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 built in 2014. This is a group 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)

Agenda

- Demo video
- A story about this vulnerability
- Hijack random target
- The principle of this vulnerability
- Advanced exploitation
- Attack internet accounts
- Countermeasures

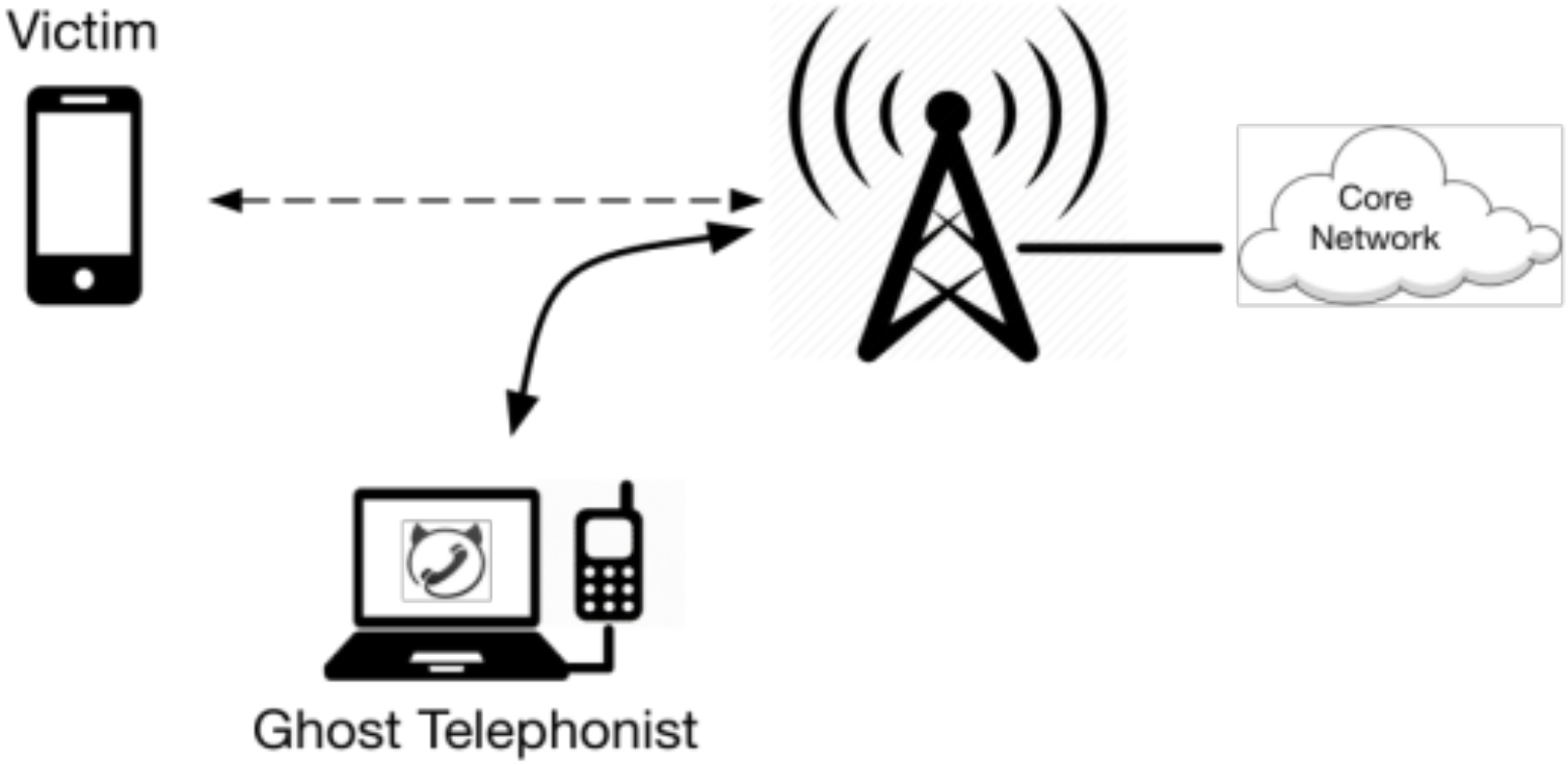
Demo Video

A story about this vulnerability

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



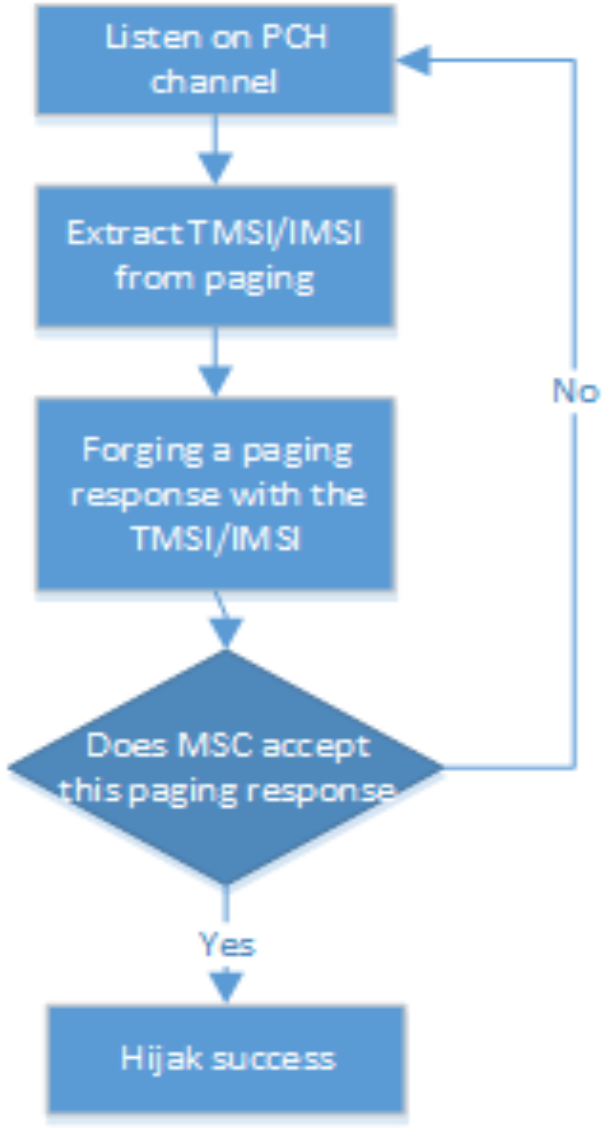
Hijack random target

Experiment Environment

Hijack random target

Attack Steps

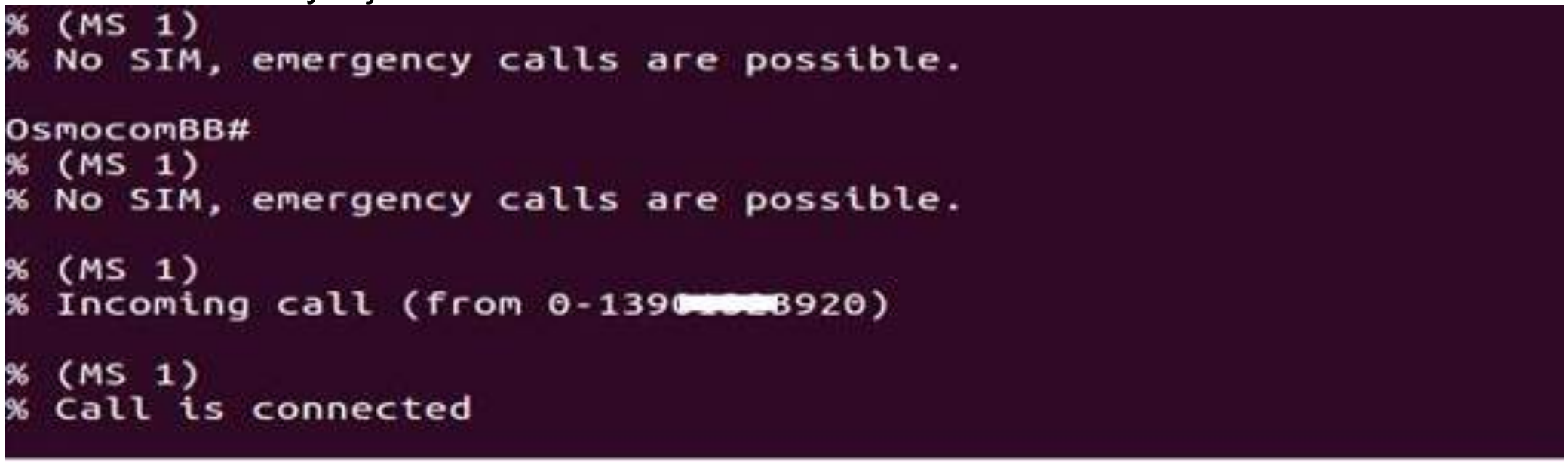
- 1) Listen on PCH channel
- 2) Extract TMSI/IMSI in paging
- 3) Forging a paging response with the TMSI/IMSI
- 4) Check whether MSC accepts the paging response



Hijack random target

Hijack Result

- C118 has no SIM card.
- C118 successfully hijacked one call from 139*****920.



Hijack random target

What can attacker do in further?

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

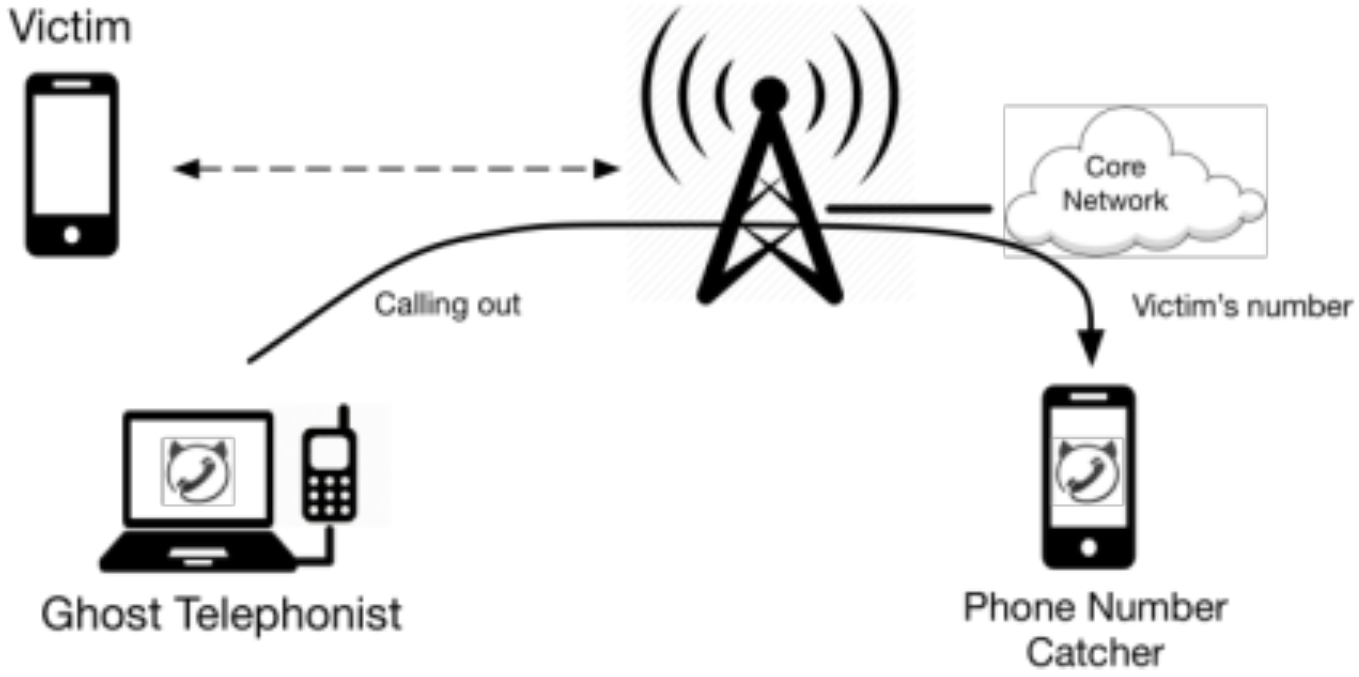
- What does attacker know now
  - Victim's TMSI or IMSI
  - Caller's phone number

Hijack random target

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'.

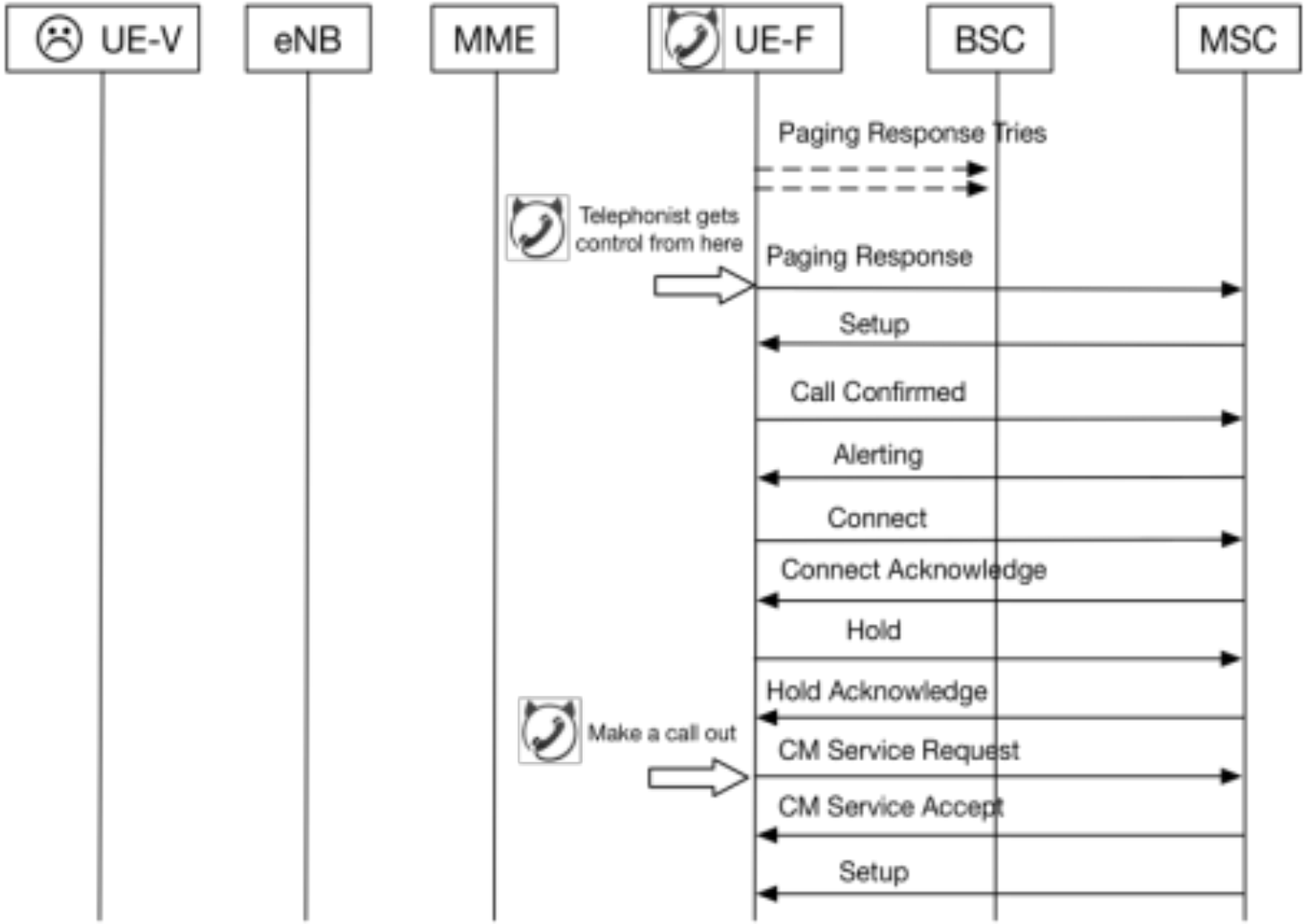
- So attacker can make a call to another in-hand phone to know the victim's ISDN number.



Get Victim's Phone Number

Attack Signaling Flow

- 1) Send 'hold'
- 2) Send 'CM Service Request'



Get Victim's Phone Number

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.

```
LAPDm     81 U P, func=SABM(DTAP) (RR) Paging Response
LAPDm     81 I, N(R)=0, N(S)=0(DTAP) (CC) Setup
LAPDm     81 I, N(R)=1, N(S)=0(DTAP) (CC) Call Confirmed
LAPDm     81 I, N(R)=1, N(S)=1(DTAP) (CC) Alerting
LAPDm     81 I, N(R)=2, N(S)=2(DTAP) (CC) Connect
LAPDm     81 I, N(R)=1, N(S)=0(DTAP) (CC) Connect Acknowledge
LAPDm     81 I, N(R)=1, N(S)=1(DTAP) (CC) Hold
LAPDm     81 I, N(R)=2, N(S)=1(DTAP) (CC) Hold Acknowledge
LAPDm     81 I, N(R)=2, N(S)=2(DTAP) (MM) CM Service Request
LAPDm     81 I, N(R)=3, N(S)=2(DTAP) (MM) CM Service Accept
LAPDm     81 I, N(R)=3, N(S)=3(DTAP) (CC) Setup
LAPDm     81 I, N(R)=4, N(S)=3(DTAP) (CC) Call Proceeding
LAPDm     81 I, N(R)=4, N(S)=5(DTAP) (CC) Alerting
LAPDm     81 I, N(R)=4, N(S)=6(DTAP) (CC) Connect
LAPDm     81 I, N(R)=7, N(S)=4(DTAP) (CC) Connect Acknowledge
LAPDm     81 I, N(R)=5, N(S)=7(DTAP) (CC) Disconnect
LAPDm     81 I, N(R)=0, N(S)=5(DTAP) (CC) Release
LAPDm     81 I, N(R)=6, N(S)=0(DTAP) (CC) Release Complete
LAPDm     81 I, N(R)=0, N(S)=3(DTAP) (CC) Disconnect
LAPDm     81 I, N(R)=4, N(S)=0(DTAP) (CC) Release
LAPDm     81 I, N(R)=1, N(S)=4(DTAP) (CC) Release Complete
LAPDm     81 I, N(R)=1, N(S)=5(DTAP) (RR) Channel Release
```

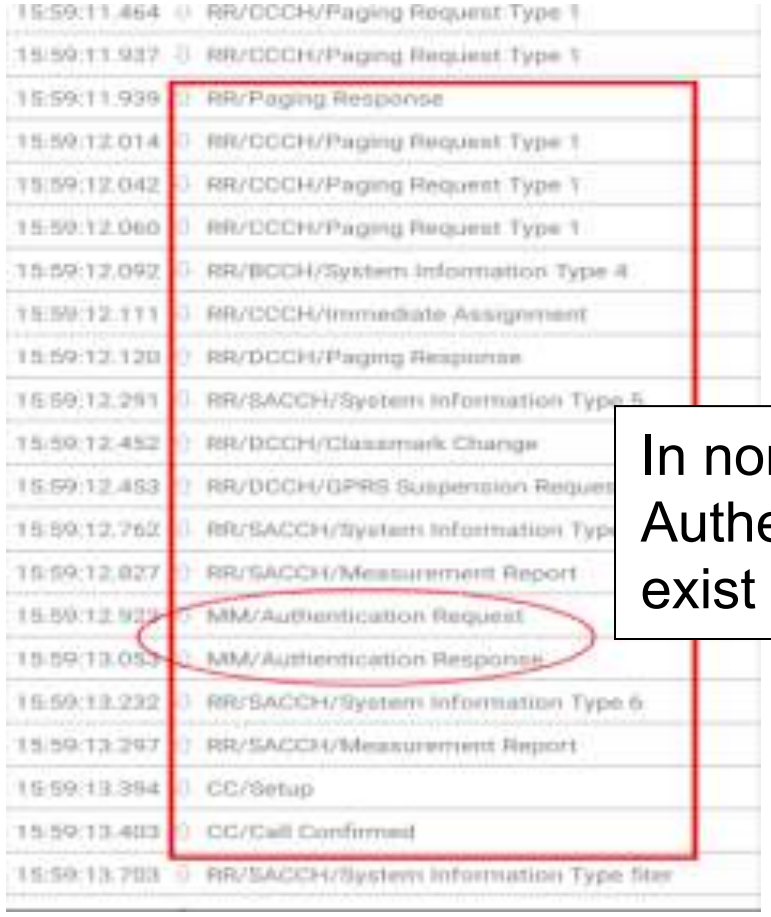
Hijack random target

Success Rate

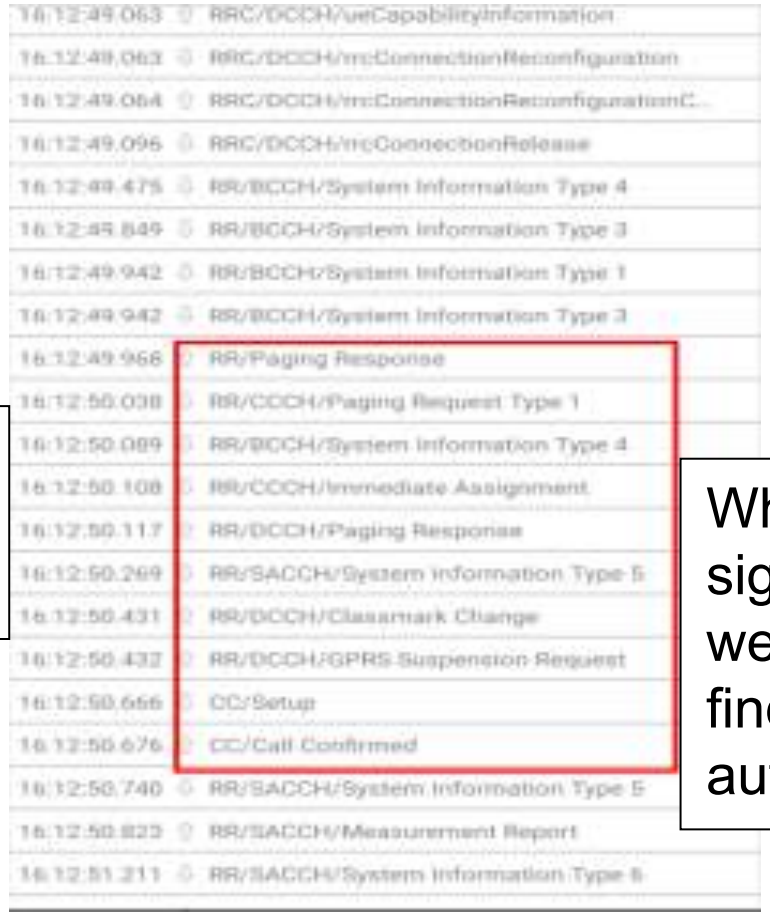
- Random attack success ratio is not high
  - If the victim sends Paging Response earlier than the attacker, the attack will fail.

The principle of CSFB vulnerability

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.

The principle of CSFB vulnerability

Voice Solutions in LTE Network

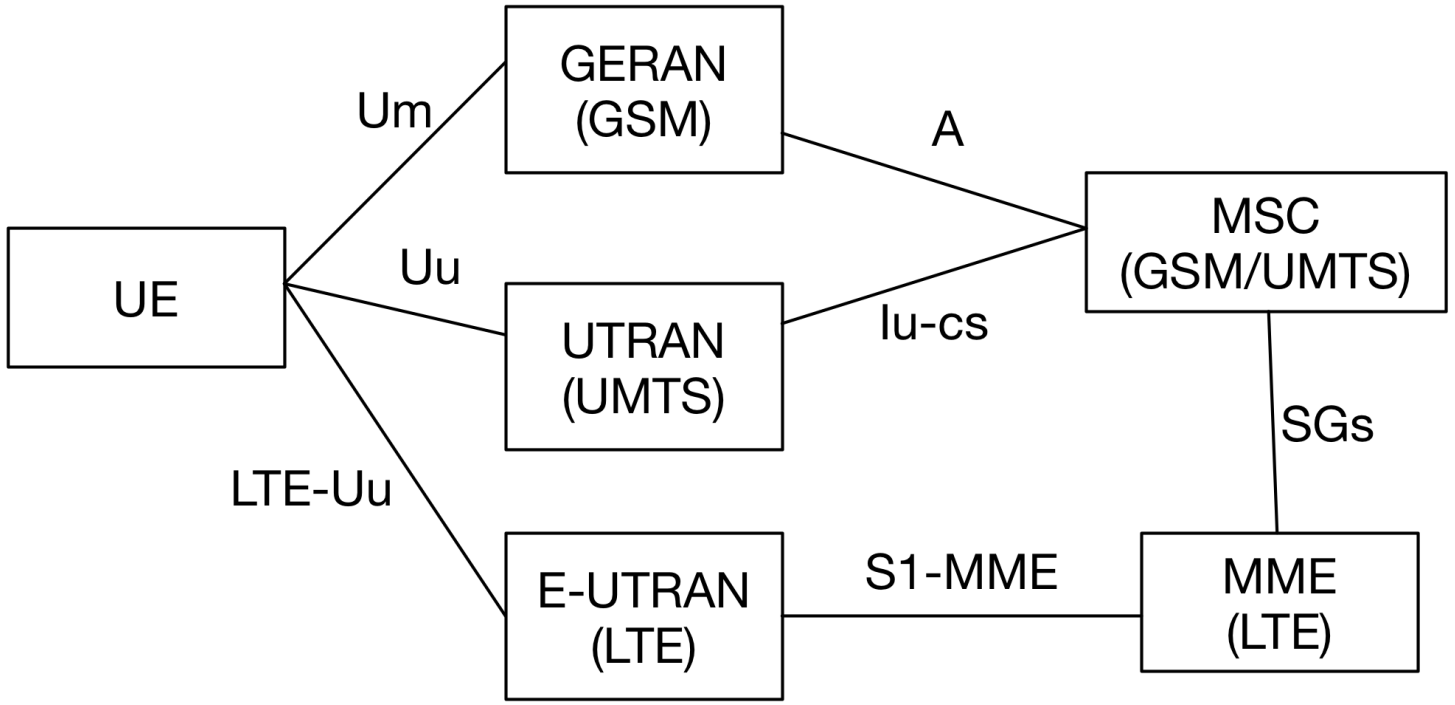
- VoLTE
  - Voice over LTE, based on IP Multimedia Subsystem (IMS)
  - Final target of network evolution

- 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

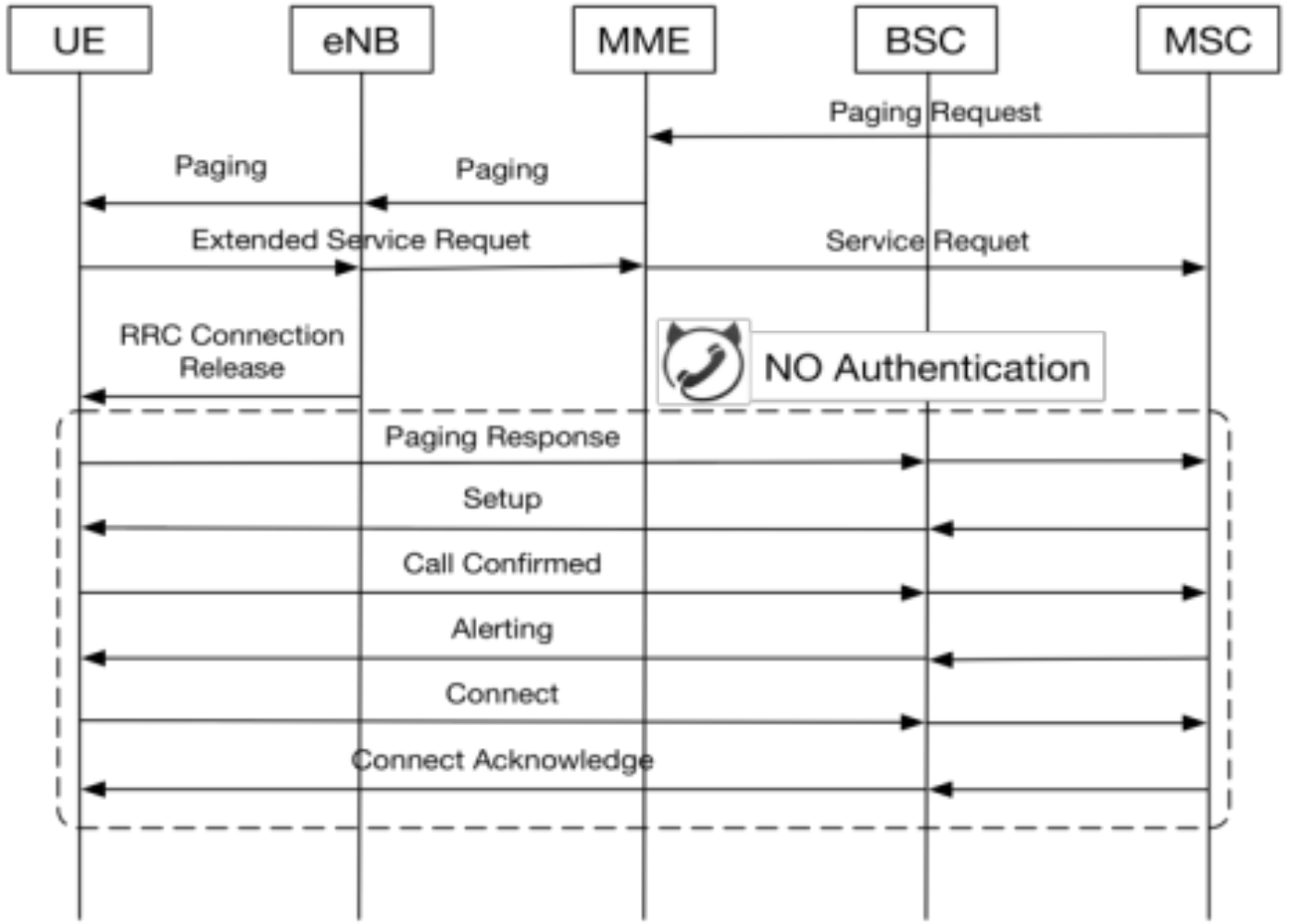
The principle of CSFB vulnerability

- Combined attach / Combined Track area update

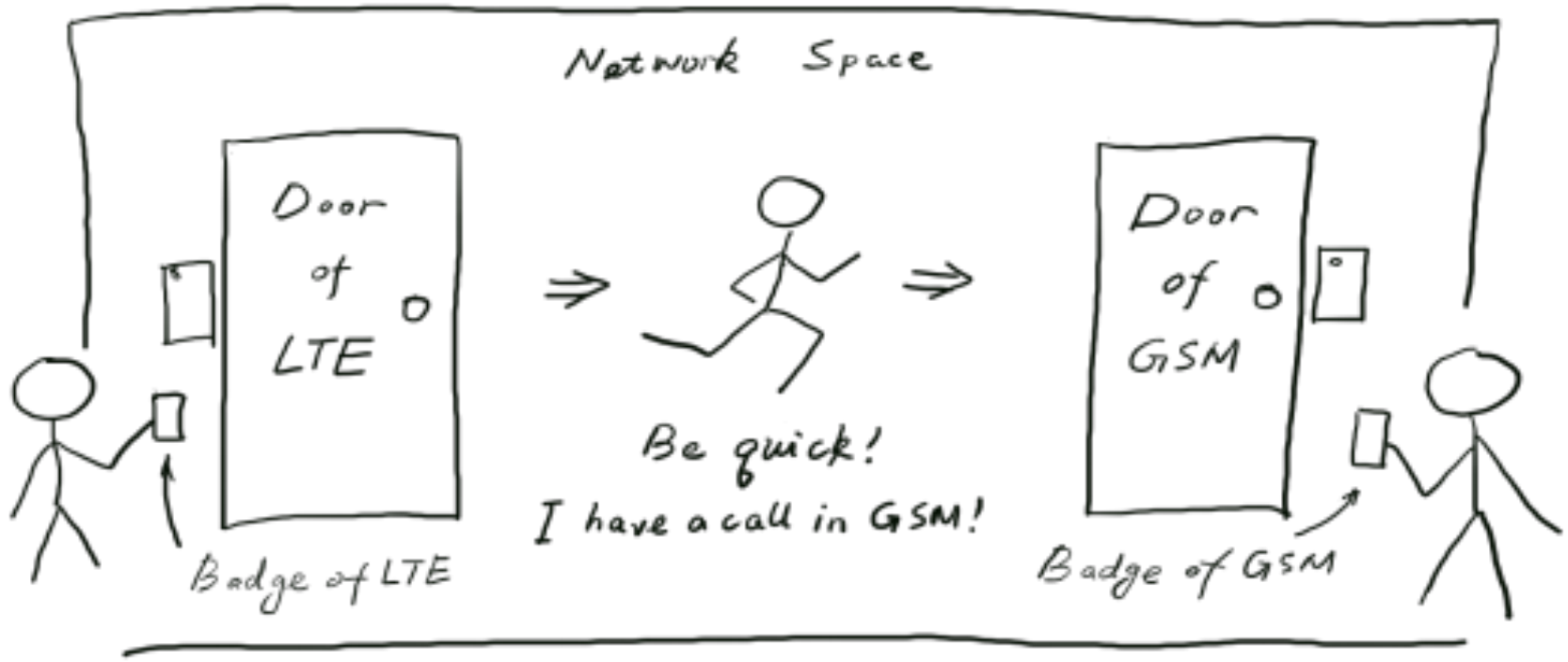


Vulnerability in CSFB

Signaling flow of CSFB MT call



Vulnerability in CSFB



- 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.

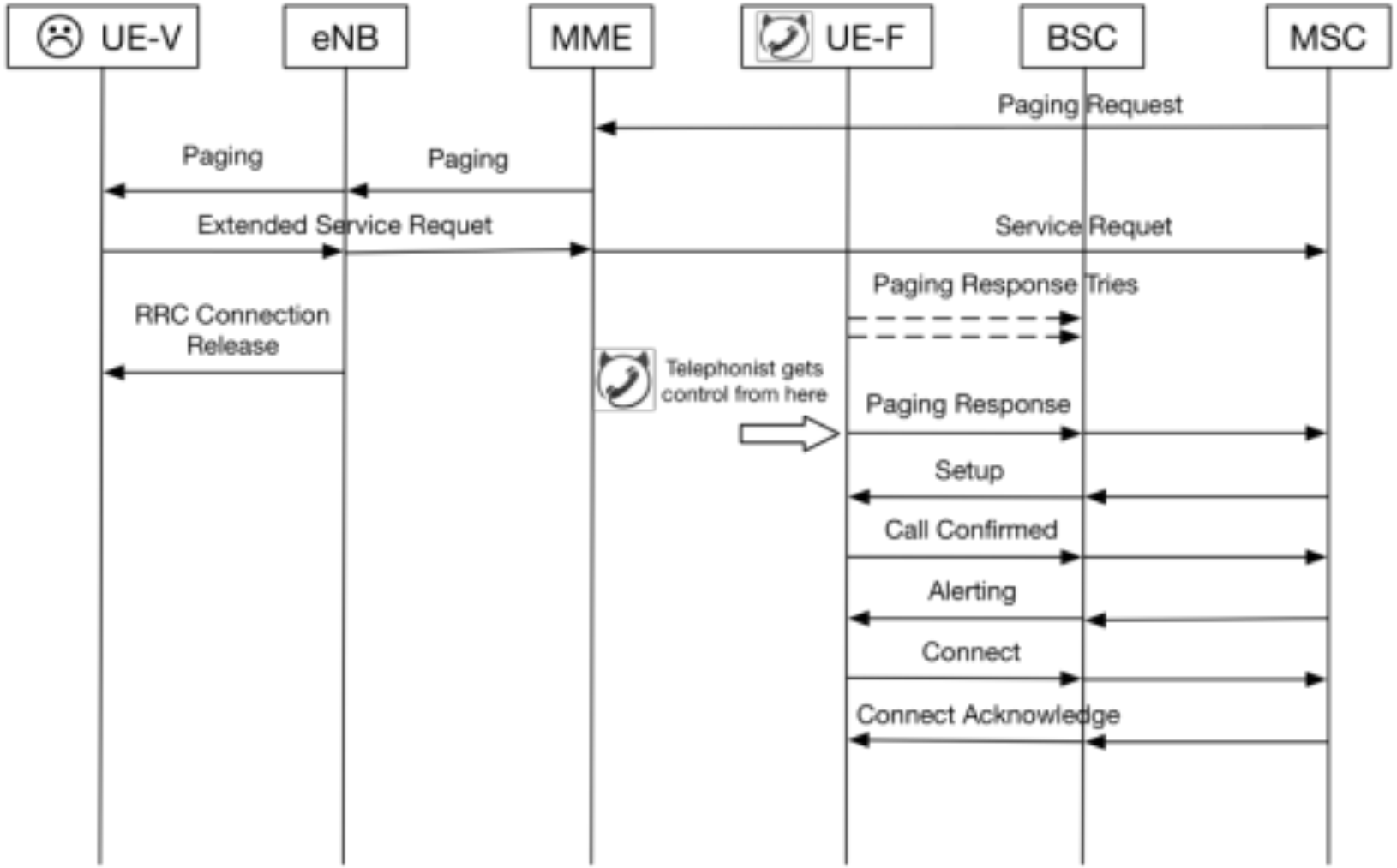
Vulnerability in CSFB

- Basic idea
  - Because CSFB hasn’t authentication procedure, attackers can send Paging Response on 2G network, impersonating the victim, then hijack the call link.

Vulnerability in CSFB

Attack Signaling Flow

The Ghost Telephonist gets control from here.



Vulnerability in CSFB

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.

Advanced exploitation

Targeted Persistent Attack

- Former discussion is about randomly 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.

Advanced exploitation

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.

Advanced exploitation

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.

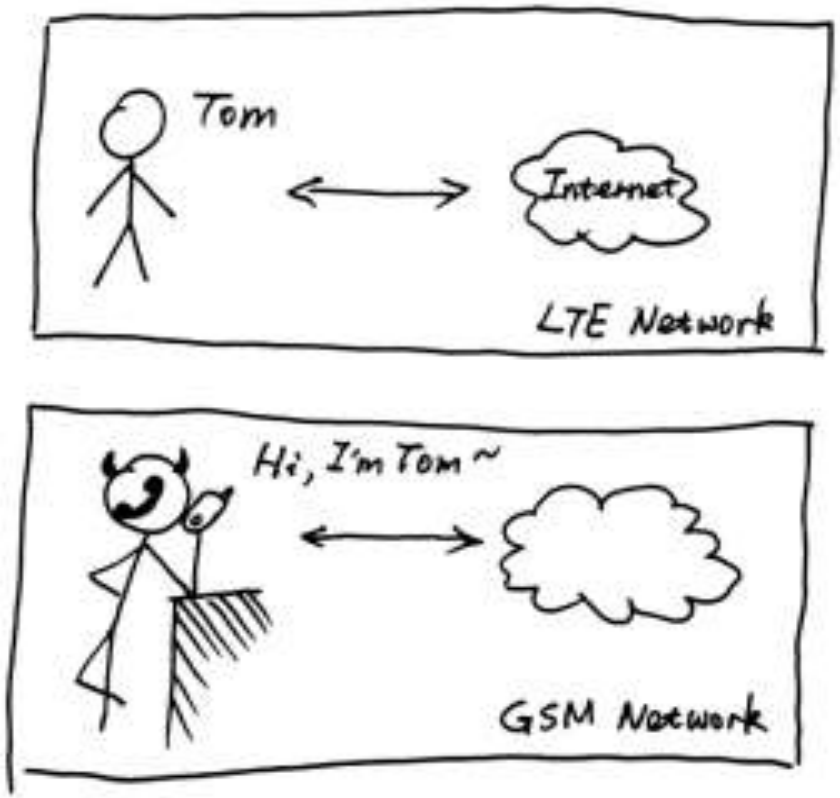
Advanced exploitation

Attack with phone number

- 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.

Advanced exploitation

- 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.



Advanced exploitation

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

Victim Cellphone	Chipset	Chipset Vendor	Fake Callee
Xiaomi Mi4c	msm8992	Qualcomm	√
Nubia Z9 max	msm8994	Qualcomm	√
iPhone 5s	mdm9615m	Qualcomm	√*
iPhone 6	mdm9625m	Qualcomm	√*
iPhone 6s	mdm9635m	Qualcomm	√
Qiku	mt6753	MTK	√*
Huawei P9	kirin960	Hisilicon	√*

[*] in this 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.

Advanced exploitation

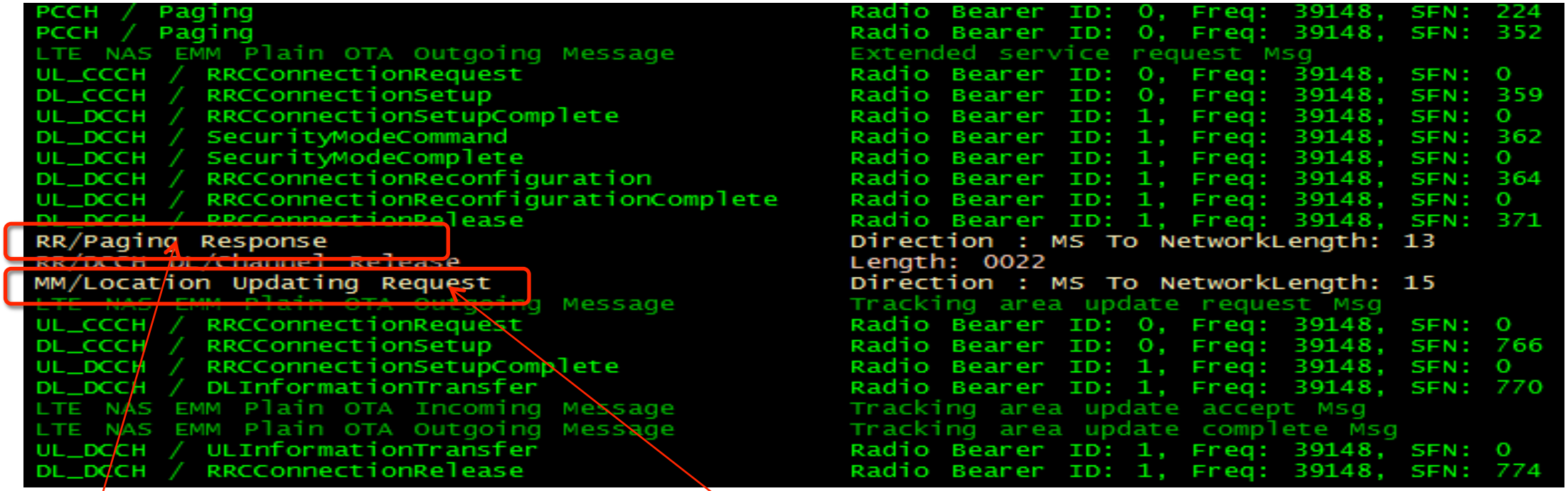
Failure Analysis

- 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 – Mi4C Cellphone,Qualcomm Chipset



Paging Response failure

Location Update not completed

Failure Analysis

Fast Return Case 2 – Qiku Cellphone, MTK Chipset

```
[NW->MS] ERRC_DLInformationTransfer
[NW->MS] EMM_CS_Service_Notification(paging identity="TMSI_PAGING_TYPE")
[MS->NW] EMM_Extended_Service_Request(service type="MT_CSFB", CSFB response="CSFB_ACCEPTED_BY_UE")
[MS->NW] ERRC_ULInformationTransfer
[NW->MS] ERRC_RRCConnectionRelease(cause:[ReleaseCause_other], redirectInfo:[1])
[MS->NW] RR__PAGING_RESPONSE
[NW->MS] RR__CHANNEL_RELEASE
[MS->NW] MM__LOCATION_UPDATING_REQUEST (LU type: MM_NORMAL_LU)
[NW->MS] MM__LOCATION_UPDATING_ACCEPT
[MS->NW] ERRC_RRCConnectionRequest
[NW->MS] ERRC_RRCConnectionSetup
[MS->NW] EMM_Tracking_Area_Update_Request(EPS update type="EMM_UPDATE_TYPE_COMBINED_TAU_IMSI_ATTACH", active flag="KAL_FALSE")
[MS->NW] ERRC_RRCConnectionSetupComplete
[NW->MS] ERRC_DLInformationTransfer
[NW->MS] EMM_Authentication_Request
[MS->NW] EMM_Authentication_Response
[MS->NW] ERRC_ULInformationTransfer
[NW->MS] ERRC_DLInformationTransfer
[NW->MS] EMM_Security_Mode_Command(integrity algorithm="INT_128_EIA2", ciphering algorithm="ENC_EEA0")
[MS->NW] EMM_Security_Mode_Complete
[MS->NW] ERRC_ULInformationTransfer
[NW->MS] ERRC_RRCConnectionReconfiguration(measCfg:[0],mobCtrlInfo:[0],dedInfoNASList:[1],radioresCfgDed:[1],secCfgHO:[0])
[MS->NW] ERRC_RRCConnectionReconfigurationComplete
[NW->MS] EMM_Tracking_Area_Update_Accept(EPS update result="EMM_UPDATE_RESULT_COMBINED_UPDATED")
[MS->NW] EMM_Tracking_Area_Update_Complete
[MS->NW] ERRC_ULInformationTransfer
```

Paging Response failure

Location Update completed

Advanced exploitation

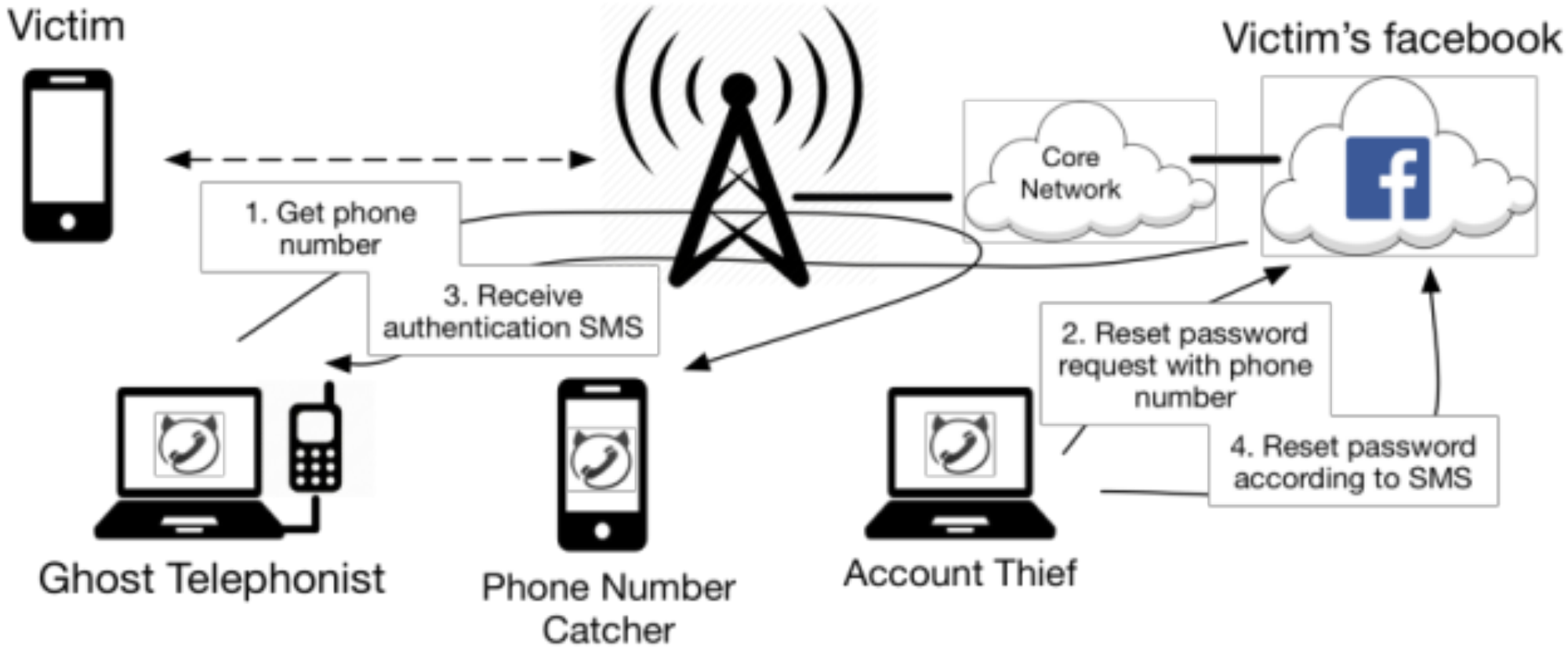
Improve success rate

- 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.

Attack Internet Account

- Login with verification SMS
  - Some applications permits 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 Internet Account



Attack Internet Account

- C118 Log shows it received the SMS sent from Facebook to the victim

Protocol	Length	Info
LAPDm	81	U P, func=SABM(DTAP) (RR) Paging Response
LAPDm	81	U F, func=UA(DTAP) (RR) Paging Response
LAPDm	81	I, N(R)=0, N(S)=0(DTAP) (CC) Setup
LAPDm	81	I, N(R)=1, N(S)=0(DTAP) (CC) Call Confirmed
LAPDm	81	I, N(R)=1, N(S)=1(DTAP) (CC) Alerting
LAPDm	81	I, N(R)=2, N(S)=2(DTAP) (CC) Connect
LAPDm	81	I, N(R)=1, N(S)=0(DTAP) (CC) Connect Acknowledge
LAPDm	81	I, N(R)=1, N(S)=1(DTAP) (CC) Hold
LAPDm	81	I, N(R)=2, N(S)=1(DTAP) (CC) Hold Acknowledge
LAPDm	81	I, N(R)=2, N(S)=2(DTAP) (MM) CM Service Request
LAPDm	81	I, N(R)=3, N(S)=2(DTAP) (MM) CM Service Accept
LAPDm	81	I, N(R)=3, N(S)=3(DTAP) (CC) Setup
LAPDm	81	I, N(R)=4, N(S)=3(DTAP) (CC) Call Proceeding
LAPDm/…	81	I, N(R)=4, N(S)=4(DTAP) (CC) Facility (GSM MAP) invoke notifySS
LAPDm	81	I, N(R)=4, N(S)=5(DTAP) (CC) Alerting
LAPDm	81	I, N(R)=4, N(S)=6(DTAP) (CC) Disconnect
LAPDm	81	I, N(R)=7, N(S)=4(DTAP) (CC) Release
LAPDm	81	I, N(R)=4, N(S)=7(DTAP) (CC) Connect
LAPDm	81	I, N(R)=0, N(S)=5(DTAP) (CC) Connect Acknowledge
LAPDm	81	I, N(R)=5, N(S)=0(DTAP) (CC) Release Complete
LAPDm	81	I, N(R)=0, N(S)=0 (Fragment)
LAPDm	81	I, N(R)=0, N(S)=1 (Fragment)
LAPDm	81	I, N(R)=0, N(S)=2 (Fragment)
LAPDm	81	I, N(R)=0, N(S)=3 (Fragment)
LAPDm	81	I, N(R)=0, N(S)=4 (Fragment)
LAPDm	81	I, N(R)=0, N(S)=5 (Fragment)
GSM SMS	81	I, N(R)=0, N(S)=6(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
LAPDm	81	I, N(R)=7, N(S)=0(DTAP) (SMS) CP-ACK
LAPDm	81	I, N(R)=7, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
LAPDm	81	I, N(R)=2, N(S)=7(DTAP) (SMS) CP-ACK
LAPDm	81	I, N(R)=6, N(S)=1(DTAP) (CC) Disconnect
LAPDm	81	I, N(R)=2, N(S)=6(DTAP) (CC) Release
LAPDm	81	I, N(R)=7, N(S)=2(DTAP) (CC) Release Complete
LAPDm	81	I, N(R)=7, N(S)=3(DTAP) (RR) Channel Release

Attack Internet Account

- 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 1: Website/App Password Reset Solution Test

Website/App	Inbound or Outbound SMS
Facebook	Inbound
Google account	Inbound
WhatApp	Inbound
Alipay (Chinese PayPal)	Inbound
WeChat (Chinese WhatApp)	Outbound
DiDi (Chinese Uber)	Inbound
Sina Weibo (Chinese Twitter)	Outbound

Attack Internet Account

Demo Video

Countermeasures

- To operators
  - Improve the CSFB authentication procedure. How long is the added latency?
  - Speed up VoLTE service deployment
- To Internet service provider
  - Be alert that the PSTN authentication is not safe.
  - The password reset procedure should be improved by additional personal information check.

GSMA CVD Program

- 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 transferred the vulnerability information to every operators.
- Now related operators are fixing or already fixed this vulnerability.

Mobile Security Research Hall of Fame

Welcome to the GSMA Mobile Security Research Hall of Fame.
The GSMA's Mobile Security Research Hall of Fame lists security vulnerability finders that have made contributions to increasing the security of the mobile industry by submitting disclosures to the GSMA or its members. It is the primary mechanism for the GSMA to recognise and acknowledge the positive impact the finder has had on the mobile industry by following the GSMA's CVD process.

The Hall of Fame also facilitates the nomination and recognition of other finders that may have made significant discoveries of vulnerabilities to individual GSMA member companies.

Entry to the Mobile Security Research Hall of Fame is purely optional and is at the discretion of the finder, the GSMA and/or the nominating GSMA member.

On behalf of the mobile industry, we would like to thank the following people for making a responsible disclosure to us and recognise their contribution to increasing the security of the mobile industry:

Date	Name	Organisation	Link
23/2/2017	Yuwei Zheng, Lin Huang, Haoqi Shan, Jun Li, Qing Yang	Unicorn Team, Radio Security Research Dept., 360 Technology	http://unicorn.360.com

Thank You ~