acceptable.
  • Speed up VoLTE service deployment

• To Internet service provider
  • Pay attention to that the PSTN authentication is not safe.
  • The password reset procedure should be improved by additional personal information check.
• What’s CVD Program?
  • CVD, Coordinated Vulnerability Disclosure Programme
  • ‘Disclosures to GSMA must focus on open standards based technologies which are not proprietary to a specific vendor but that are used across, or have significant impact on, the mobile industry (e.g. including but not limited to protocols specified by IETF, ITU, ISO, ETSI, 3GPP, GSMA etc.)’

Good platform for reporting standard based vulnerability.
GSMA CVD Program

• UnicornTeam received the FIRST acknowledgement on the Mobile Security Research Hall of Fame.

• GSMA forwarded the vulnerability information to every operators.

• Now related operators are fixing or already fixed this vulnerability.
Thank You ~