black hat®
USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

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)

Agenda

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

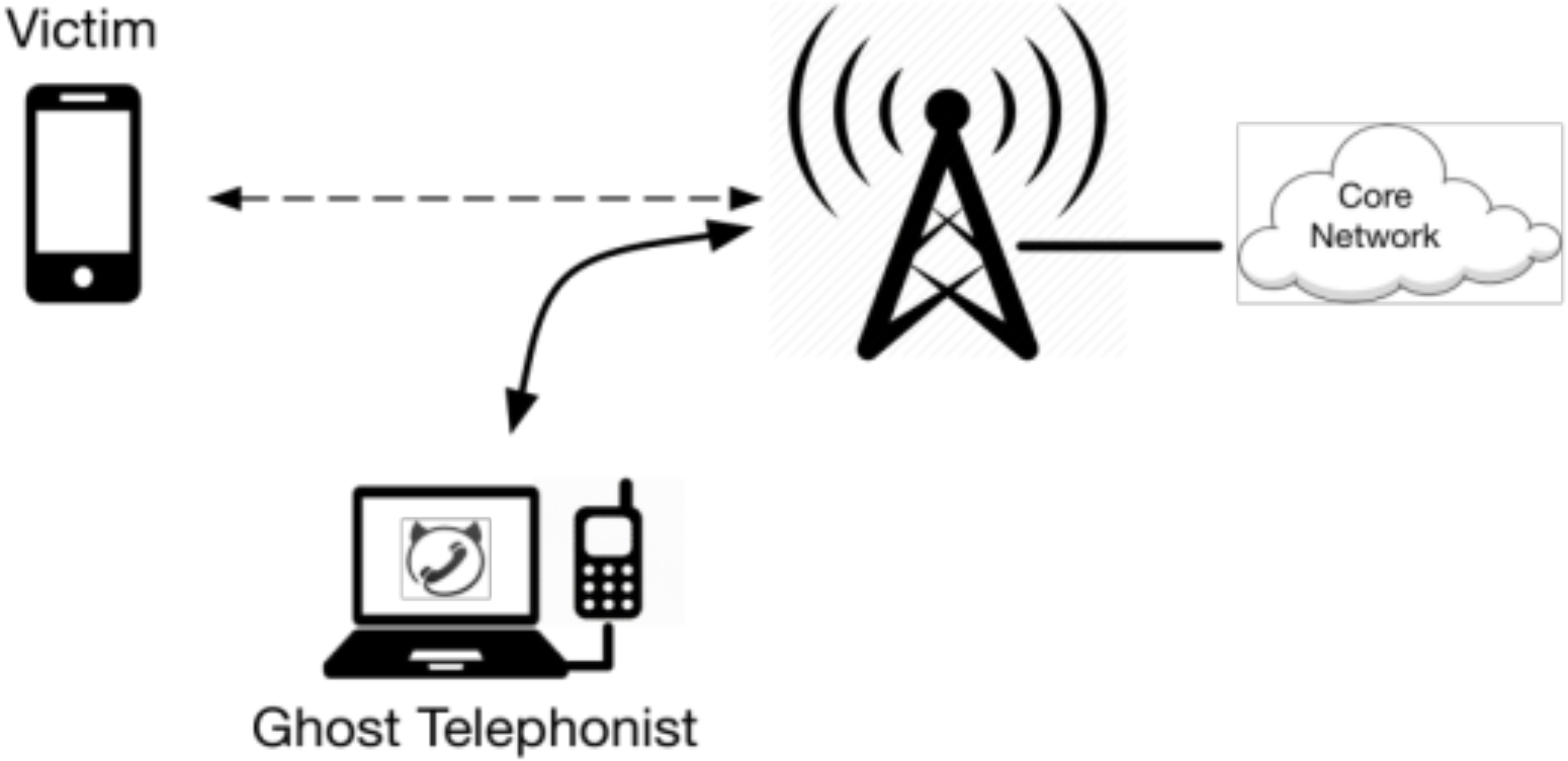
Ghost Telephonist

A story about this vulnerability

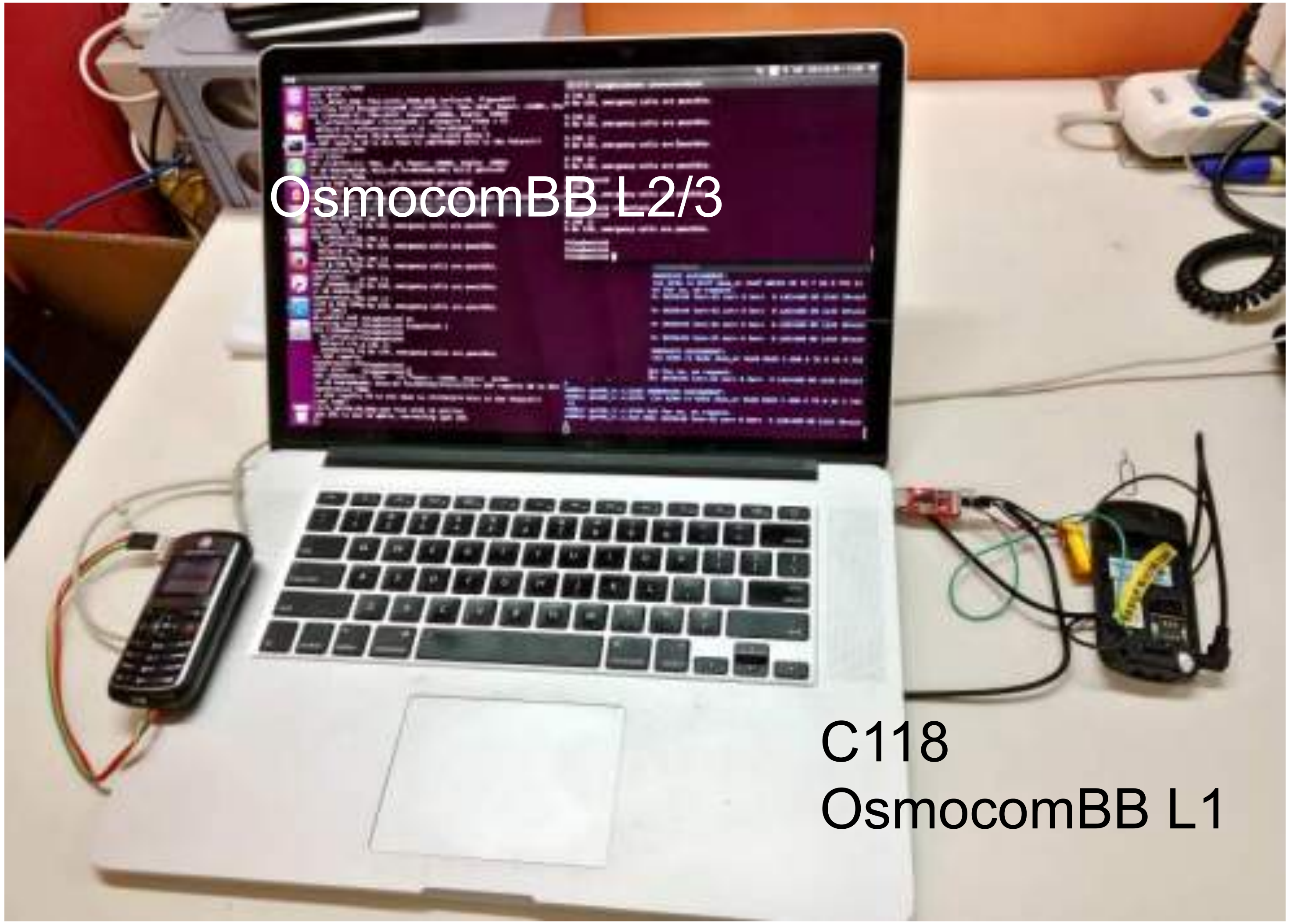
A flower does not grow sometimes when you purposely plant it whereas a willow grows and offers a shade sometimes when you purposelessly transplant it.

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



Experiment Setting



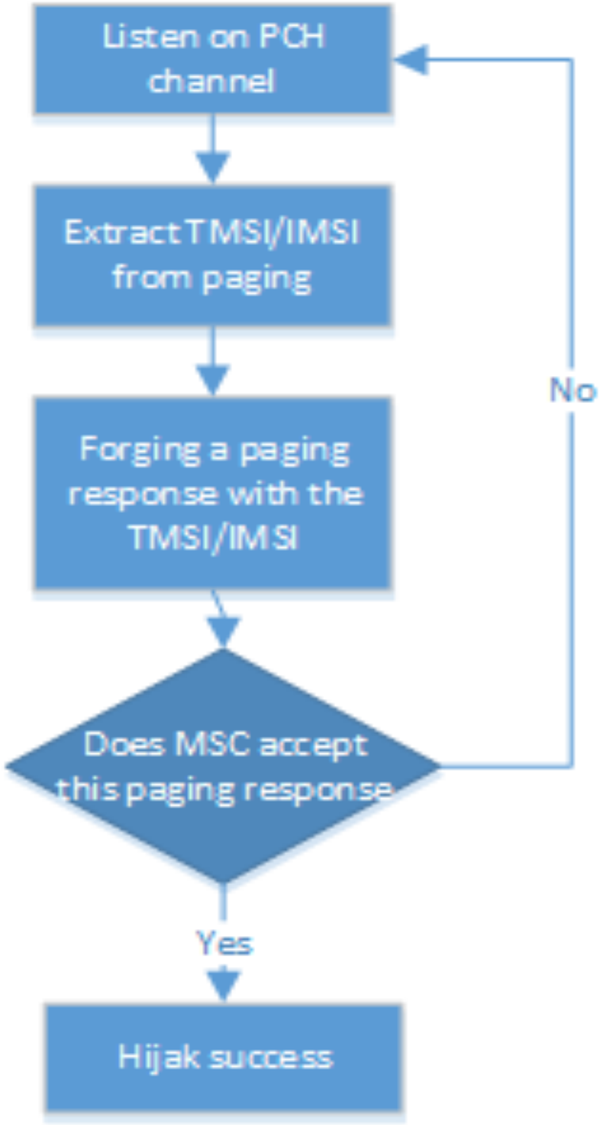
OsmocomBB L2/3

C118
OsmocomBB L1

Random Attack Steps

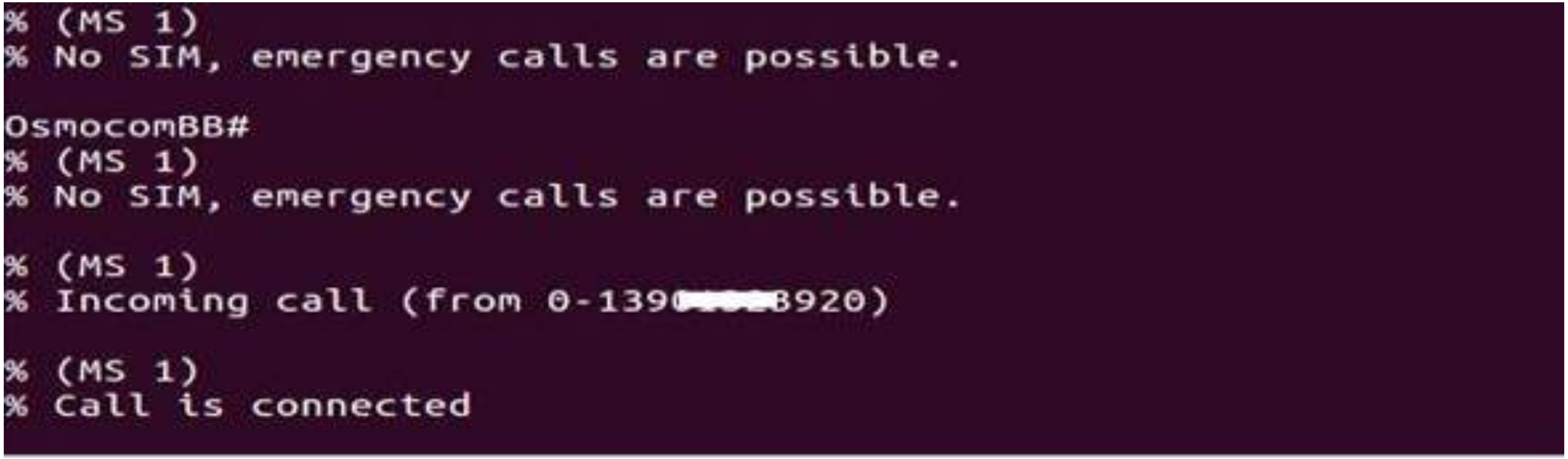
Attack Steps

- 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


Listen on PCH channel
Extract TMSI/IMSI from paging
Forging a paging response with the TMSI/IMSI
Does MSC accept this paging response
No
Yes
Hijak success

Hijack Result

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



```
% (MS 1)
% No SIM, emergency calls are possible.

OsmocomBB#
% (MS 1)
% No SIM, emergency calls are possible.

% (MS 1)
% Incoming call (from 0-139[redacted]920)

% (MS 1)
% Call is connected
```

Hijack Random Target

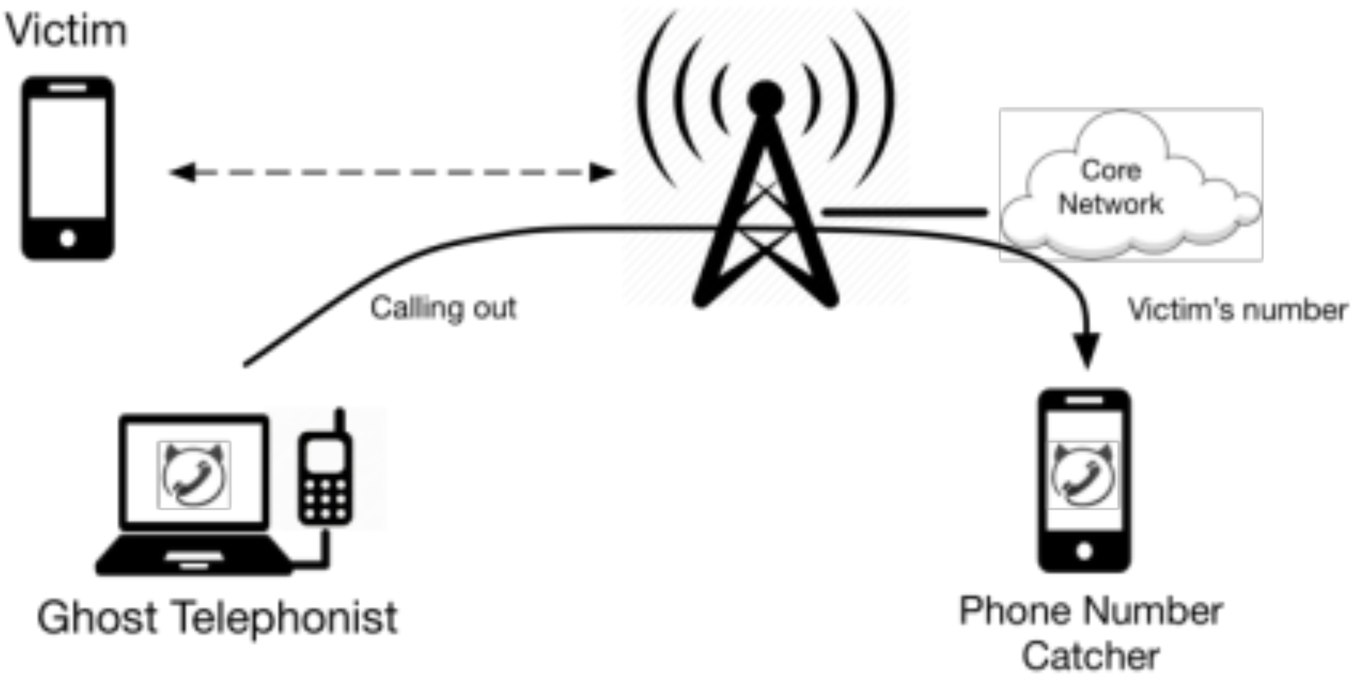
What can attacker do in further?

- 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

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'.

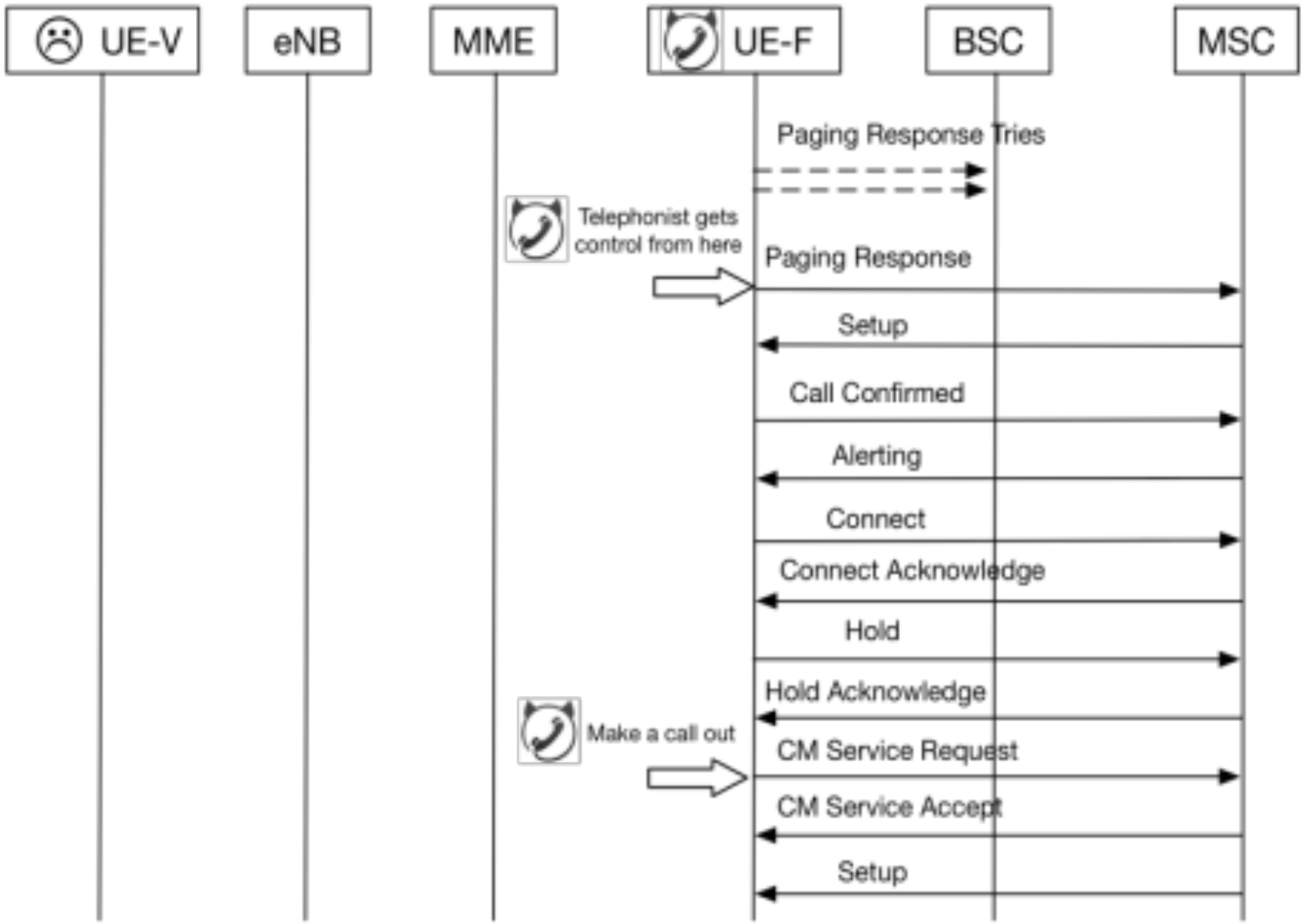
- So attacker can make a call to another in-hand phone to know the victim's ISDN number.



Get Victim’s Phone Number

Attack Signaling Flow

- 1) Send ‘hold’
- 2) Send ‘CM Service Request’

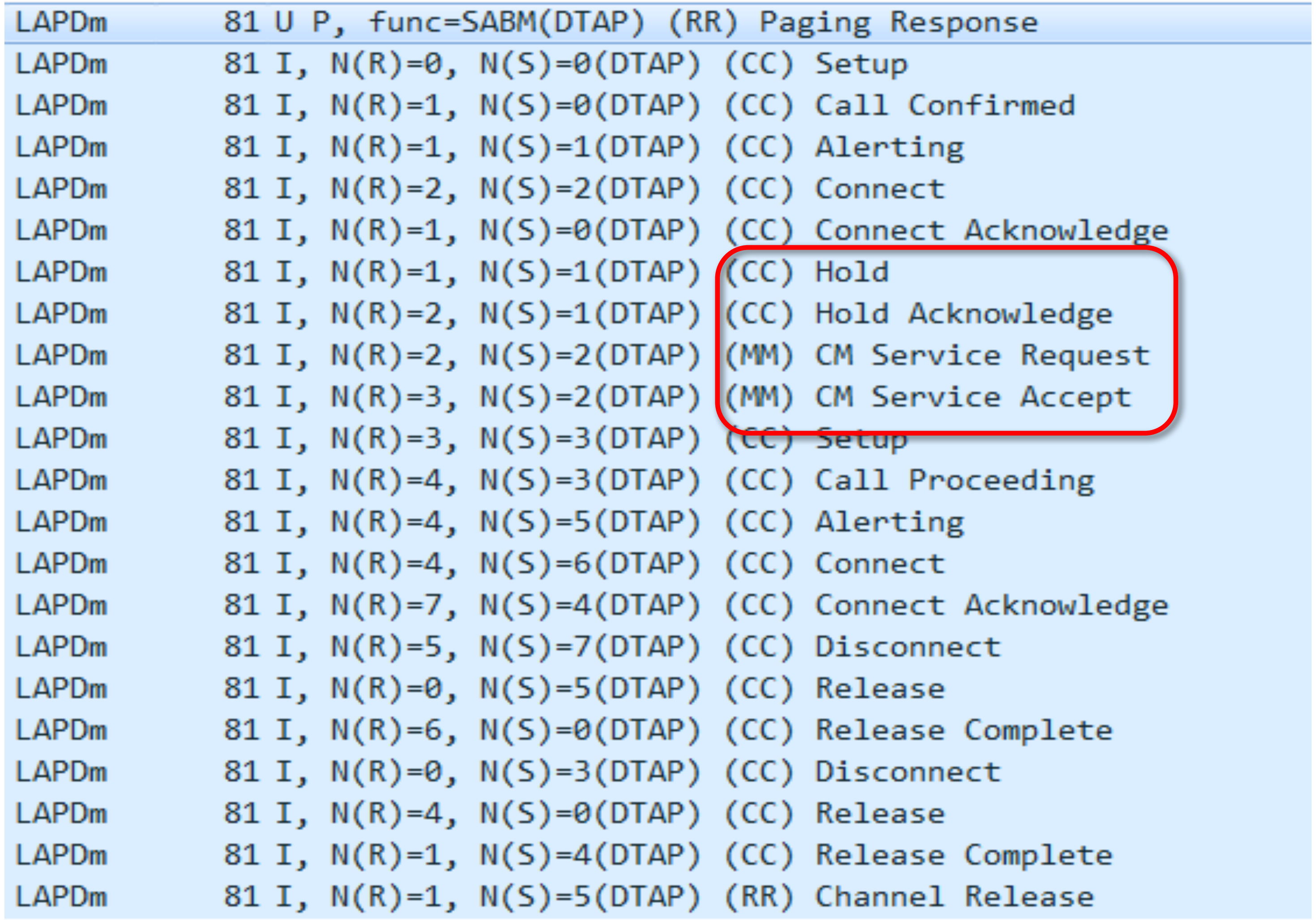


Get Victim’s Phone Number

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.



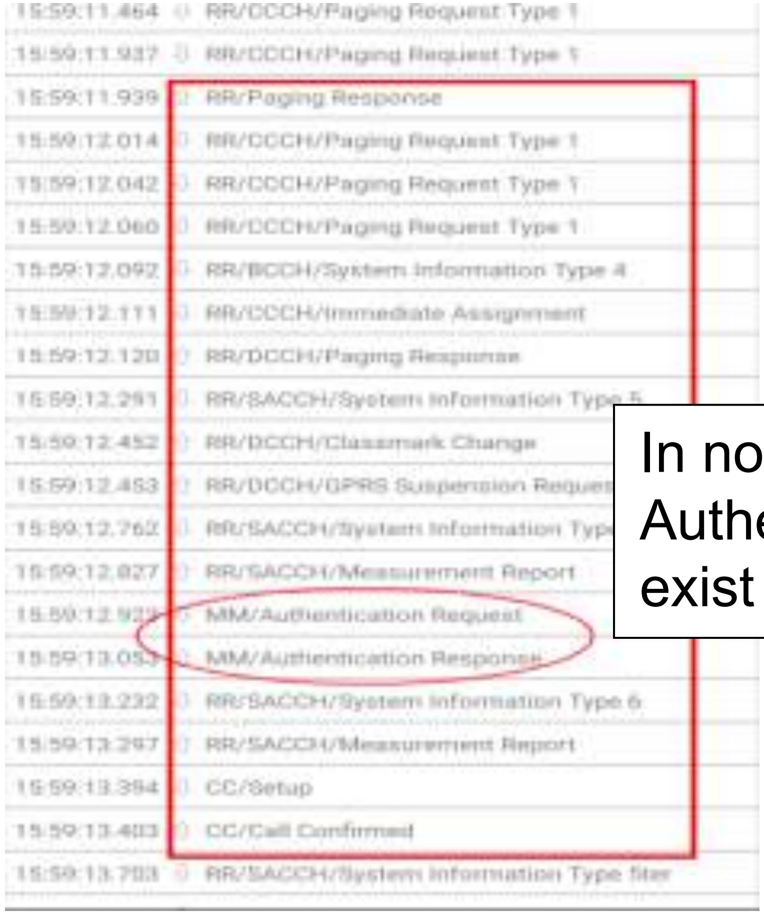
```
LAPDm        81 U P, func=SABM(DTAP) (RR) Paging Response
LAPDm        81 I, N(R)=0, N(S)=0(DTAP) (CC) Setup
LAPDm        81 I, N(R)=1, N(S)=0(DTAP) (CC) Call Confirmed
LAPDm        81 I, N(R)=1, N(S)=1(DTAP) (CC) Alerting
LAPDm        81 I, N(R)=2, N(S)=2(DTAP) (CC) Connect
LAPDm        81 I, N(R)=1, 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
```

Look for the Reason

Why do some attacks succeed, but some not?

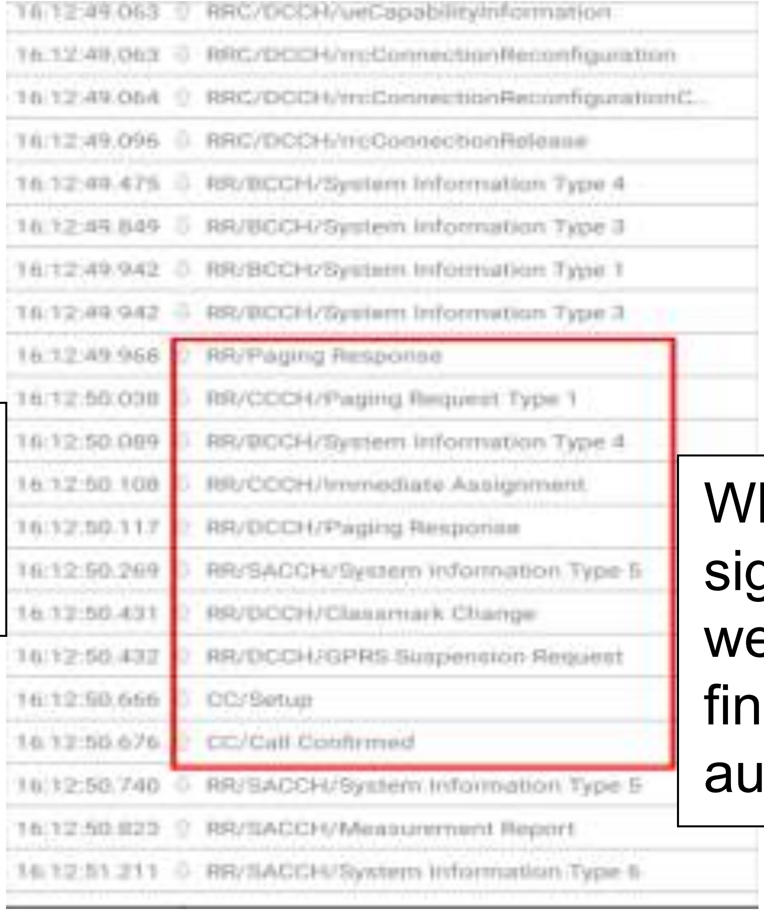
- Until now, our vision keeps in the 2G field…from the view of OsmocomBB.
- Is it introduced by the vulnerable GSM network?
- NO. We found if we set cellphone to be ‘2G-only’. Every call requires authentication.

Normal 2G Call vs. CSFB Call



```
15:59:11.464  RR/CCCH/Paging Request Type 1
15:59:11.937  RR/CCCH/Paging Request Type 1
15:59:11.939  RR/Paging Response
15:59:12.014  RR/CCCH/Paging Request Type 1
15:59:12.042  RR/CCCH/Paging Request Type 1
15:59:12.060  RR/CCCH/Paging Request Type 1
15:59:12.092  RR/BCCH/System Information Type 4
15:59:12.111  RR/CCCH/Immediate Assignment
15:59:12.120  RR/DCCH/Paging Response
15:59:12.291  RR/SACCH/System Information Type 5
15:59:12.452  RR/DCCH/Classmark Change
15:59:12.453  RR/DCCH/GPRS Suspension Reques
15:59:12.762  RR/SACCH/System Information Typ
15:59:12.827  RR/SACCH/Measurement Report
15:59:12.92   MM/Authentication Request
15:59:13.05   MM/Authentication Response
15:59:13.232  RR/SACCH/System Information Type 6
15:59:13.297  RR/SACCH/Measurement Report
15:59:13.394  CC/Setup
15:59:13.403  CC/Call Confirmed
15:59:13.703  RR/SACCH/System Information Type 5ter
```

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



```
16:12:49.063  RRC/DCCH/ueCapabilityInformation
16:12:49.063  RRC/DCCH/rrcConnectionReconfiguration
16:12:49.064  RRC/DCCH/rrcConnectionReconfigurationC...
16:12:49.096  RRC/DCCH/rrcConnectionRelease
16:12:49.475  RR/BCCH/System Information Type 4
16:12:49.849  RR/BCCH/System Information Type 3
16:12:49.942  RR/BCCH/System Information Type 1
16:12:49.942  RR/BCCH/System Information Type 3
16:12:49.966  RR/Paging Response
16:12:50.038  RR/CCCH/Paging Request Type 1
16:12:50.089  RR/BCCH/System Information Type 4
16:12:50.108  RR/CCCH/Immediate Assignment
16:12:50.117  RR/DCCH/Paging Response
16:12:50.269  RR/SACCH/System Information Type 5
16:12:50.431  RR/DCCH/Classmark Change
16:12:50.432  RR/DCCH/GPRS Suspension Request
16:12:50.666  CC/Setup
16:12:50.676  CC/Call Confirmed
16:12:50.740  RR/SACCH/System Information Type 5
16:12:50.823  RR/SACCH/Measurement Report
16:12:51.211  RR/SACCH/System Information Type 6
```

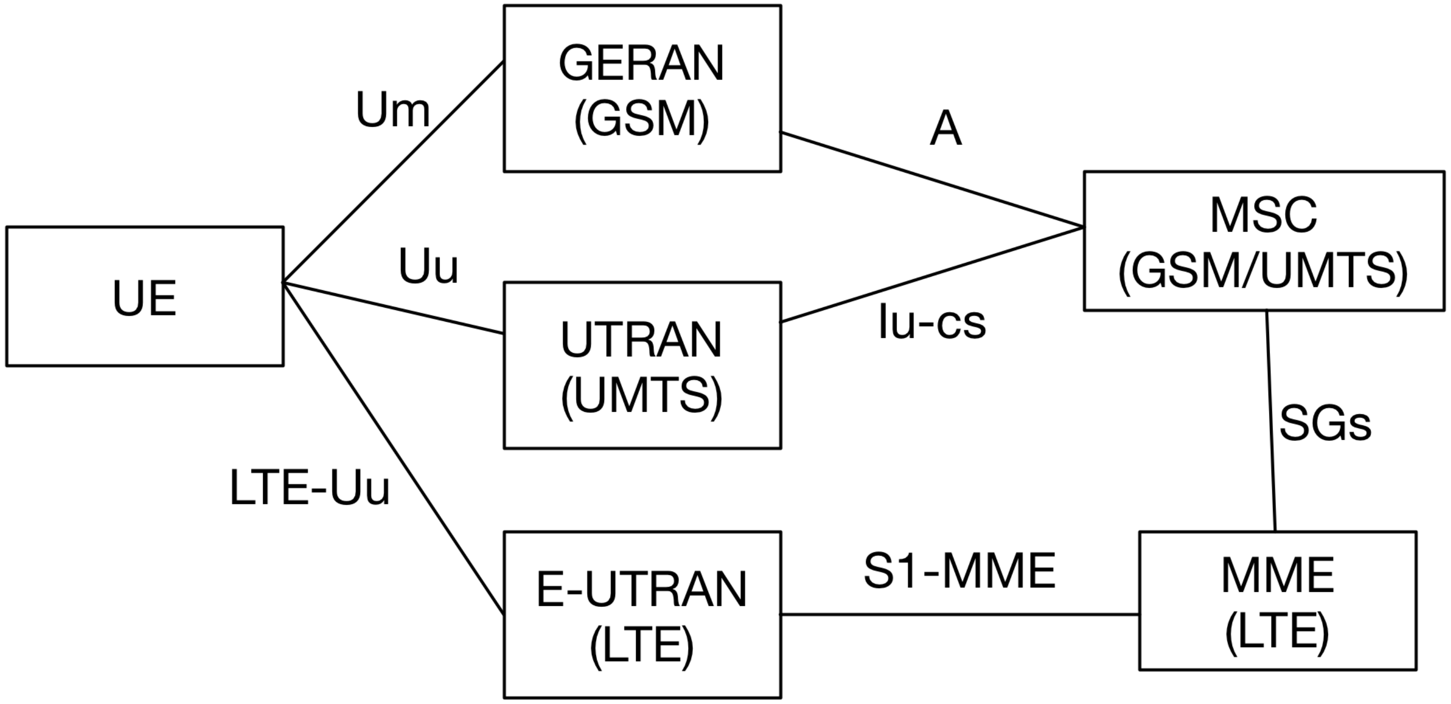
When we analyze the signaling flow of CSFB, we were surprised to find that there is no authentication step.

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

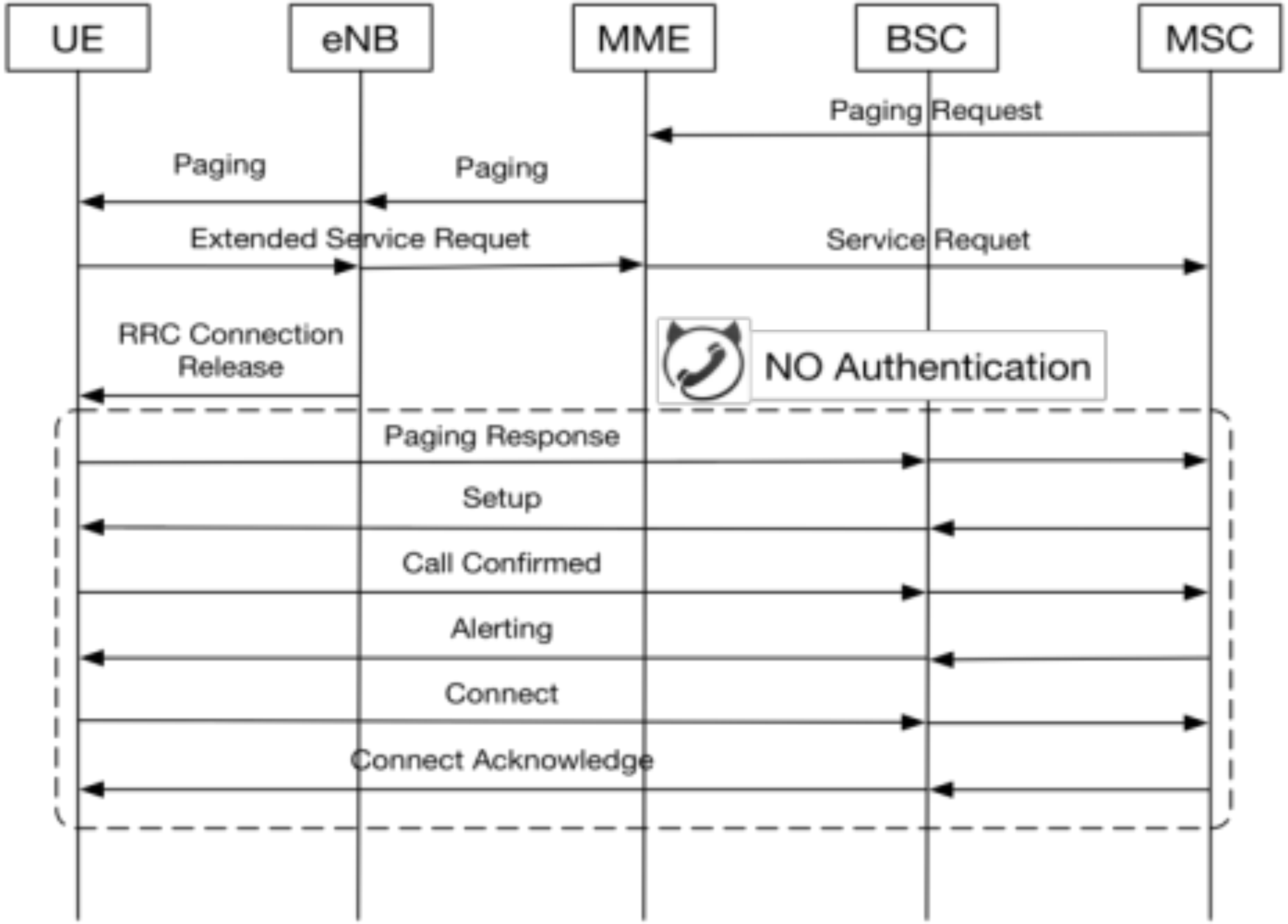
Network Architecture

- Combined attach / Combined Track area update

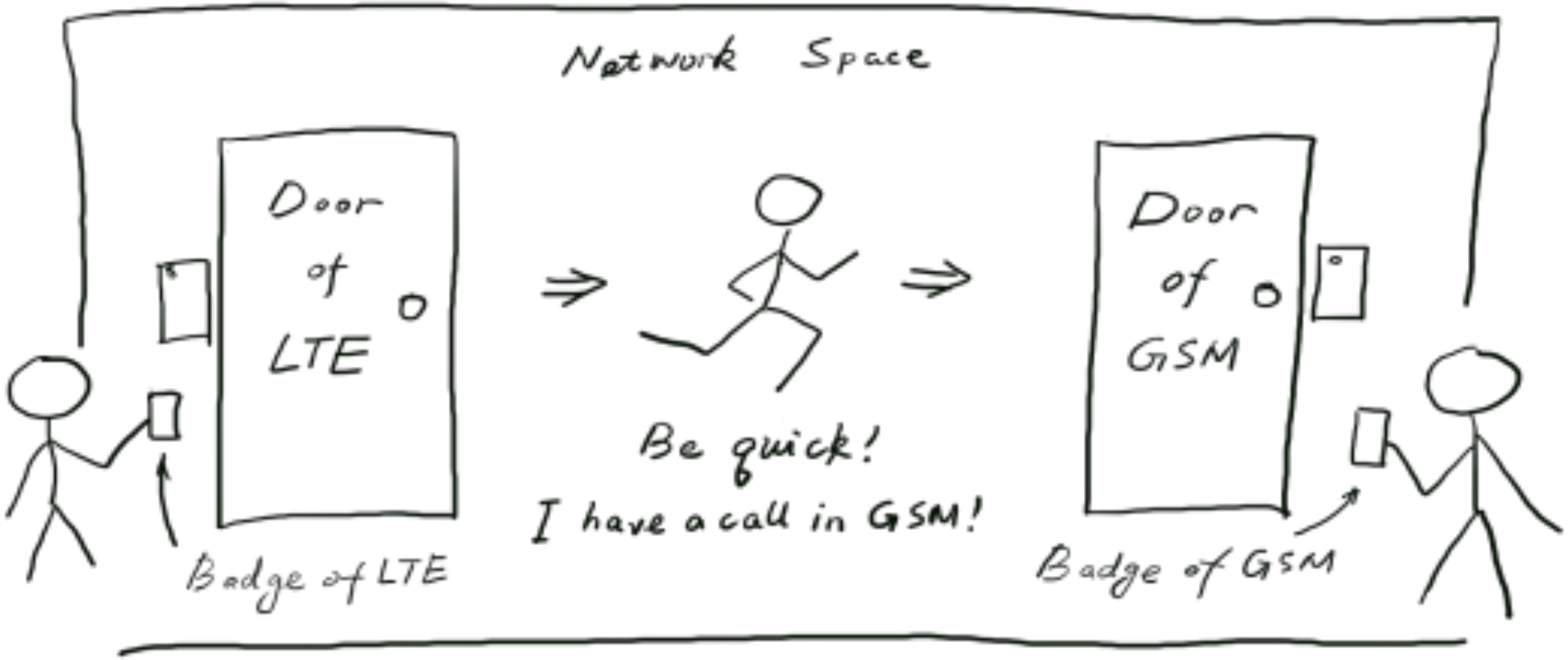


Vulnerability in CSFB

Signaling flow of CSFB MT call



Vulnerability in CSFB



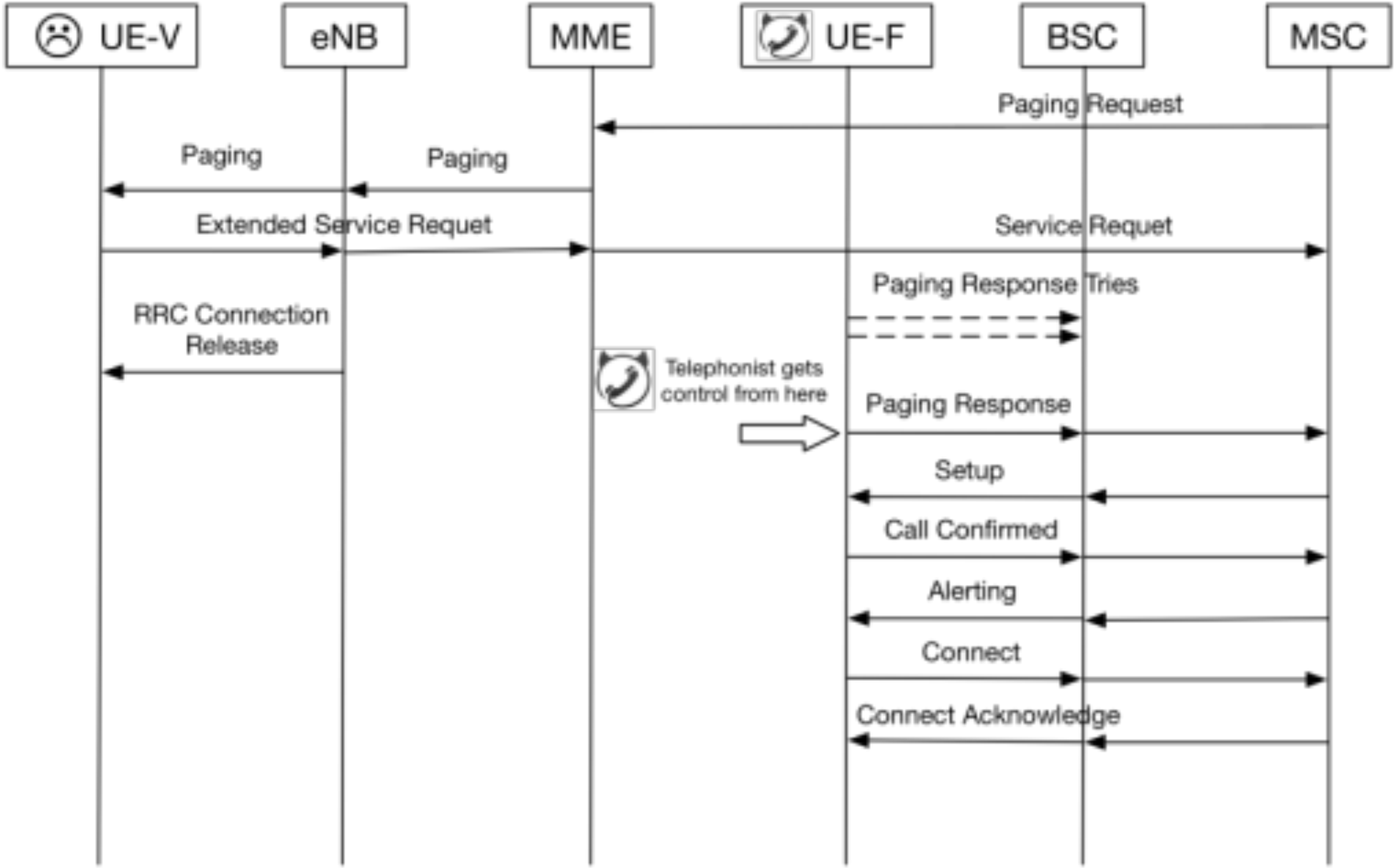
- The principle is like someone comes out from the door of LTE, then enters the door of GSM. He shouts, ‘I must be as quick as possible!’ Then he is permitted to enter, without the badge of GSM.

How to Exploit

- Basic idea
  - Because CSFB has no authentication procedure, attackers can send Paging Response on 2G network, impersonating the victim, thus hijack the call link.

Attack Signaling Flow

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

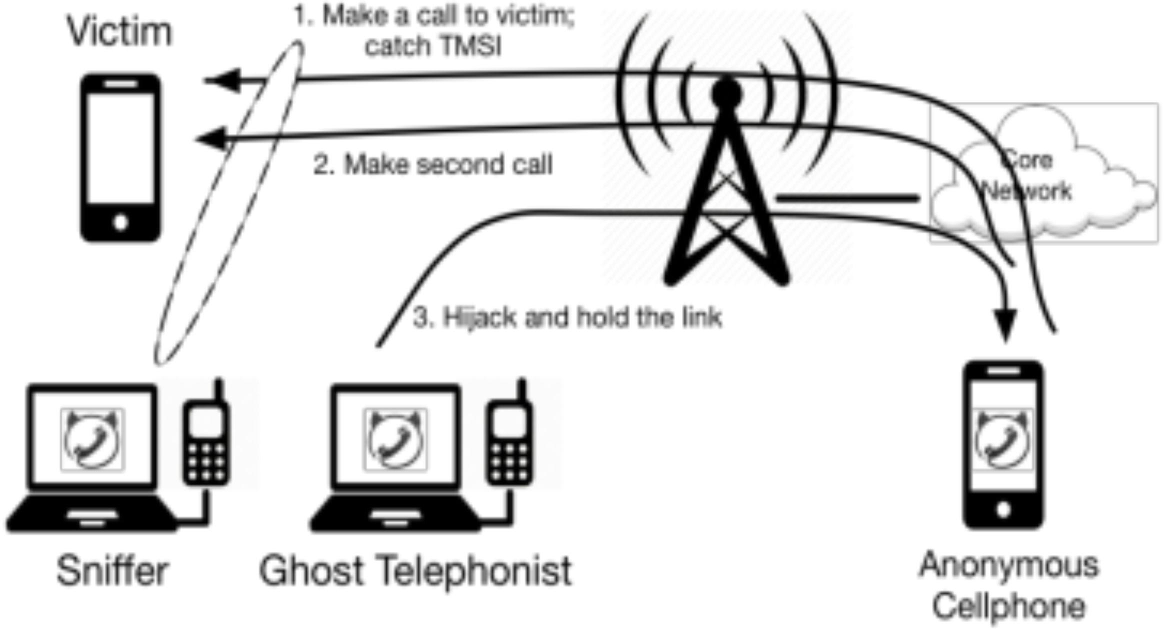
- Condition
  - Attacker knows victim’s TMSI
- Attack Steps
  - 1) Persistently sending Paging Response with this TMSI
  - 2) Once victim has a Paging procedure existing, attacker can quickly control the link.

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.

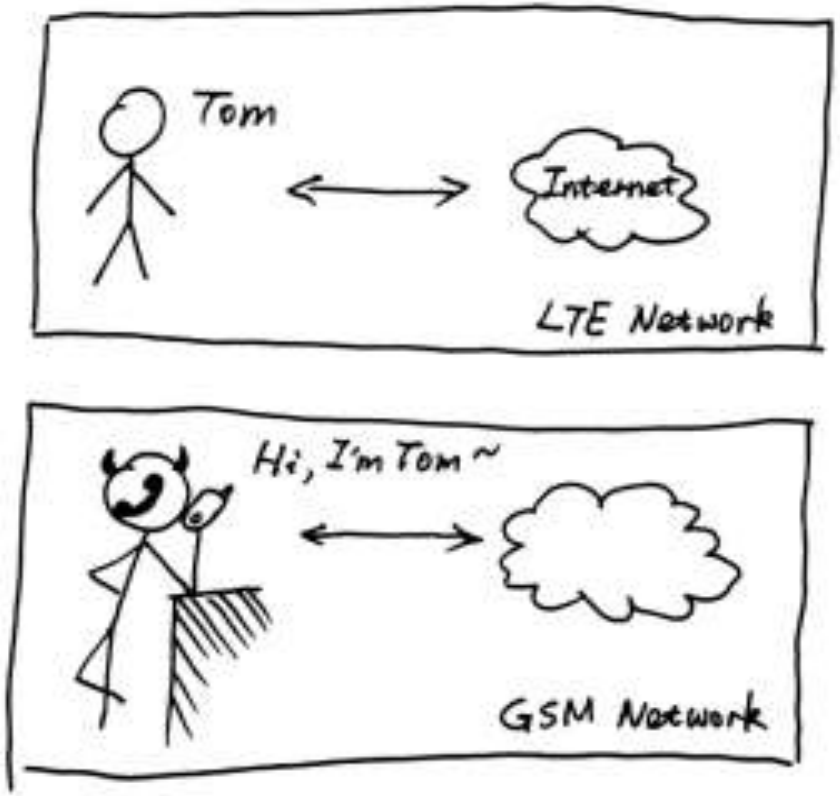
Attack with Phone Number

- 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.



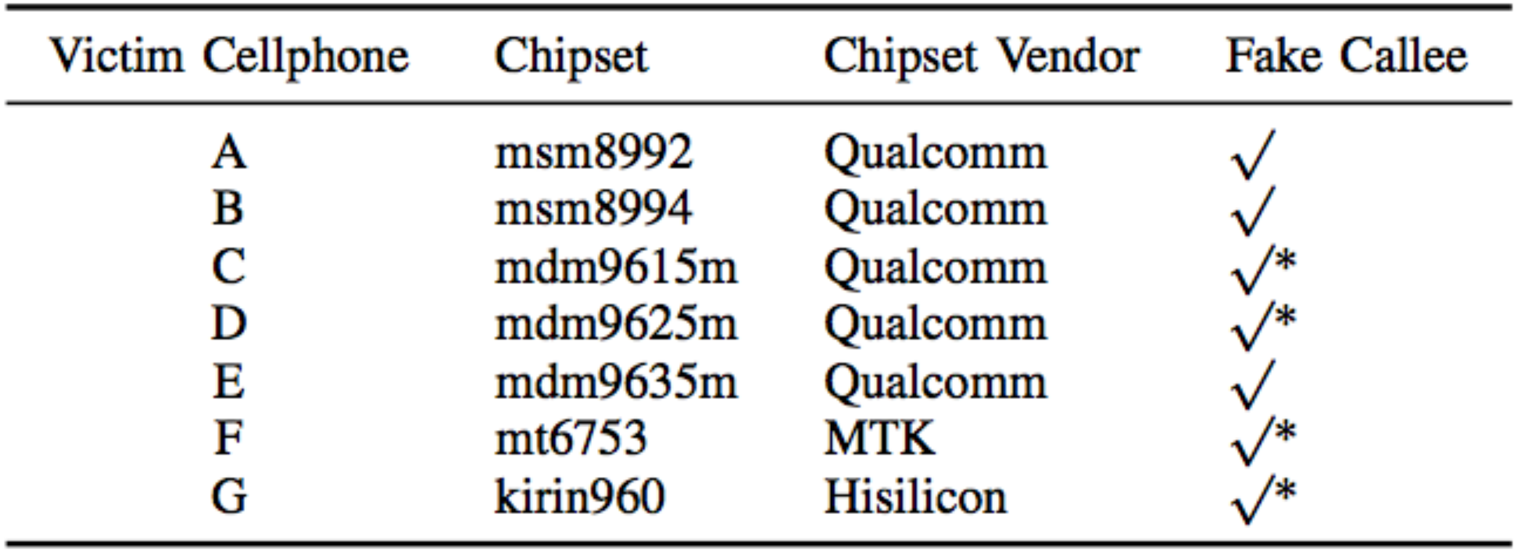
Features of Telephonist Attack

- 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.



Victim Cellphone	Chipset	Chipset Vendor	Fake Callee
A	msm8992	Qualcomm	√
B	msm8994	Qualcomm	√
C	mdm9615m	Qualcomm	√*
D	mdm9625m	Qualcomm	√*
E	mdm9635m	Qualcomm	√
F	mt6753	MTK	√*
G	kirin960	Hisilicon	√*

[*] means jamming is needed in the attack.

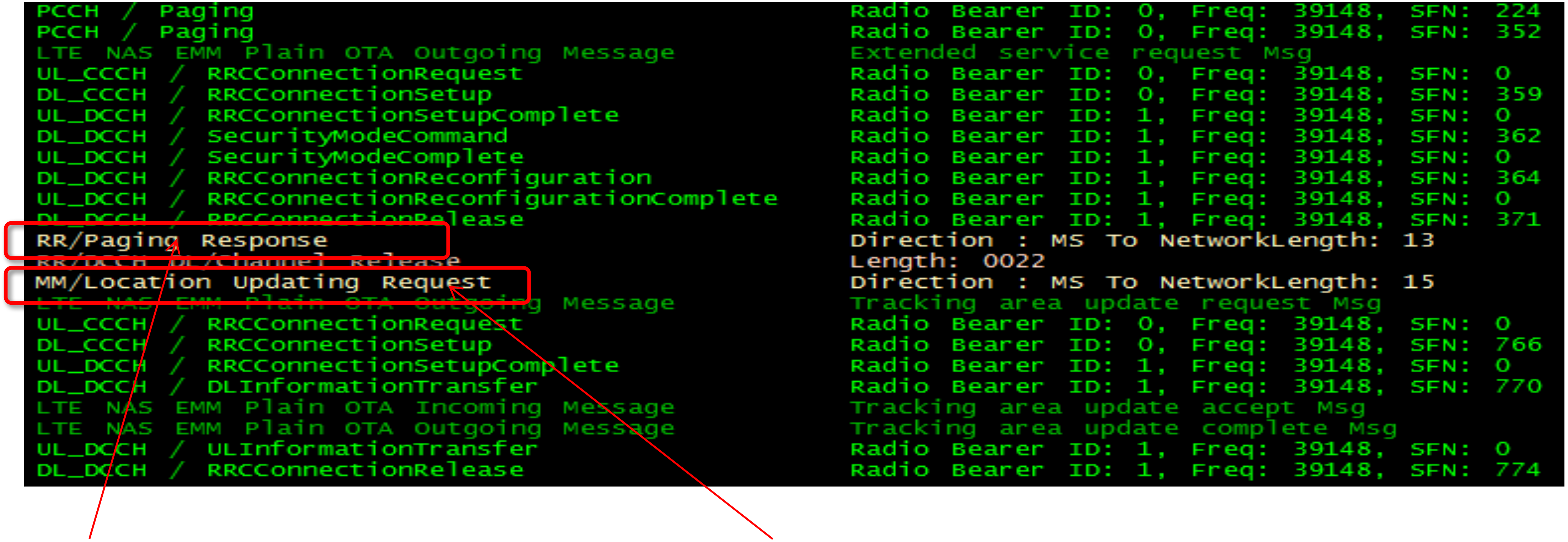
Cellphones with [*] have better defense against this attack. Jamming is needed to cut off the connection between victim cellphones and the network.

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



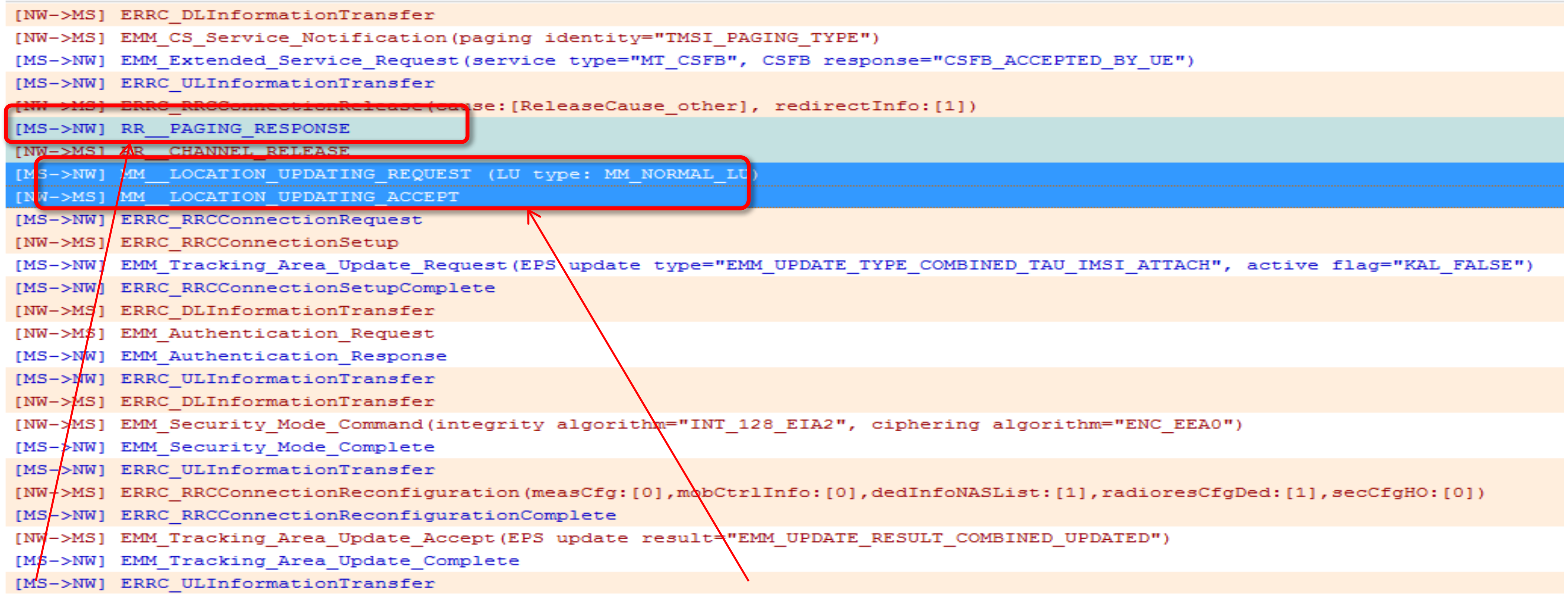
```
PCCH / Paging                                     Radio Bearer ID: 0, Freq: 39148, SFN: 224
PCCH / Paging                                     Radio Bearer ID: 0, Freq: 39148, SFN: 352
LTE NAS EMM Plain OTA Outgoing Message            Extended service request Msg
UL_CCCH / RRCConnectionRequest                    Radio Bearer ID: 0, Freq: 39148, SFN: 0
DL_CCCH / RRCConnectionSetup                      Radio Bearer ID: 0, Freq: 39148, SFN: 359
UL_DCCH / RRCConnectionSetupComplete              Radio Bearer ID: 1, Freq: 39148, SFN: 0
DL_DCCH / SecurityModeCommand                     Radio Bearer ID: 1, Freq: 39148, SFN: 362
UL_DCCH / SecurityModeComplete                    Radio Bearer ID: 1, Freq: 39148, SFN: 0
DL_DCCH / RRCConnectionReconfiguration            Radio Bearer ID: 1, Freq: 39148, SFN: 364
UL_DCCH / RRCConnectionReconfigurationComplete    Radio Bearer ID: 1, Freq: 39148, SFN: 0
DL_DCCH / RRCConnectionRelease                    Radio Bearer ID: 1, Freq: 39148, SFN: 371
RR/Paging Response                                Direction : MS To NetworkLength: 13
RR/DCCH DL/Channel Release                        Length: 0022
MM/Location Updating Request                      Direction : MS To NetworkLength: 15
LTE NAS EMM Plain OTA Outgoing Message            Tracking area update request Msg
UL_CCCH / RRCConnectionRequest                    Radio Bearer ID: 0, Freq: 39148, SFN: 0
DL_CCCH / RRCConnectionSetup                      Radio Bearer ID: 0, Freq: 39148, SFN: 766
UL_DCCH / RRCConnectionSetupComplete              Radio Bearer ID: 1, Freq: 39148, SFN: 0
DL_DCCH / DLInformationTransfer                   Radio Bearer ID: 1, Freq: 39148, SFN: 770
LTE NAS EMM Plain OTA Incoming Message            Tracking area update accept Msg
LTE NAS EMM Plain OTA Outgoing Message            Tracking area update complete Msg
UL_DCCH / ULInformationTransfer                   Radio Bearer ID: 1, Freq: 39148, SFN: 0
DL_DCCH / RRCConnectionRelease                    Radio Bearer ID: 1, Freq: 39148, SFN: 774
```

Paging Response failure

Location Update not completed

Failure Analysis

Fast Return Case 2 – Cellphone F, 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

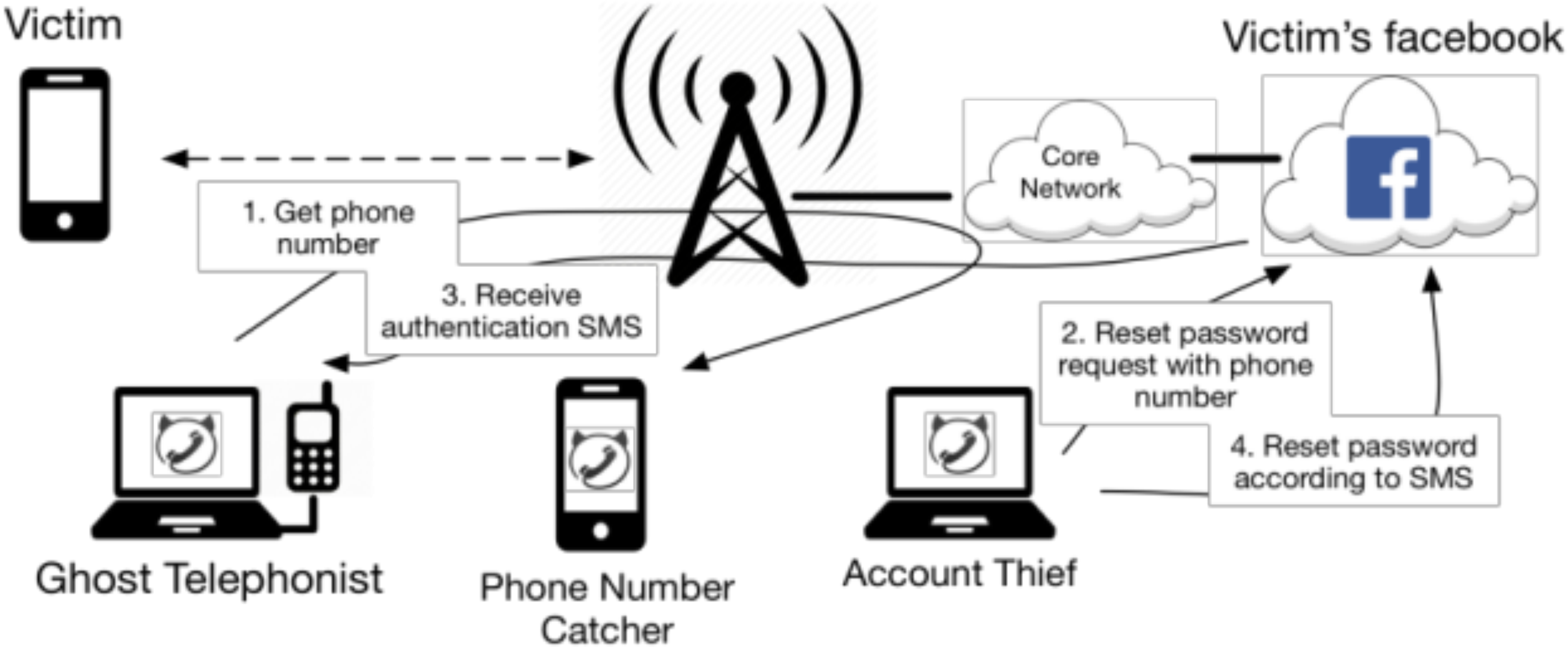
Supplemented by Jamming

- 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.

Attack Internet Account

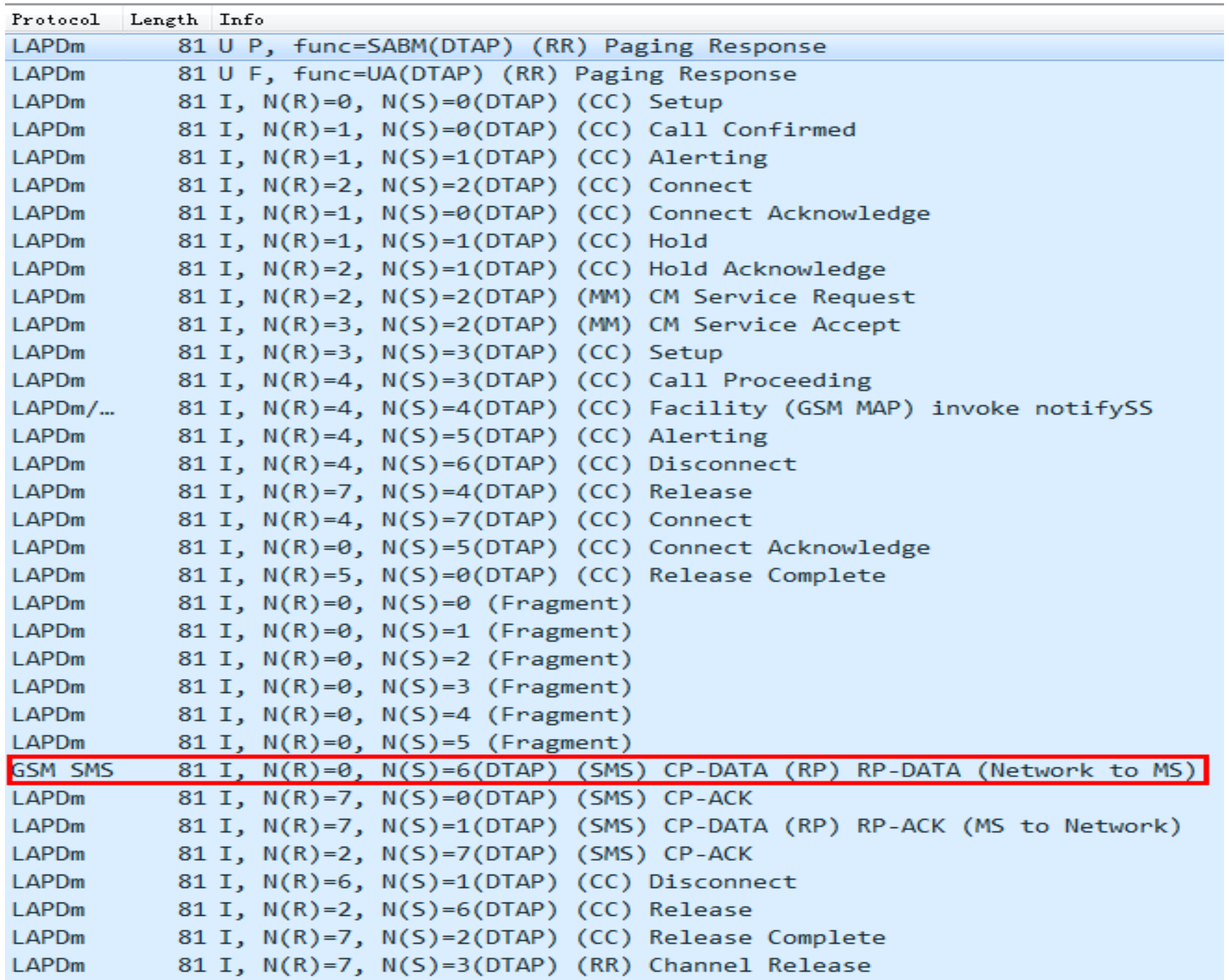
- Login with verification SMS
  - Some applications permits login with cellphone number + verification SMS. Don’t require inputting password.
- Reset login password with verification SMS
  - A lot of Internet application accounts use verification SMS to reset the login password. Attacker can use the cellphone number to start a password reset procedure then hijack the verification SMS.

Attack Steps


Victim
Victim's facebook
Core Network
1. Get phone number
3. Receive authentication SMS
2. Reset password request with phone number
4. Reset password according to SMS
Ghost Telephonist
Phone Number Catcher
Account Thief

Attack Signalling Flow

- 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.

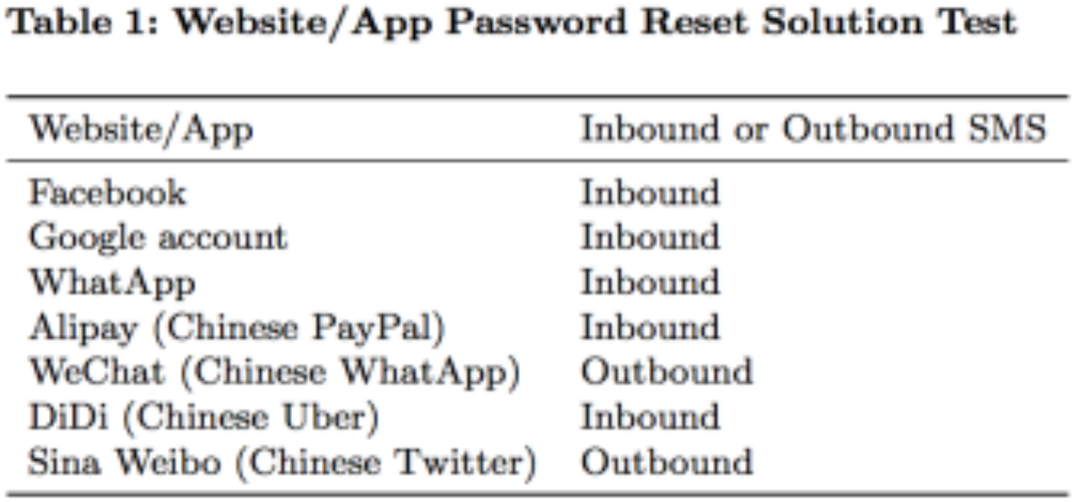


Table 1: Website/App Password Reset Solution Test

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

MOTOROLA
layer1.bin
Sniffer
C118
360

Constraints and Impacts

- 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.

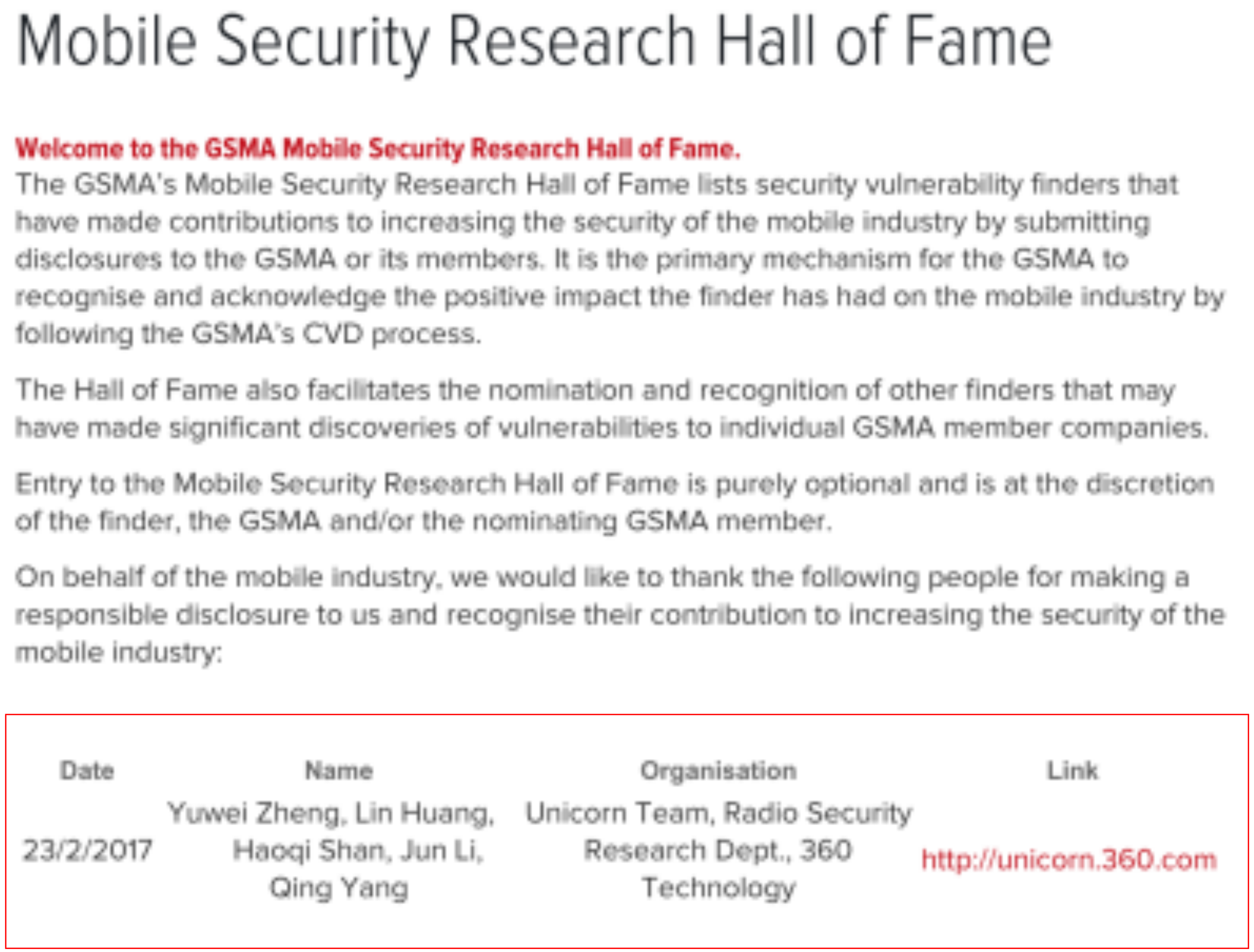
GSMA CVD Program

- 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 forwarded 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 ~