Hacking mobile network via SS7: interception, shadowing and more

Dmitry Kurbatov
Vladimir Kropotov
Positive Research
Agenda

• Intro
• Attacks prerequisites, costs and case studies
• Official and underground market brief
• Possible Security measures
• Forecasts
In Service LTE Networks

<table>
<thead>
<tr>
<th>Operator/Network Name</th>
<th>Deployment Status</th>
<th>LTE Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific Telecom</td>
<td>In Service December 2014</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific Telecom</td>
<td>In Service December 2014</td>
<td></td>
</tr>
<tr>
<td>Taiwan Star Mobile</td>
<td>In Service August 2014</td>
<td></td>
</tr>
<tr>
<td>Chunghwa Telecom</td>
<td>In Service May 2014</td>
<td>LTE-900, LTE-1800</td>
</tr>
<tr>
<td>FarEasTone / China Mobile</td>
<td>In Service June 2014</td>
<td></td>
</tr>
<tr>
<td>Taiwan Mobile Company</td>
<td>In Service June 2014</td>
<td></td>
</tr>
</tbody>
</table>
VoLTE Networks

http://ltemaps.org/
The most of the world performs HANGDOVER

LTE only for web browsing

To perform a call subscriber is downgraded to 3G (handover)
Interconnect / roaming
Kind of IPv4 vs IPv6 dilemma
SS7 is still most used interconnect/roaming network

Mobility
Call control
Billing
Crypto
2014 - year of SS7 security issues

Hackito Ergo Sum 2014
- Locating mobile phones

Positive Hack Days IV
- How to Intercept a Conversation Held on the Other Side of the Planet

Washington Post
- Secretly track cellphones

31C3
- SS7: Locate. Track. Manipulate
- Mobile self-defense
SS7 for (bad) guys

Tracking
• Locating mobile phones and secretly tracking

Denial of Service
• Disrupt subscriber connectivity and service availability

Interception
• Listen to calls, intercept short messages

Threats to Operator

Threats to IoT
Basic Terms

• IMSI ~ SIM Card
• IMEI ~ Device
• MSISDN ~ Your Number
• HLR ~ Subscriber DB
• MSC ~ Call Processing
Tracking / 跟踪(位置)
Common Step 0 for Any Attack

1. Attacker sends request `SendRoutingInfoForSM` addressing MAP message by MSISDN
   - own address
   - serving MSC address
   - IMSI
Get Cell ID

1. Attacker sends request provideSubscriberInfo addressing MAP message by IMSI and asking for subscriber location

2. MSC replies with Cell ID:
   - MCC - 250
   - MNC - 90
   - LAC 4A67
   - CID 673D
Get Location...

**Search in Internet** for physical location by MCC, MNC, LAC, CID

- **MCC**: 250
- **MNC**: 90
- **LAC**: 4A67
- **CID**: 673D
...and Track User Just Like SkyLock

Underground market demands

Tracking subscriber using the phone number
Yep, Even in 2010
Tracking

Nobody wants to be constantly monitored.

Tracking is a violation of “Personal data protection” laws.

Very hard to stop:

• AnyTimeInterrogation
• ProvideSubscriberInfo
• ProvideSubscriberLocation
DoS / 阻斷服務攻擊

To make someone unavailable

To stop data leakage

What else?
Common Step 0 for Any Attack

1. Attacker sends request SendRoutingInfoForSM addressing MAP message by MSISDN
2. HLR replies with:
   - own address
   - serving MSC address
   - IMSI
Denial of Service. Step 1

1. Attacker registers Bob on the fake MSC
2. HLR sets up new location for Bob
3. HLR asks real MSC to release a memory
Denial of Service. Step 2

1. Alex calls Bob
2. MSC is looking for Bob and asks HLR to provide information
3. HLR asks fake MSC to provide Roaming Number
demo
Interception / 截聽
How to Intercept SMS (截聽短信)

• A virus on a smartphone – and what if a certain subscriber is a target? How to infect him particularly?
• Reissue SIM? It works only once.
• Radio signal interception (GSM A5/1)? You need to be nearby.
• Via SS7 network
Fake Mobile Phone Towers Operating In The UK

A Sky News investigation uncovers the use of IMSI catchers, which can collect the data of innocent people as they use their phone.

By Tom Cheshire, Technology Correspondent

Sky News has found evidence that rogue mobile phone towers, which can listen in on people’s calls without their knowledge, are being operated in the UK.

An investigation by Australian TV show 60 Minutes demonstrates how hackers based thousands of miles away in Germany were able to record the calls of an Australian senator and track his movements.
A Cheap Way For Tapping

10$ + OpenSource

+ osmocomBB + WIRESHARK
(f)or

$$7$$
Common Step 0 for Any Attack

1. Attacker sends request SendRoutingInfoForSM addressing MAP message by MSISDN
2. HLR replies with:
   • own address
   • serving MSC address
   • IMSI
SMS Interception. Step 1

1. Attacker registers Bob on the fake MSC
2. HLR sets up new location for Bob
3. HLR asks real MSC to release a memory
SMS Interception. Step 2

1. Alex sends SMS to Bob
2. MSC translates the SMS to SMS-C
3. SMS-C requests HLR for Bob`s location
4. HLR replies with a fake MSC address
5. SMS-C translates SMS to the fake MSC
demo
OH MY GOD

WHO THE HELL CARES?
SMS Interception, We “Really Missed” You

• Access to payment service
• Recover passwords for email and social networks
• Online banking OTP
Illegal cases

SMS Interception

Куплю перехват СМС/Востановление сим [Дорого]

29.10.2012

Куплю перехват сим/востановление сим. Дорого. Буду покупать на постоянной основе. jabber:

Работа с QIWI кошельками - или как перехватить СМС-подтверждения?

02.02.2013

Собственно сабж. Вручу кошельки киви, но очень часто бывает что стоят СМС-подтверждения или СМС уведомления на перевод средств с кошелька на кошельк. Хотя бы хотел четко и точно ответить ей.

Интересуют устройства для перехвата СМС
Обсуждение в разделе «Электроника и Фрикинг», начал(-а) TommyLick, 13.08.2015.

13.08.2015

Добрый день, интересуют устройства для перехвата СМС и разговоров. Кто владеет информацией где можно приобрести данные игрушки прошу в лп.
Active actions and Impersonation

— Mobile balance transfer over USSD
— Premium Rate SMS Subscriptions
— Credit cards money transfers via phone
— Even fake calls from Victim number
How to Get Into SS7
How They Can Get Into SS7

Legal with license
Semi legal without

Find a guy

Hack border device
Find a Guy


Looking to get LAC/CELL ID from a VLR lookup

Price per query up to $150. More than 50 queries per month required ($50 x 150 = $7,500 monthly).

In case you are able to immediately provide a demo lookup, you are welcome to bid.

Please do not bid if you are not capable of providing advanced location-based services.

Skills required: GSM Geolocation, SSS signaling, Tier1

Tips for bidders:
- Looking for a LBS provider who can immediately offer us a advanced VLR lookup service that will return the LAC code and the CID of a MSIDN using a HTTP API.
- You have to do perform a SS7 MAP Anytime interrogation query to get the LAC and CID from the VLR.
- In case you are able to immediately provide a demo lookup, you are welcome to bid.
- Please do not bid if you are not capable of providing advanced location-based services.
- Skills required: GSM Geolocation, SSS signaling, Tier1

Tips for bidders:
- Looking for a LBS provider who can immediately offer us a advanced VLR lookup service that will return the LAC code and the CID of a MSIDN using a HTTP API.
- You have to do perform a SS7 MAP Anytime interrogation query to get the LAC and CID from the VLR.
- In case you are able to immediately provide a demo lookup, you are welcome to bid.
- Please do not bid if you are not capable of providing advanced location-based services.
- Skills required: GSM Geolocation, SSS signaling, Tier1
Find a Guy


Looking for SS7 access

Hello!
I'm interested in telecommunications network access via Sigtran (SS7) to make HLR lookup requests, perform geo location search of cell phones, and send bulk SMS.
I need direct access only to send MAP messages; getting access via an API is not required. Decent pay.
If you have an offer, please contact me personally.
smithyjohny@vilemail.net

Email sent from *****ham@safe-mail.net

In case you are able to immediately provide a demo lookup you are welcome to bid.
Please do not bid if you are not capable of providing advanced location based services.

Skills required: Gsm Geolocation, SS7 signaling, Tier1

- Please do not bid if you are not capable of providing advanced location based services.
- In case you are able to immediately provide a demo lookup you are welcome to bid.
- Smithyjohny@vilemail.net
- Email sent from *****ham@safe-mail.net

Skills required: Gsm Geolocation, SS7 signaling, Tier1

- Please do not bid if you are not capable of providing advanced location based services.
- In case you are able to immediately provide a demo lookup you are welcome to bid.
- Smithyjohny@vilemail.net
- Email sent from *****ham@safe-mail.net
Find a Guy

Hello!
I'm interested in telecommunications network access via Sigtran (SS7) to make HLR lookup requests, perform geo location search of cell phones, and send bulk SMS.
I need direct access only to send MAP messages; getting access via an API is not required. Decent pay.
If you have an offer, please contact me personally.
smithyjohny@vremail.net
Hack border device
Today: IP Connectivity
Misconfiguration Example

Critical

Open Telnet, no password

---

SHODAN

Critical

Open Telnet, no password
Research Updates

• SS7 security threats
• Mobile Internet vulnerabilities (GPRS)
• SIM vulnerabilities

http://www.ptsecurity.com/library/whitepapers/
http://blog.ptsecurity.com/
Questions?

Dmitry Kurbatov
dkurbatov@ptsecurity.com

Vladimir Kropotov
vkropotov@ptsecurity.com