Hacking mobile network via SS7: interception, shadowing and more

Dmitry Kurbatov
Security specialist
Positive Research
Korea is an LTE country

GSMA WELCOMES LAUNCH OF WORLD’S FIRST COMMERCIAL INTERCONNECTED VoLTE SERVICE IN SOUTH KOREA

In Service LTE Networks
VoLTE Networks

VoLTE Networks

http://ltemaps.org/
The rest of the world performs handover

LTE only for web browsing

To perform a call subscriber is downgraded to 3G (handover)
INTERCONNECTED VoLTE

June 18, 2015 | Press Release

South Korean Mobile Operators to Launch Commercial Interconnected VoLTE Service. Delivering Higher Quality Voice and Faster Connection

London: The GSMA welcomes the announcement by South Korea’s mobile network operators to launch the world’s first commercial interconnected VoLTE service. The service, which is supported by the Ministry of Science, ICT and Future Planning as well as the GSMA, was officially unveiled by Minister Yang Hee Choi this week and will launch later this month. It will deliver higher quality calls and seamless switching between voice and video, as well as faster connection speeds to subscribers of all three networks. Currently, VoLTE services are only available to subscribers of the same network.
Interconnect / roaming

SS7

2G / 3G

GRX

3G / 4G

3G / 4G

IPX
The rest of the world
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 and internet traffic

Threats to Operator

Threats to IoT
Tracking
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
1. Attacker sends request to provideSubscriberInfo by 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 Cell ID
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

Tracking

Nobody wants to be constantly monitored.

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

Very hard to stop:

- AnyTimeInterrogation
- ProvideSubscriberInfo
- ProvideSubscriberLocation
DoS

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
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
How to Intercept SMS

• 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
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?
Bad Guys Needed It So Much

• Access to payment service
• Recover passwords for email and social networks
• Online banking OTP
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, SS7 signaling, Tier 1

Requirements:
- Programming
- Mobile location
- LAC ID lookup, cell lac lookup, lac lookup, gsm geolocation, vlr lookup, cell lac lookup, vlr lac, lac cell, geolocation lookup lac, mtsds, geolocation api, lac id gam, lac id, cell lac lookup google mnc lac, cell lac mnc, cell lac database, cell lac, google map api cell lac, cell lac google, cell lac info, cell lac latitude longitude java, google map cell lac, excel vba lookup cut cell, lbs, lookup
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@vlenmail.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: Osm Geolocation, SS7 signaling, Tier1

Additional skills: lac cid lookup, cid lac lookup, lac lookup, vir geolocation, vir lookup, cell lac lookup, vir lac, lac cell, geolocation lookup lac, midsch, geolocation api, lac cid gam, lac cid, cell lookup google mcc lac, cell lac mcc, cell lac database, cell lac, google map api cell lac, cell lac google, cell lac info, cell lac latitude longitude java, google map cell lac, excel vba lookup cut cell, lbs lookup.
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@vtrimail.net
Hack border device
Today: IP Connectivity

[SHODAN search results for port 2123]

- **175.113.123.24**
  - **SK Broadband**
  - Added on 04.02.2015
  - GPRS Tunneling Protocol
  - Correct data length for version 1
  - Version: 1
  - Flags: XXX1.0010
  - Type: 2 (Echo response)
  - Length: 6
  - Data: \x0c\x00\x00\x00\x0e\x02

- **121.173.248.253**
  - **Korea Telecom**
  - Added on 04.02.2015
  - GPRS Tunneling Protocol
  - Correct data length for version 1
  - Version: 1
  - Flags: XXX1.0010
  - Type: 2 (Echo response)
  - Length: 6
  - Data: \x0c\x00\x00\x00\x0e\x03

- **120.199.138.55**
  - **China Mobile**
  - Added on 04.02.2015
  - GPRS Tunneling Protocol
  - Correct data length for version 1
Misconfiguration Example

Open Telnet, no password

Critical

---

Zero day vulnerability, ZTE ZORG Software Version ZOR14.04.10.01.003

All right reserved (1997-2007) *
Without the owner’s prior written consent, *
no decompila and reverse-engineering shall be allowed *

<ORANGE-GCSN>
Research Updates

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

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

Dmitry Kurbatov
dkurbatov@ptsecurity.com