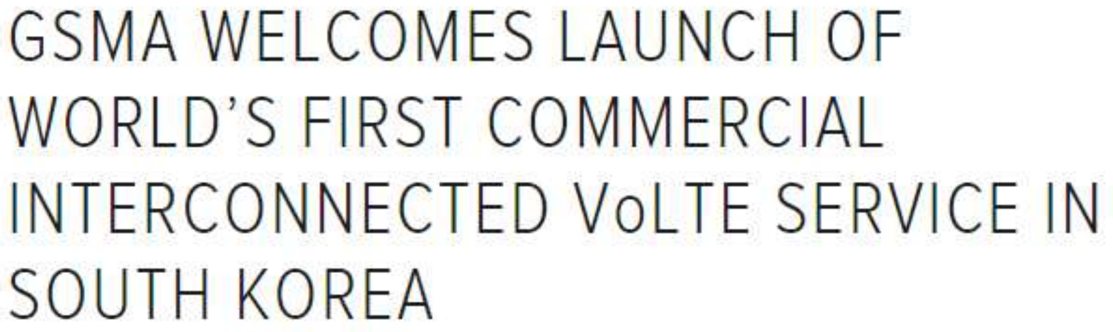
Hacking mobile network via SS7: interception, shadowing and more

Dmitry Kurbatov

Security specialist

Positive Research

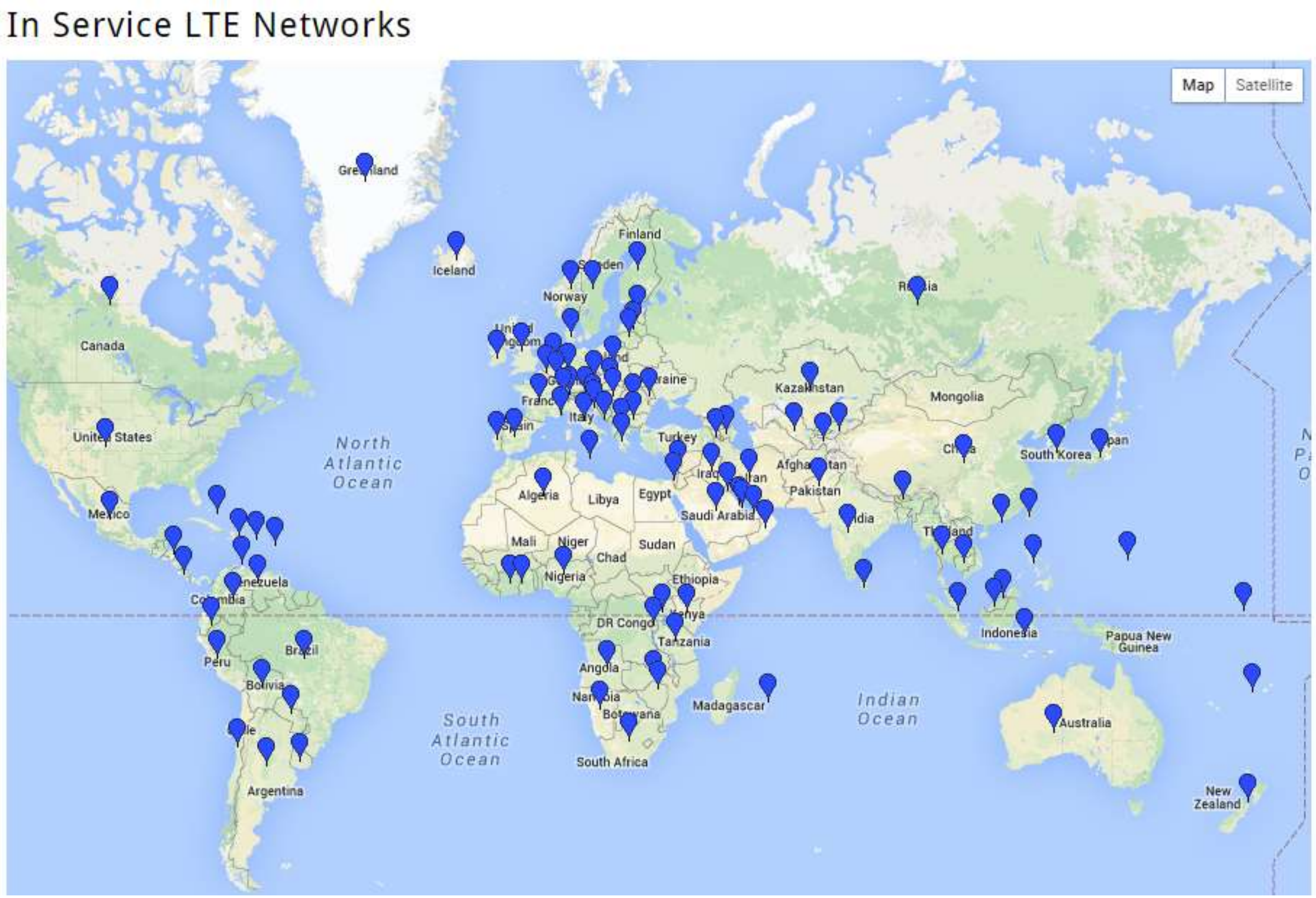
Korea is an LTE country



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

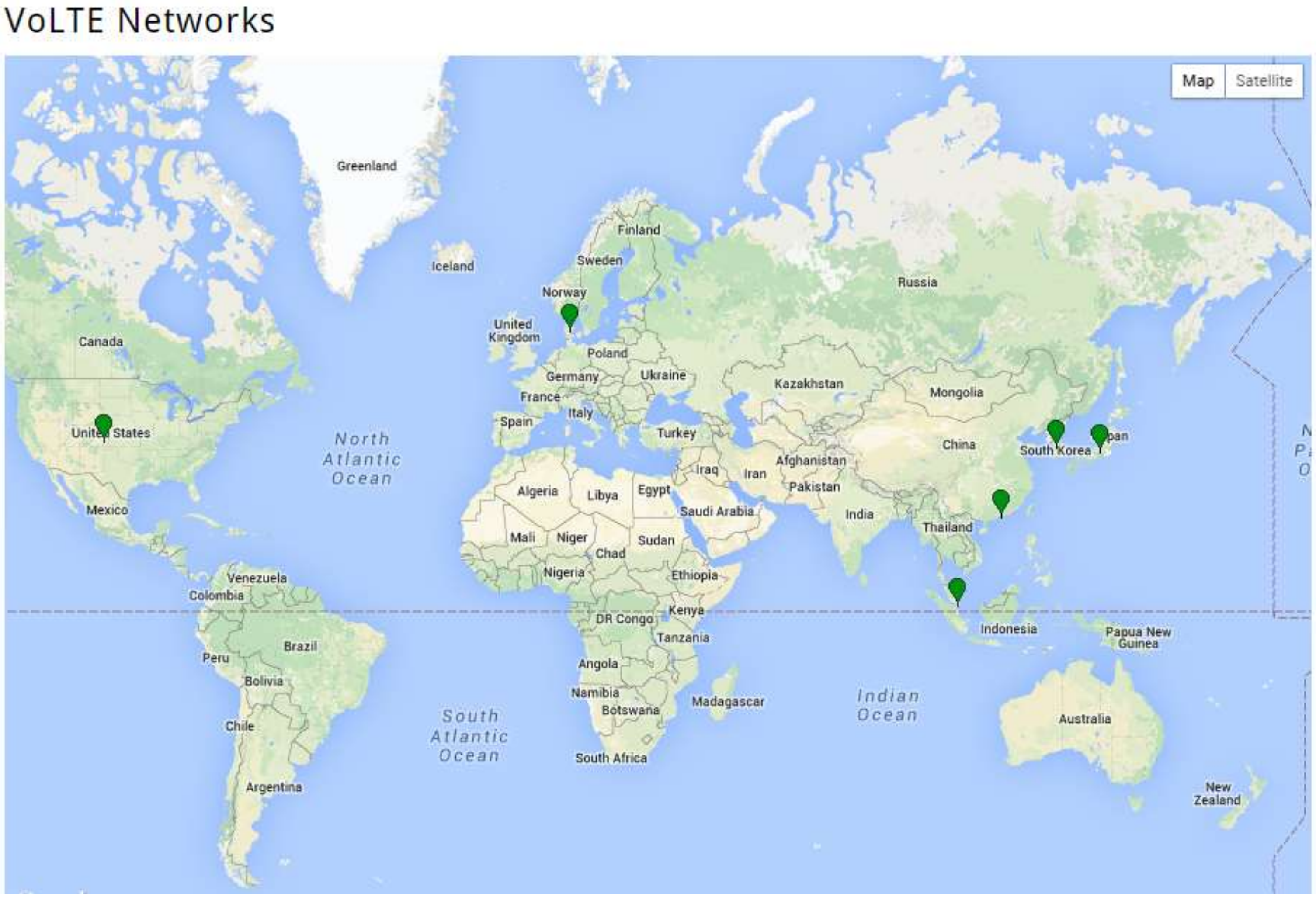
http://www.gsma.com/newsroom/press-release/gsma-welcomes-launch-of-worlds-first-commercial-interconnected-volte-service-in-south-korea/

In Service LTE Networks



In Service LTE Networks

VoLTE Networks



VoLTE Networks

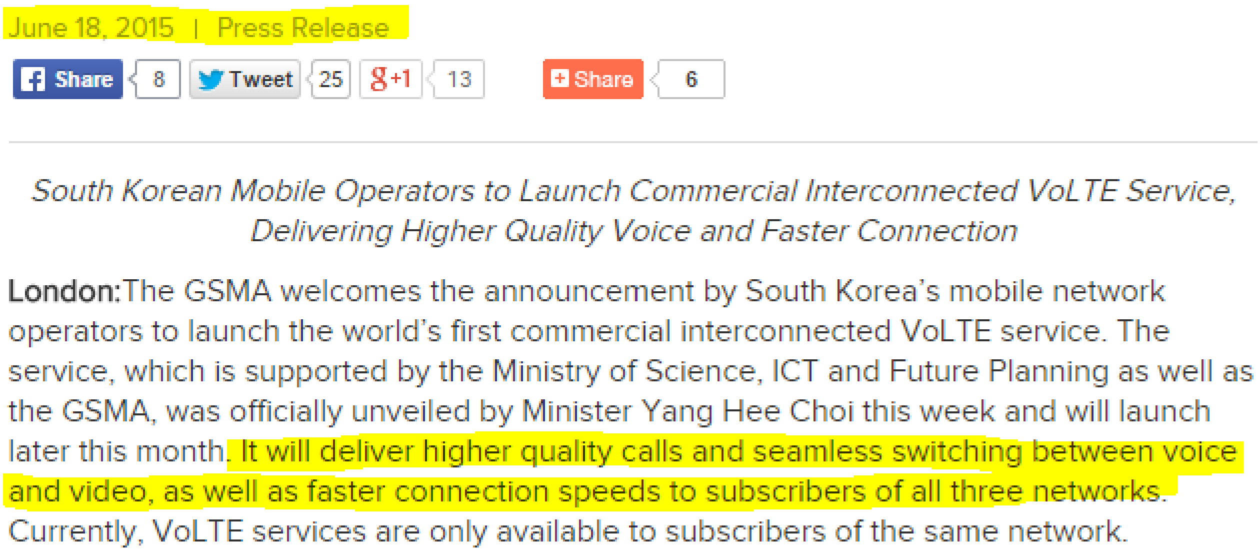
http://ltemaps.org/

The rest of the world performs handover

LTE only for web browsing

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

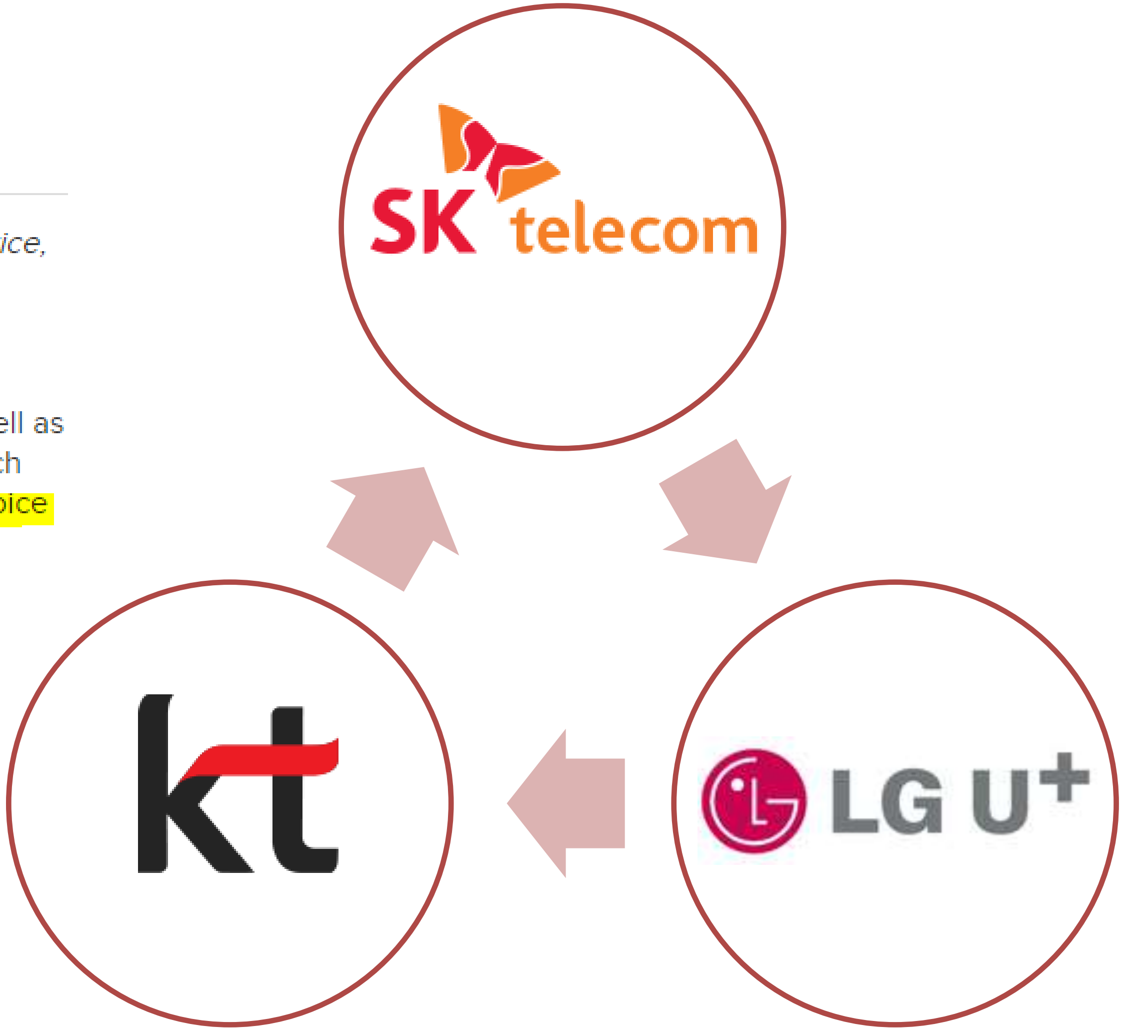
INTERCONNECTED VoLTE



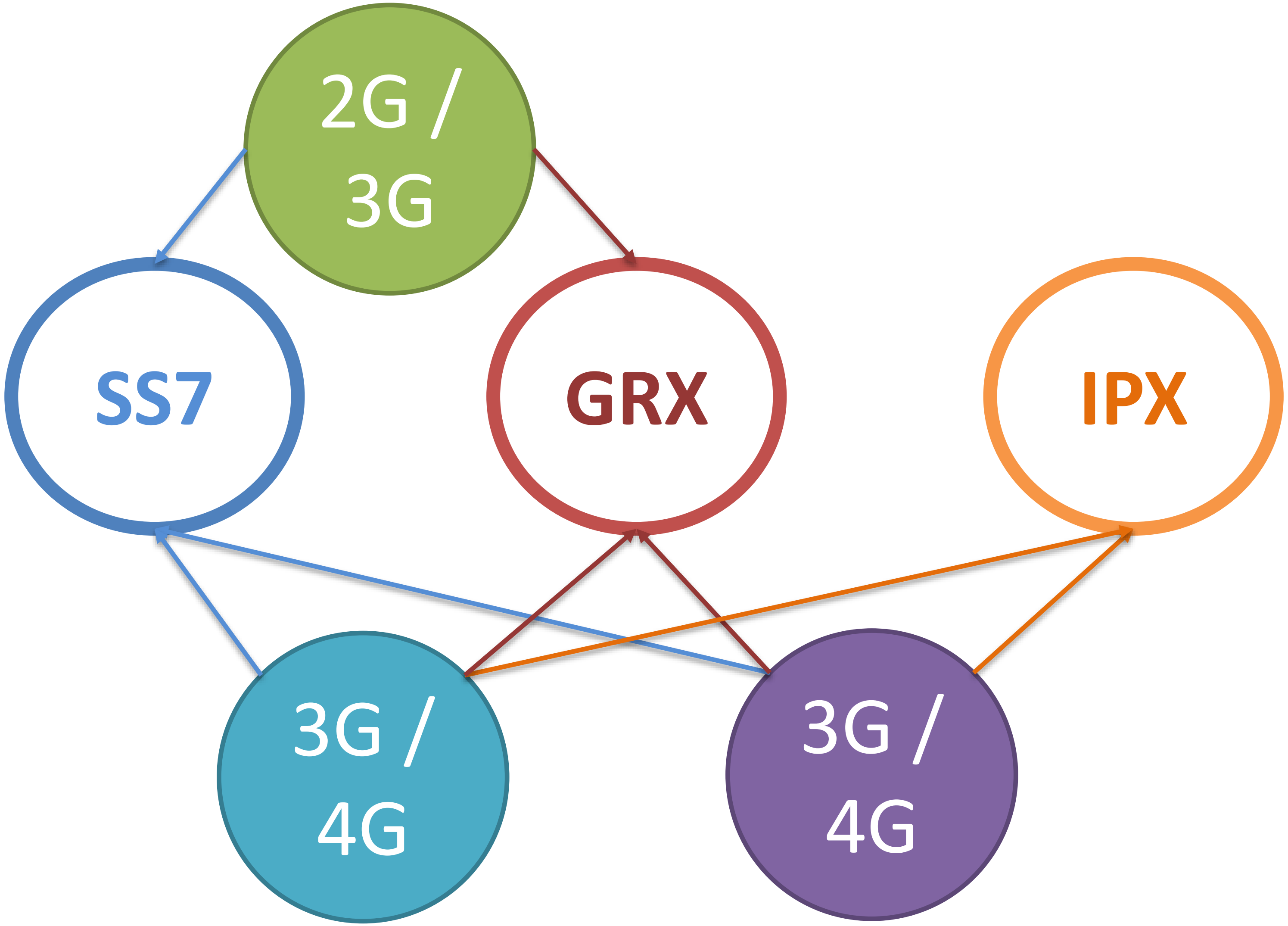
June 18, 2015 | Press Release

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

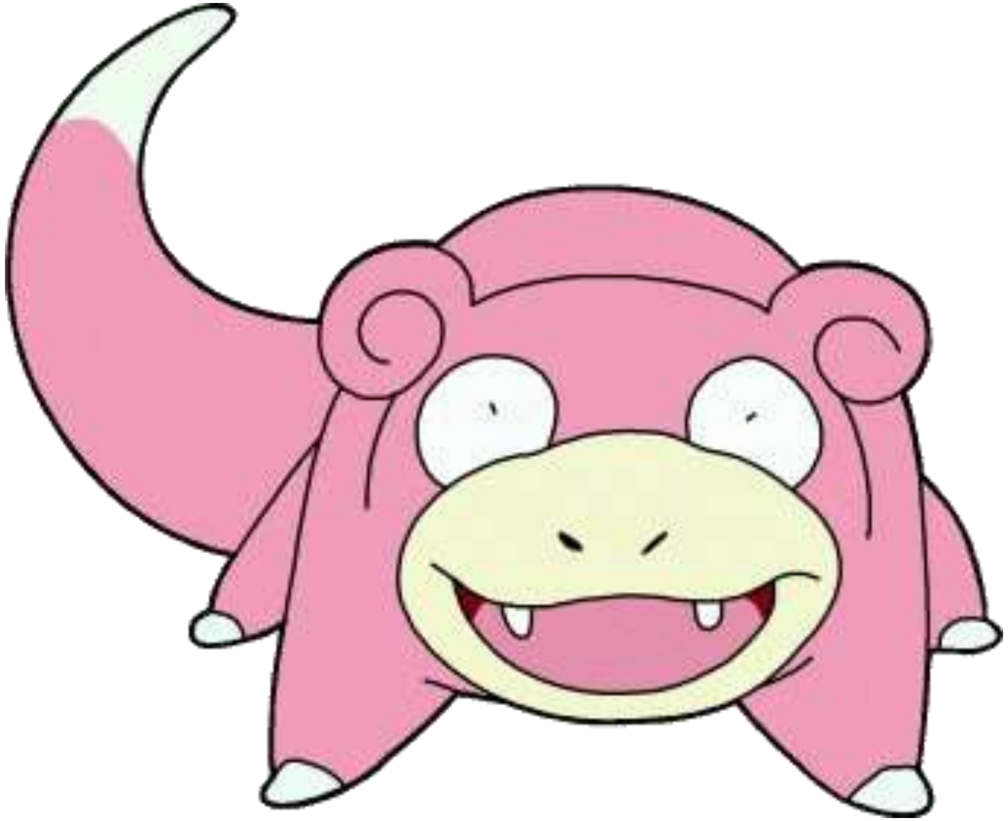
London: The GSMA welcomes the announcement by South Korea's mobile network operators to launch the world's first commercial interconnected VoLTE service. The service, which is supported by the Ministry of Science, ICT and Future Planning as well as the GSMA, was officially unveiled by Minister Yang Hee 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.

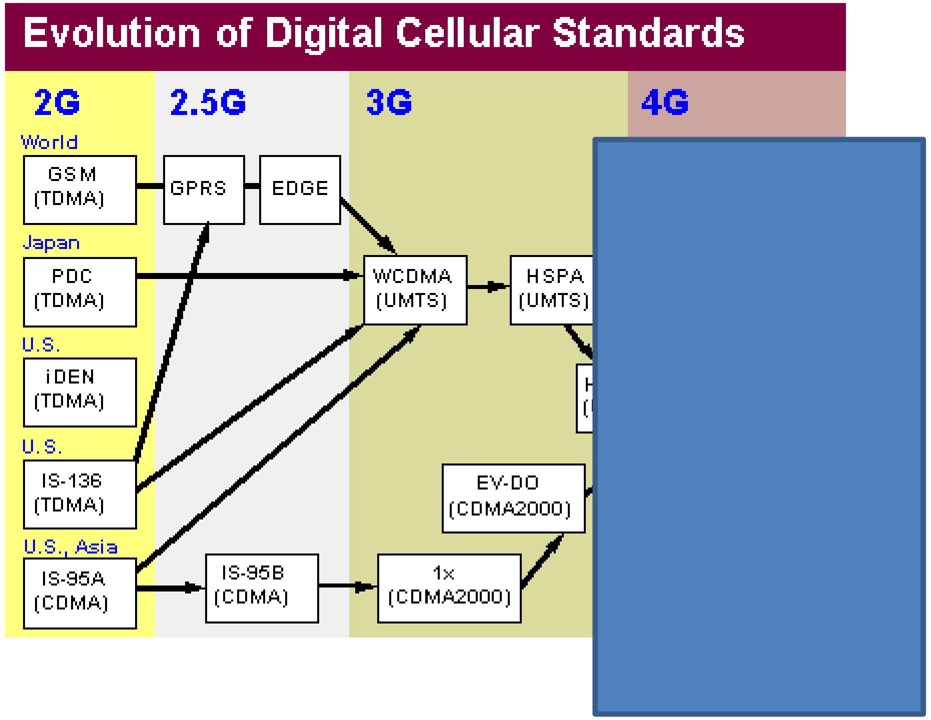


Interconnect / roaming

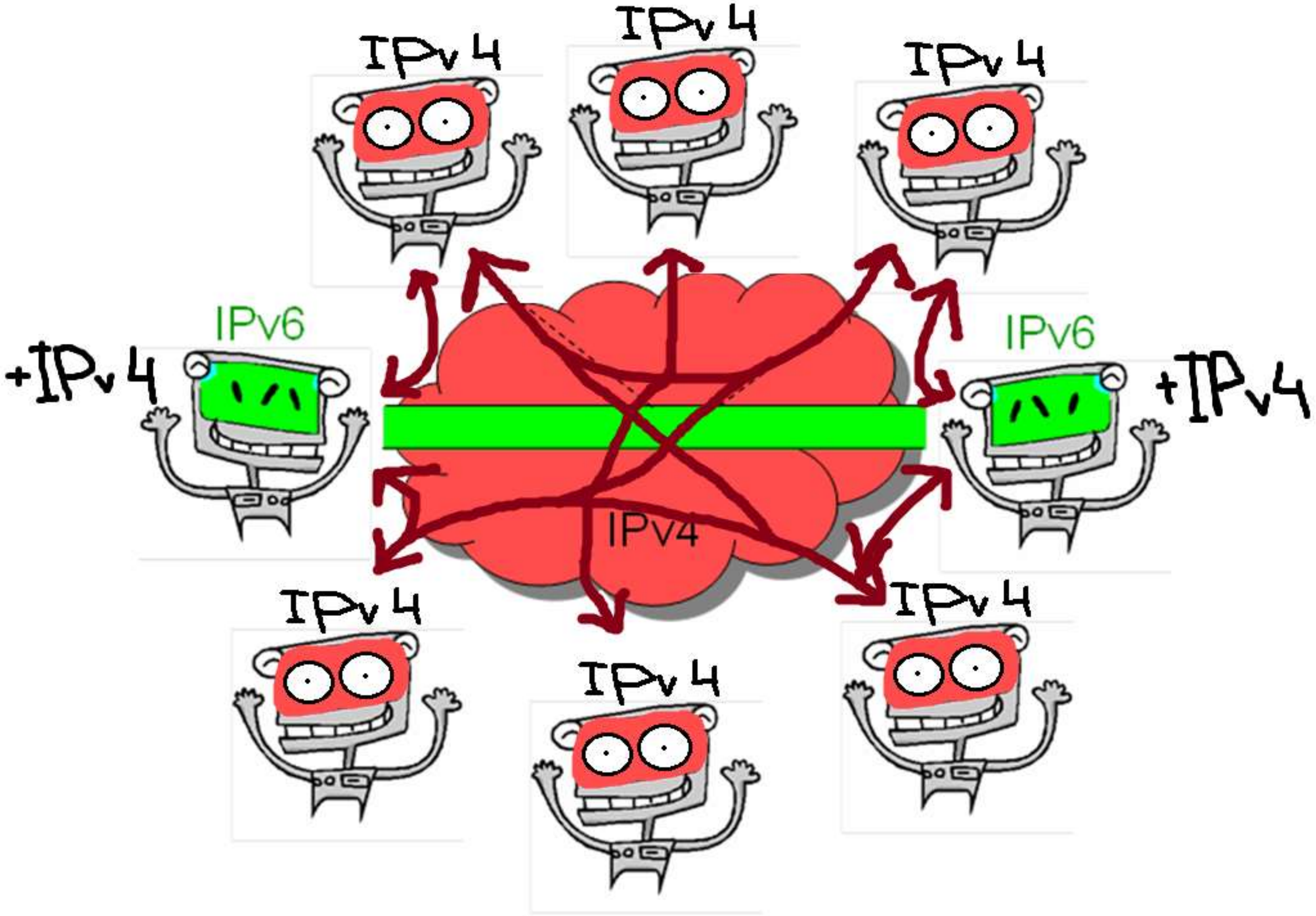


The rest of the world



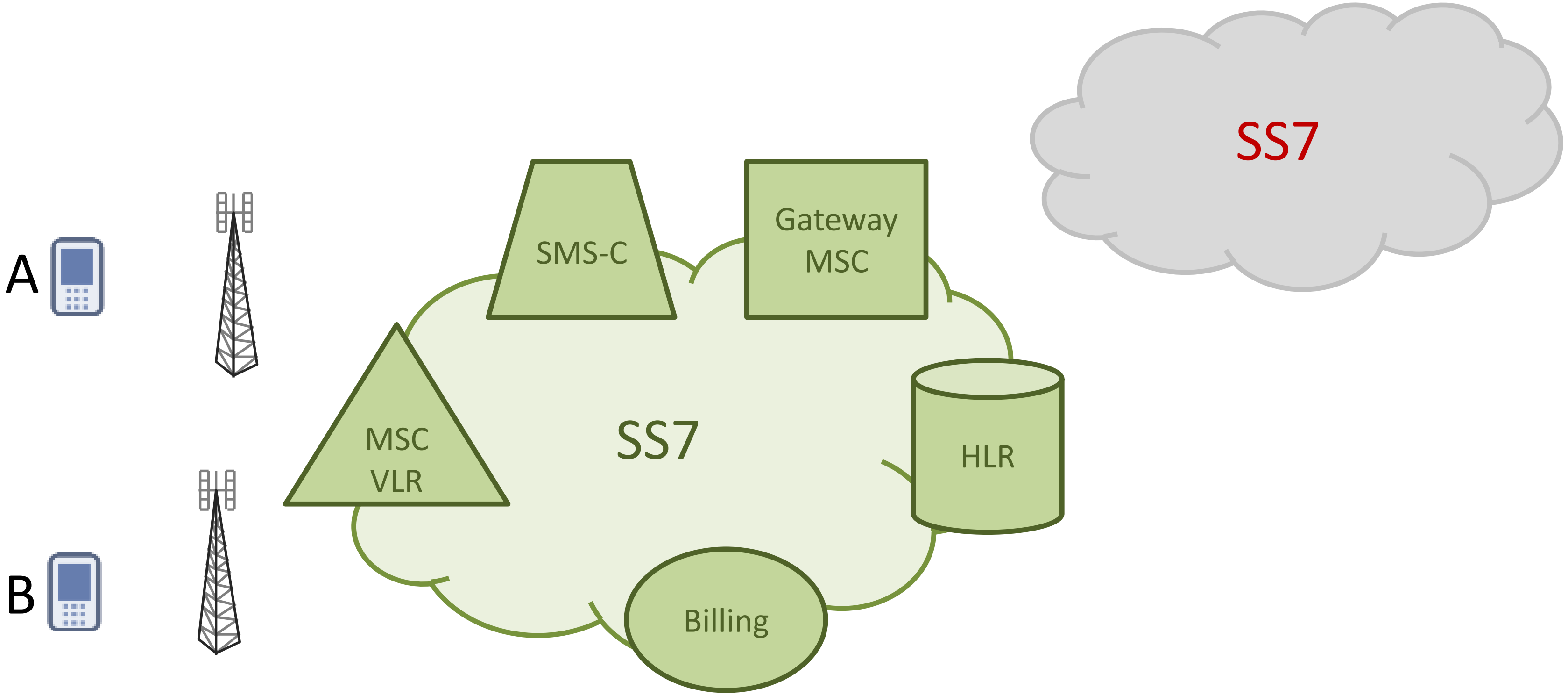


Kind of IPv4 vs IPv6 dilemma



SS7 is still most used interconnect/ roaming network

Mobility
Call control
Billing
Crypto



2014 - year of SS7 security issues

HACKITO ERGO SUM

phdIV Positive Hack Days

31C3 a new dawn 31st Chaos Communication Congress

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

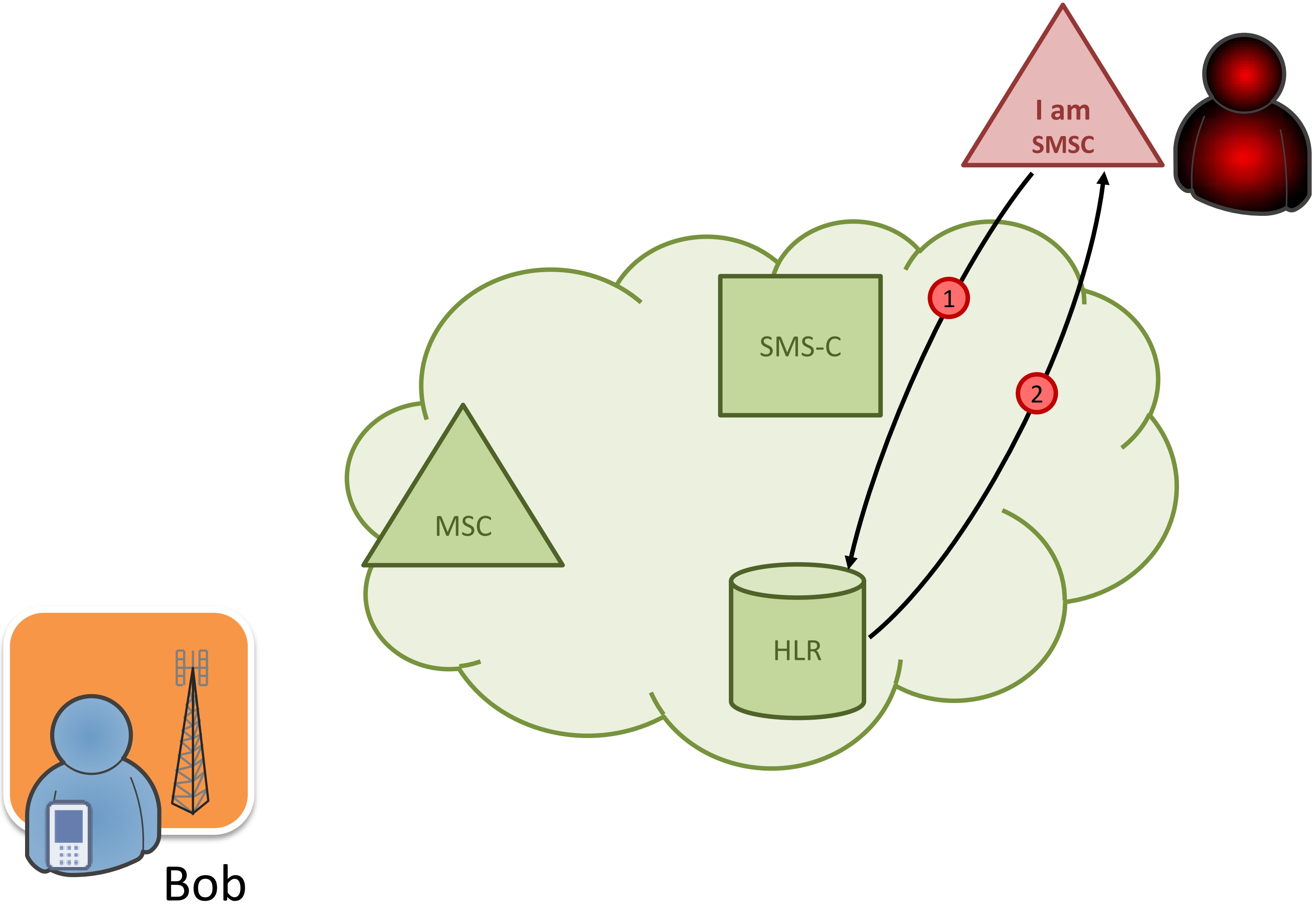
- Listen to calls, intercept short messages and internet traffic

Threats to Operator

Threats to IoT

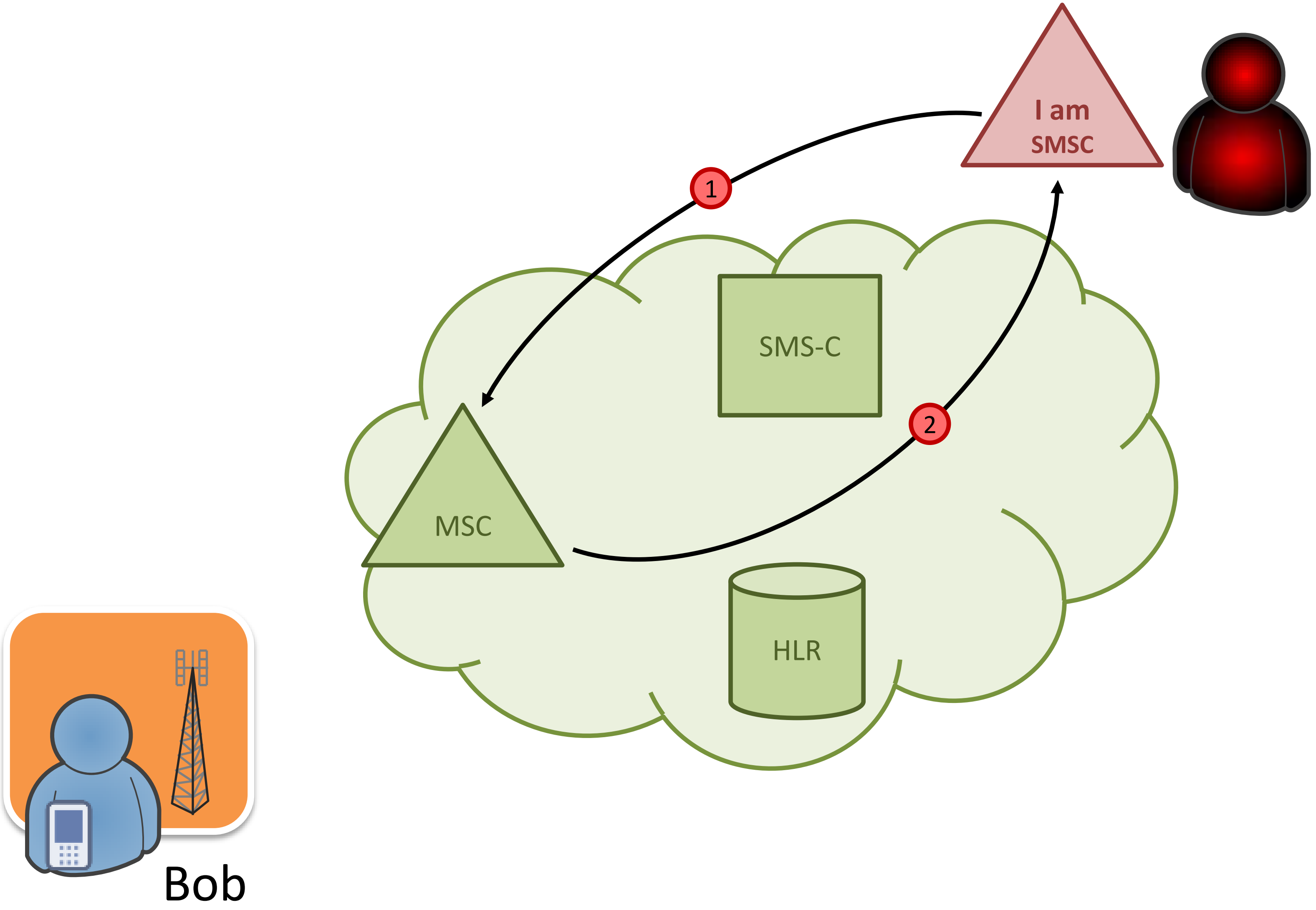
Tracking

Common Step 0 for Any Attack



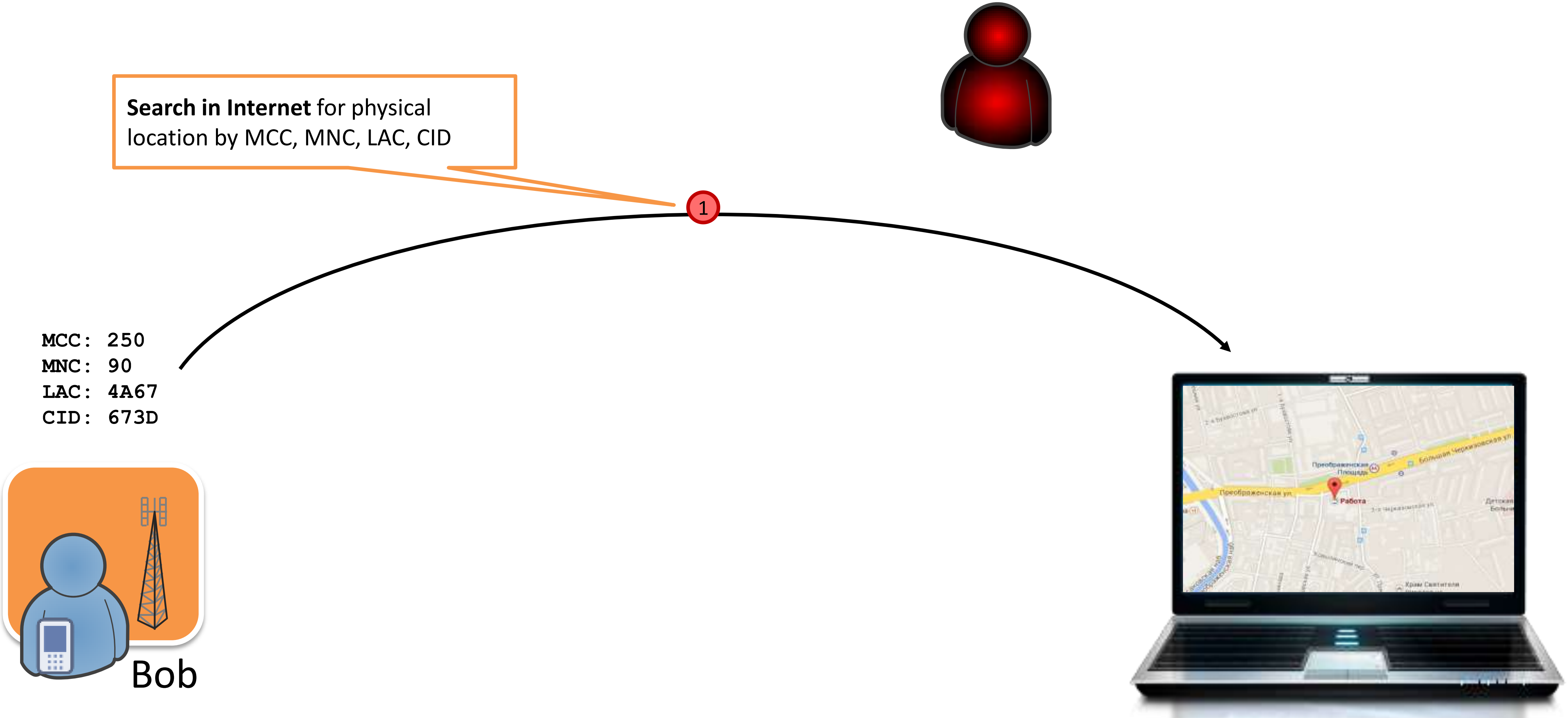
1. Attacker sends request SendRoutingInfoForSM addressing MAP message by MSISDN
2. HLR replies with:
   - own address
   - serving MSC address
   - IMSI

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

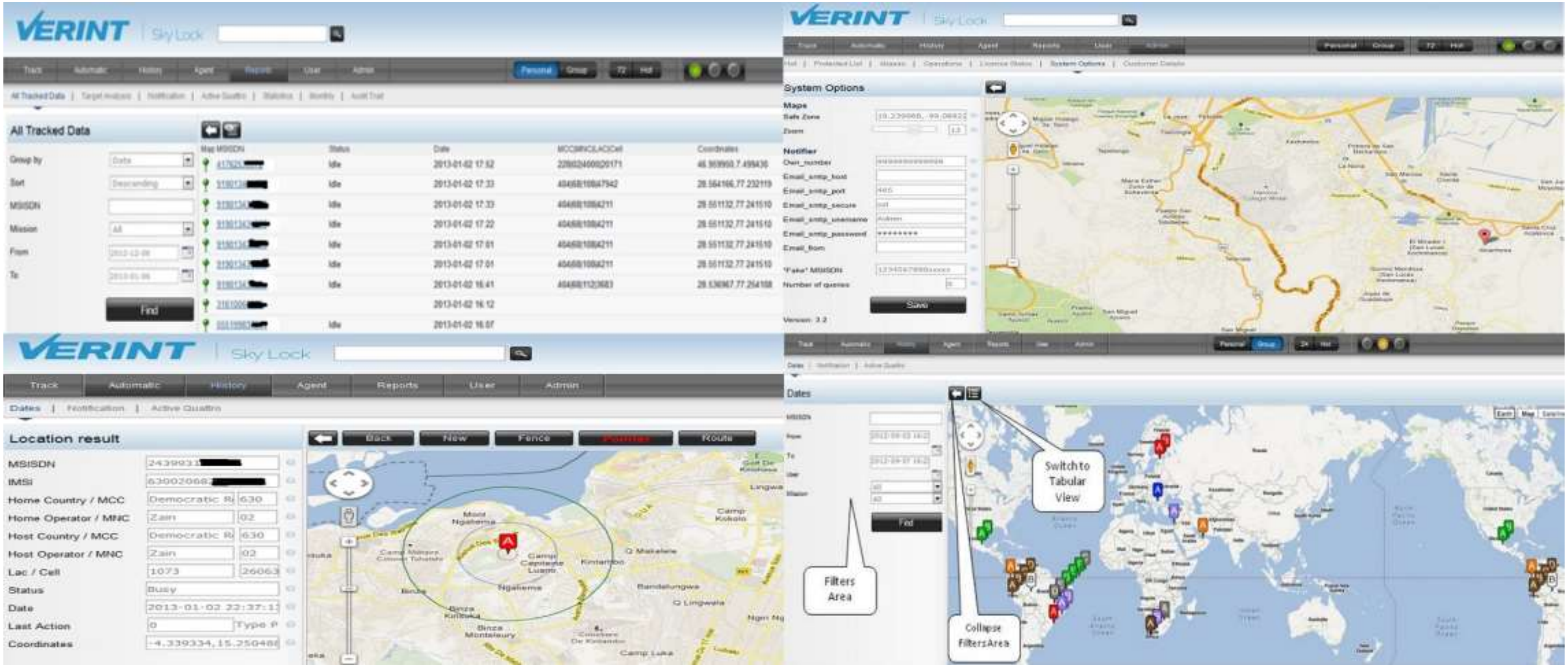
Get Location…



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



All Tracked Data

Group by: Date
Sort: Descending
MSISDN:
Mission: All
From: 2012-12-06
To: 2013-01-06

Map MSISDN	Status	Date	MCC|MNC|LAC|Cell	Coordinates
41762[redacted]	Idle	2013-01-02 17:52	22802400020171	46.959950,7.499436
9190138[redacted]	Idle	2013-01-02 17:33	40468|10847942	28.564166,77.232119
919013[redacted]	Idle	2013-01-02 17:33	40468|1084211	28.551132,77.241510
919013[redacted]	Idle	2013-01-02 17:22	40468|1084211	28.551132,77.241510
919013[redacted]	Idle	2013-01-02 17:01	40468|1084211	28.551132,77.241510
919013[redacted]	Idle	2013-01-02 17:01	40468|1084211	28.551132,77.241510
919013[redacted]	Idle	2013-01-02 16:41	40468|1123683	28.536967,77.254108
2161006[redacted]		2013-01-02 16:12		
5531998[redacted]	Idle	2013-01-02 16:07		

System Options

Maps
Safe Zone: 19.229960, -99.08822
Zoom: 12

Notifier
Own_number: 4499999999999
Email_smtp_host:
Email_smtp_port: 465
Email_smtp_secure: ssl
Email_smtp_username: Admin
Email_smtp_password: ********
Email_from:

"Fake" MSISDN: 1234567890xxxxx
Number of queries: 5

Version: 3.2

Location result

MSISDN	2439931[redacted]	
IMSI	63002068[redacted]	
Home Country / MCC	Democratic R	630
Home Operator / MNC	Zain	02
Host Country / MCC	Democratic R	630
Host Operator / MNC	Zain	02
Lac / Cell	1073	26063
Status	Busy	
Date	2013-01-02 22:37:1	
Last Action	0	Type P
Coordinates	-4.339334,15.25048	

Dates

MSISDN:
From: 2012-09-03 16:22
To: 2012-09-07 16:22
User: All
Mission: All

http://s3.documentcloud.org/documents/1275167/skylock-product-description-2013.pdf

Tracking

Nobody wants to be constantly monitored.

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

Very hard to stop:

- AnyTimeInterrogation
- ProvideSubscriberInfo
- ProvideSubscriberLocation

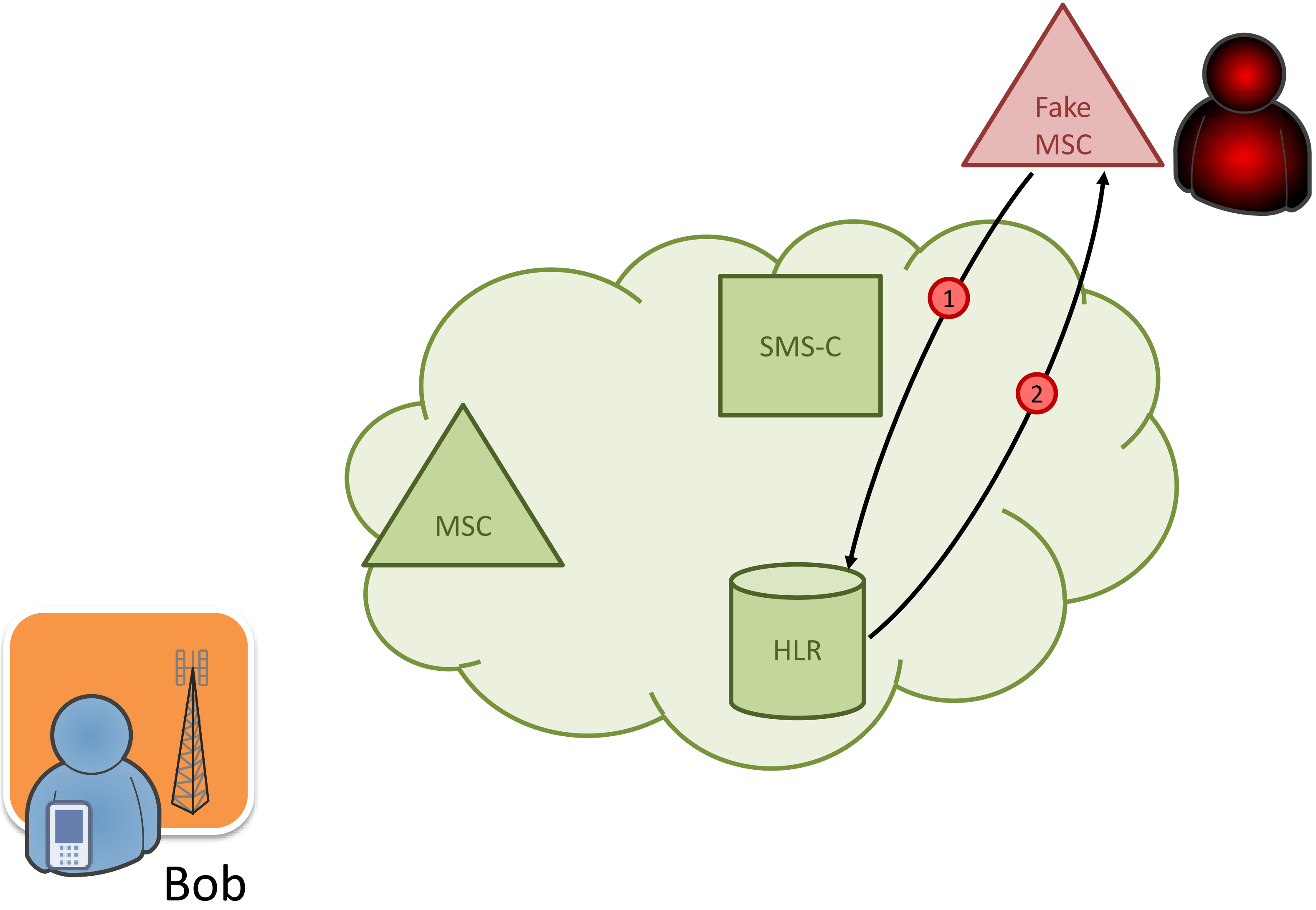
DoS

To make someone unavailable

To stop data leakage

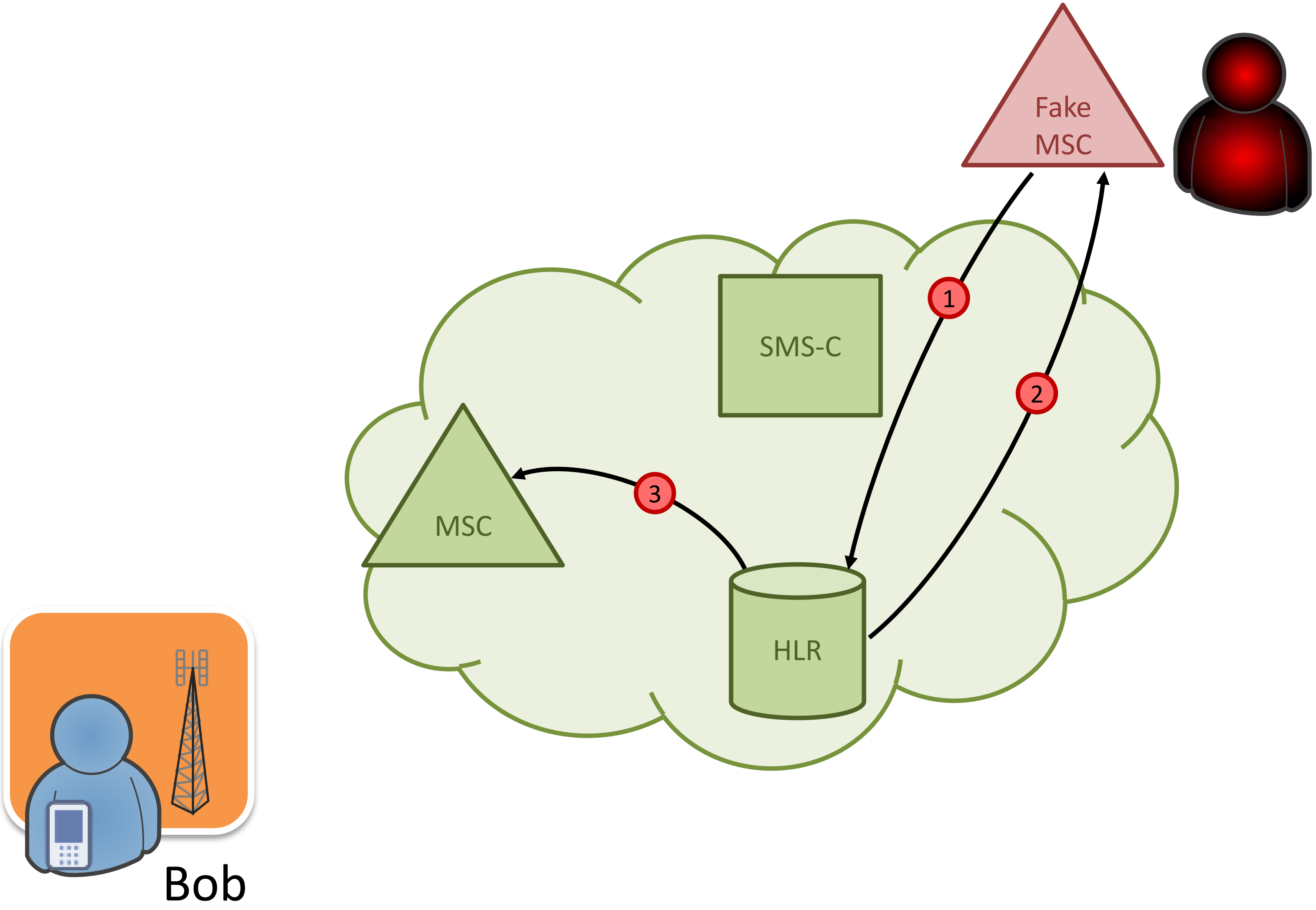
What else?

Common Step 0 for Any Attack



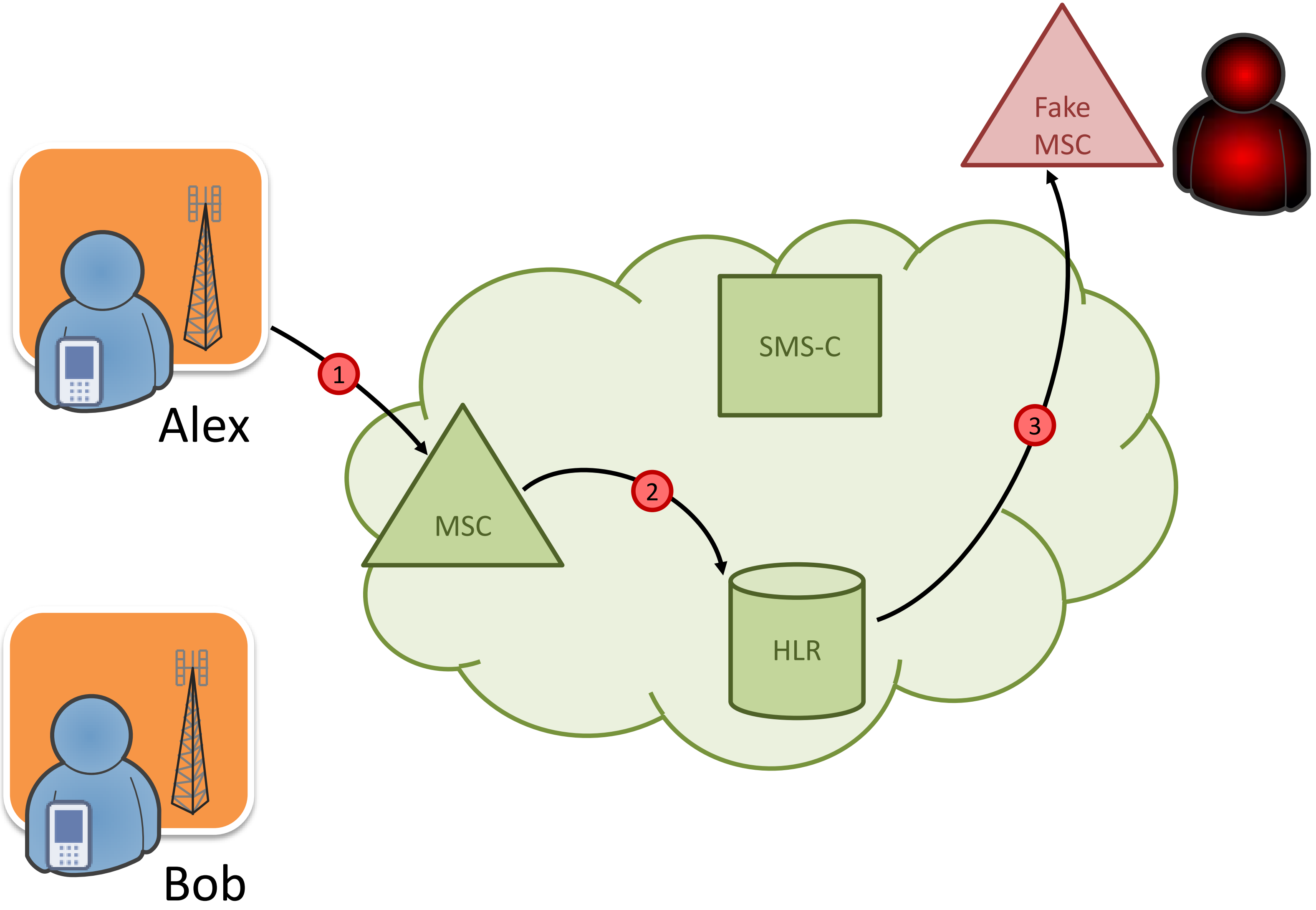
1. Attacker sends request SendRoutingInfoForSM addressing MAP message by MSISDN
2. HLR replies with:
   - own address
   - serving MSC address
   - IMSI

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

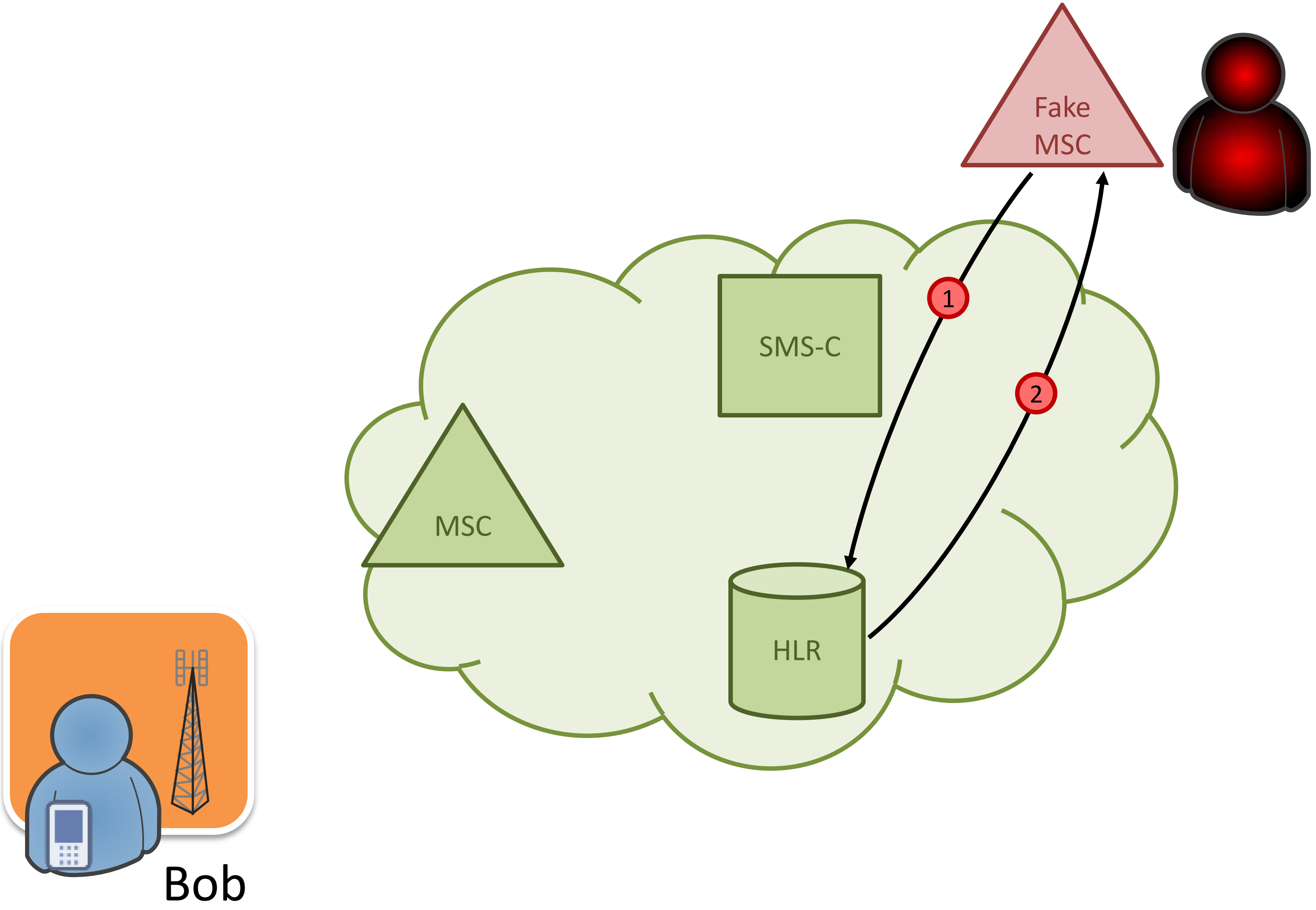
demo

Interception

How to Intercept SMS

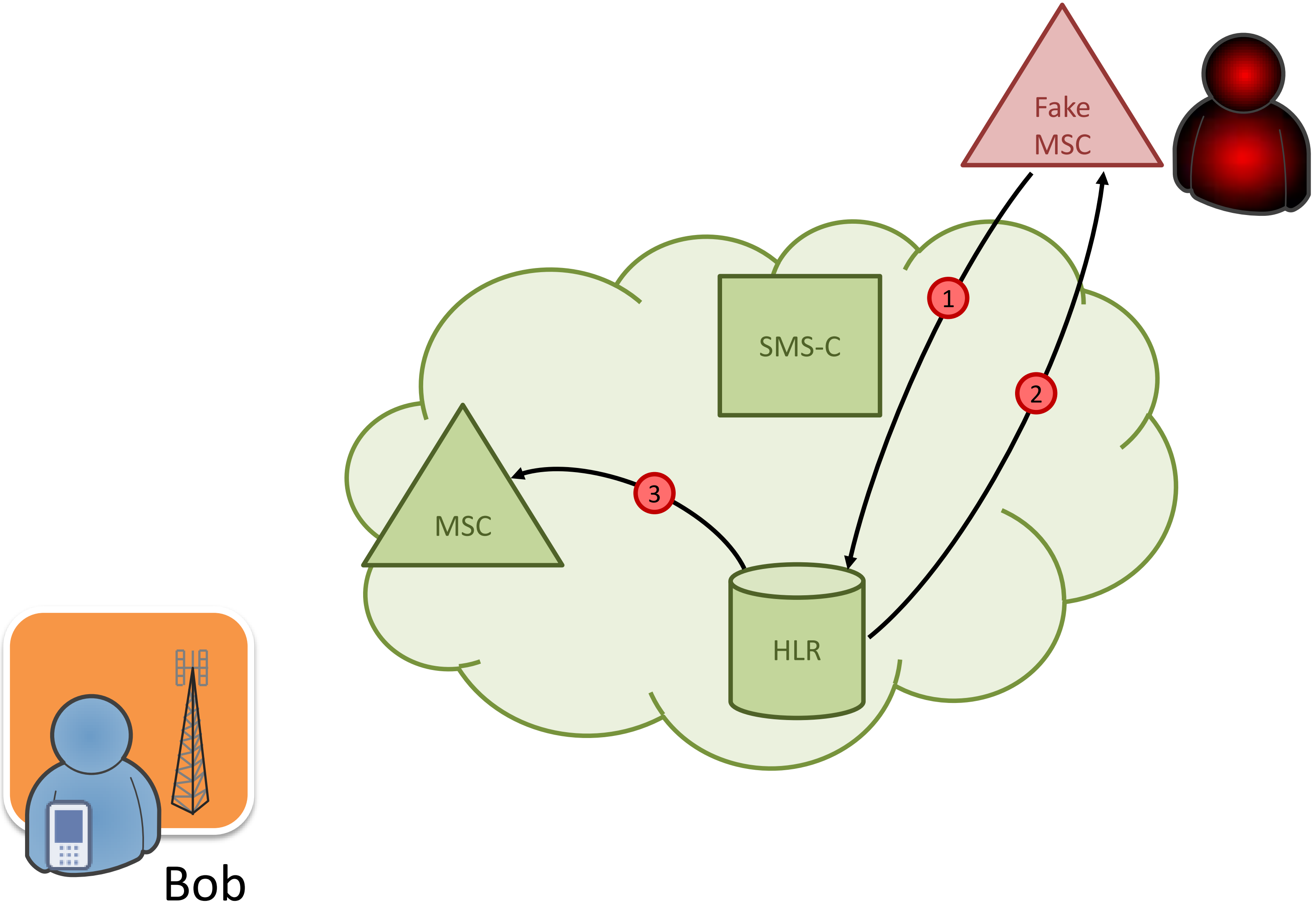
- A virus on a smartphone – and what if a certain subscriber is a target? How to infect him particularly?
- Reissue SIM? It works only once.
- Radio signal interception (GSM A5/1)? You need to be nearby.
- Via SS7 network

Common Step 0 for Any Attack



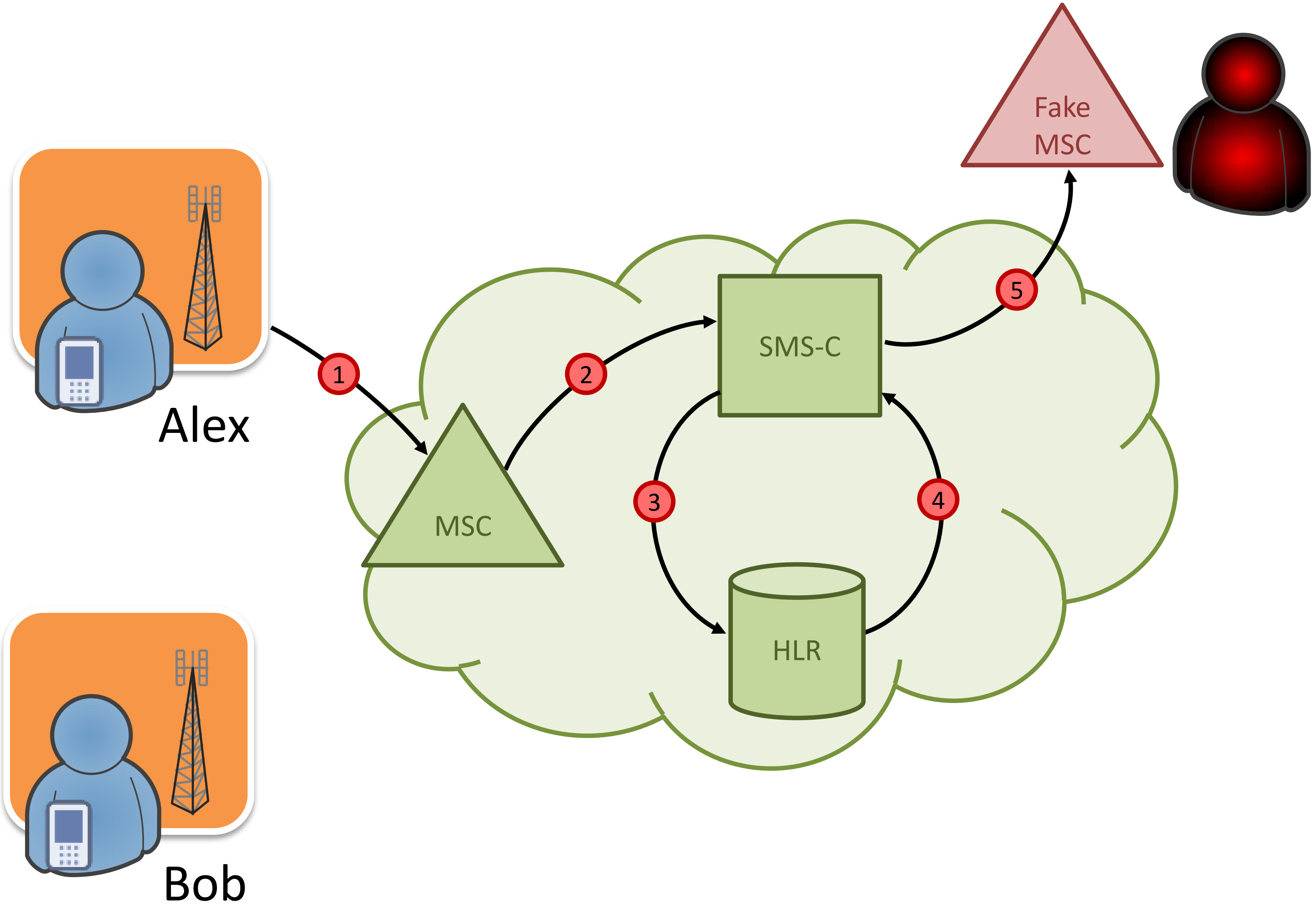
1. Attacker sends request SendRoutingInfoForSM addressing MAP message by MSISDN
2. HLR replies with:
   - own address
   - serving MSC address
   - IMSI

SMS Interception. Step 1



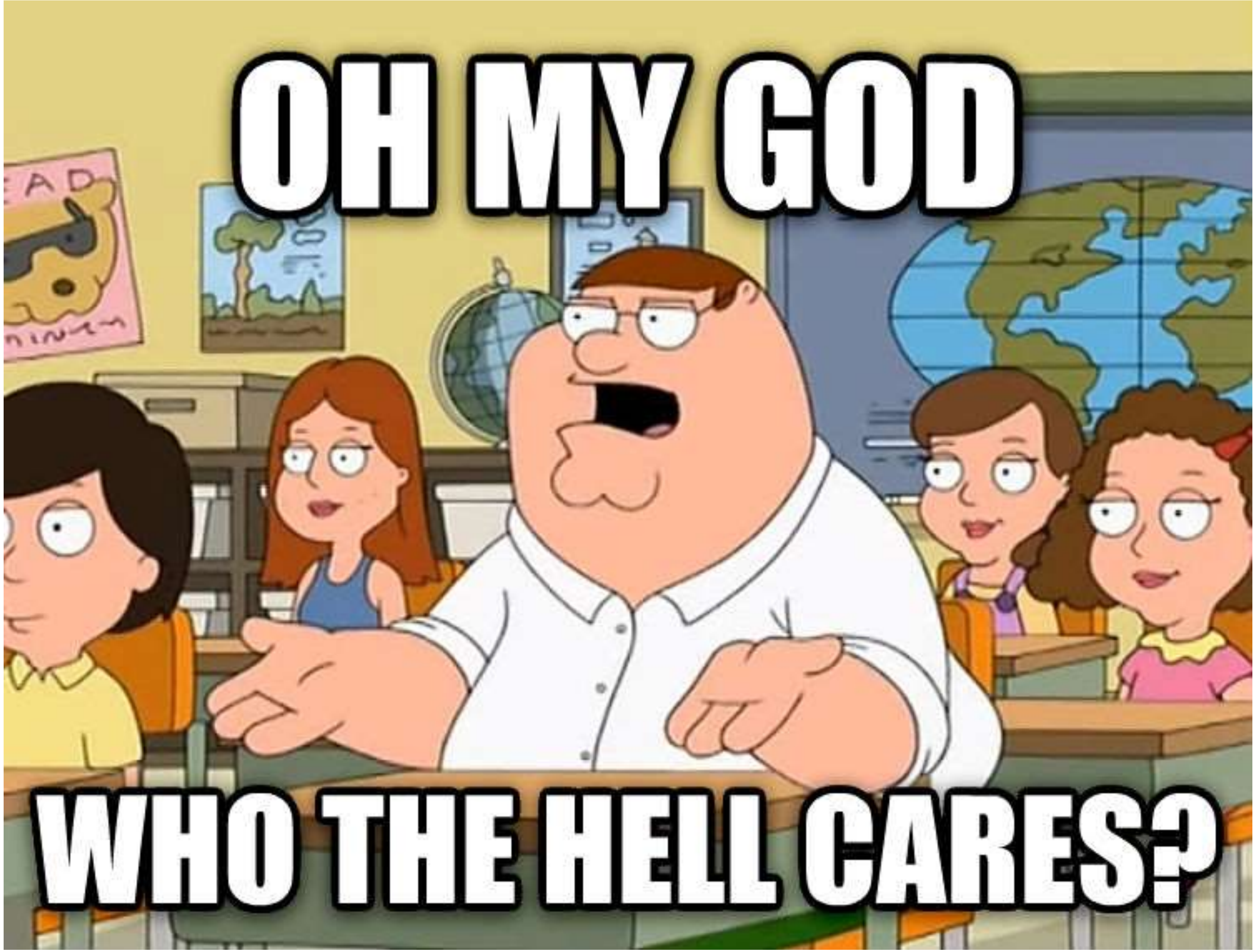
1. Attacker registers Bob on the fake MSC
2. HLR sets up new location for Bob
3. HLR asks real MSC to release a memory

SMS Interception. Step 2



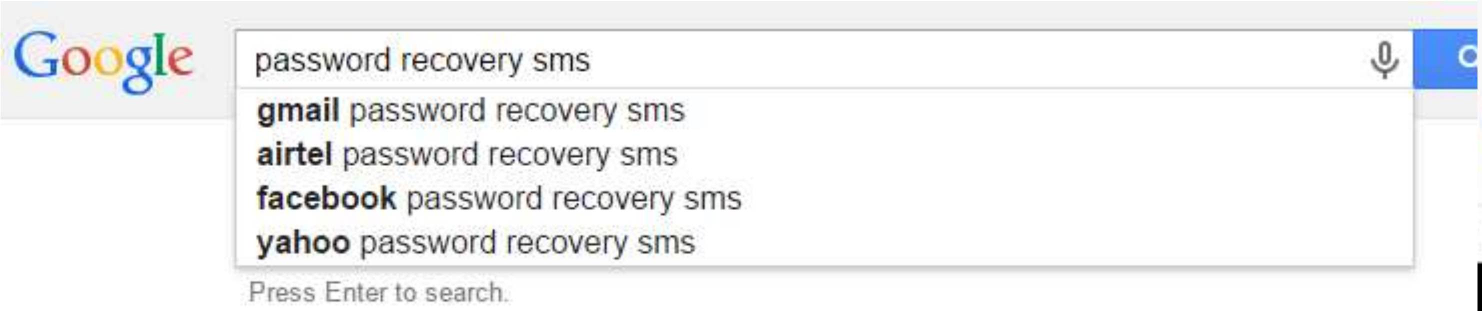
1. Alex sends SMS to Bob
2. MSC translates the SMS to SMS-C
3. SMS-C requests HLR for Bob`s location
4. HLR replies with a fake MSC address
5. SMS-C translates SMS to the fake MSC

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

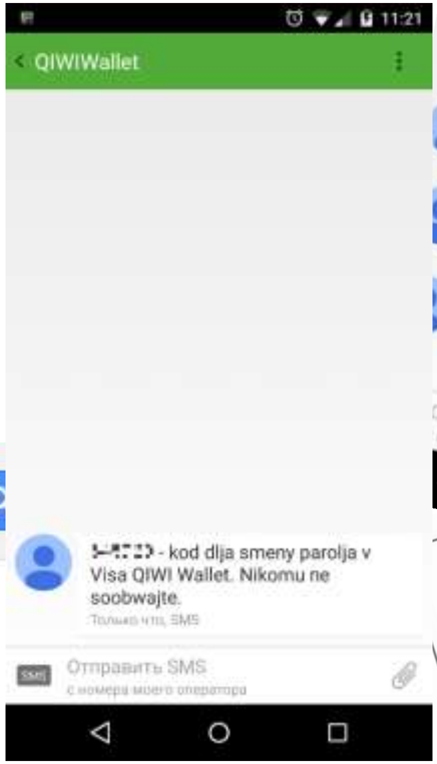


Google

password recovery sms

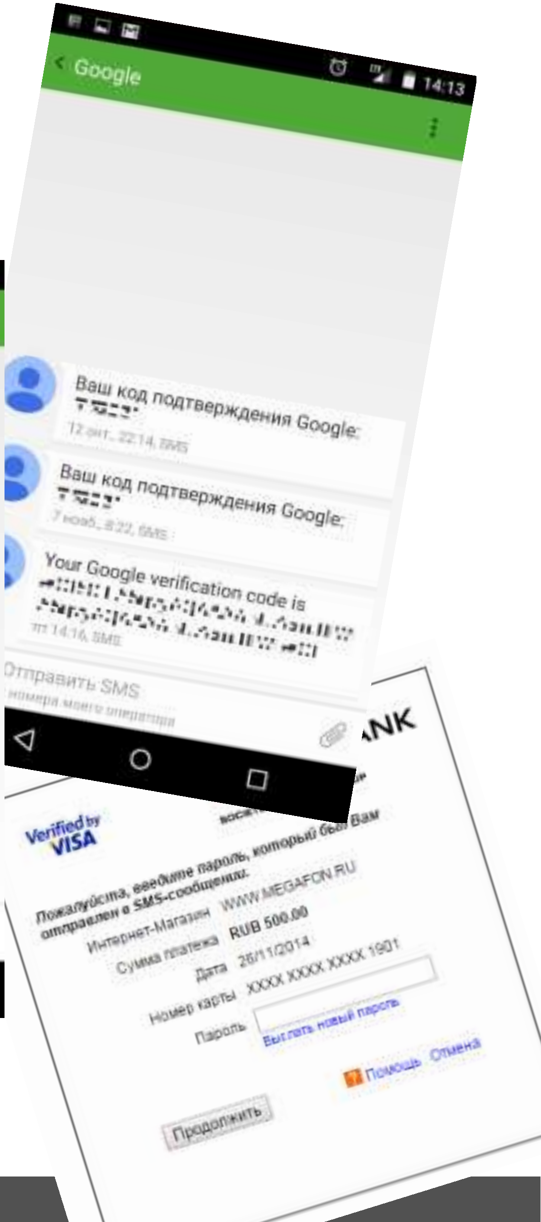
gmail password recovery sms
airtel password recovery sms
facebook password recovery sms
yahoo password recovery sms

Press Enter to search.



[redacted] - kod dlja smeny parolja v Visa QIWI Wallet. Nikomu ne soobwajte.
Только что, SMS

Отправить SMS
с номера моего оператора



Ваш код подтверждения Google: [redacted]
12 окт., 22:14, SMS

Ваш код подтверждения Google: [redacted]
7 нояб., 8:22, SMS

Your Google verification code is [redacted]
пт 14:16, SMS

Отправить SMS
с номера моего оператора

Пожалуйста, введите пароль, который был Вам отправлен в SMS-сообщении.

Интернет-Магазин WWW.MEGAFON.RU
Сумма платежа RUB 500.00
Дата 26/11/2014
Номер карты XXXX XXXX XXXX 1901
Пароль
Выслать новый пароль

Помощь Отмена

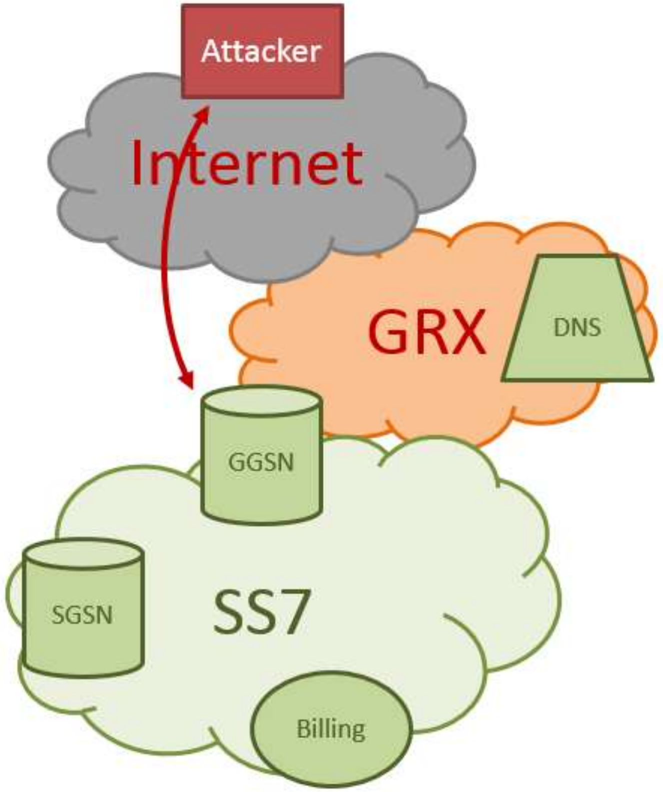
Продолжить

How to Get Into SS7

How They Can Get Into SS7

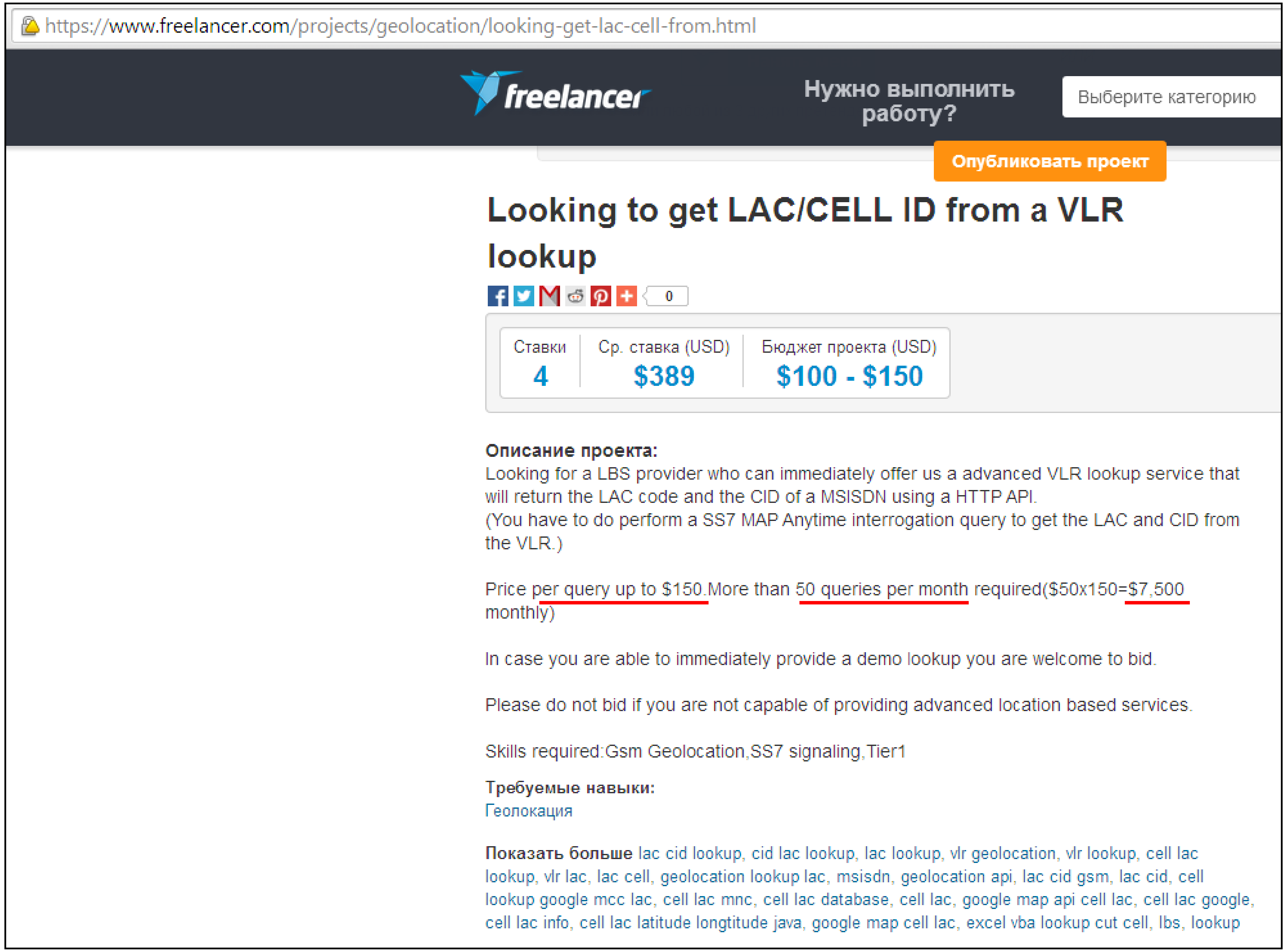
Legal with license
Semi legal without

Find a guy



Hack border device

Find a Guy



https://www.freelancer.com/projects/geolocation/looking-get-lac-cell-from.html

Looking to get LAC/CELL ID from a VLR lookup

Ставки	Ср. ставка (USD)	Бюджет проекта (USD)
4	$389	$100 - $150

Описание проекта:
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 MSISDN using a HTTP API.
(You have to do perform a SS7 MAP Anytime interrogation query to get the LAC and CID from the VLR.)

Price per query up to $150.More than 50 queries per month required($50x150=$7,500 monthly)

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

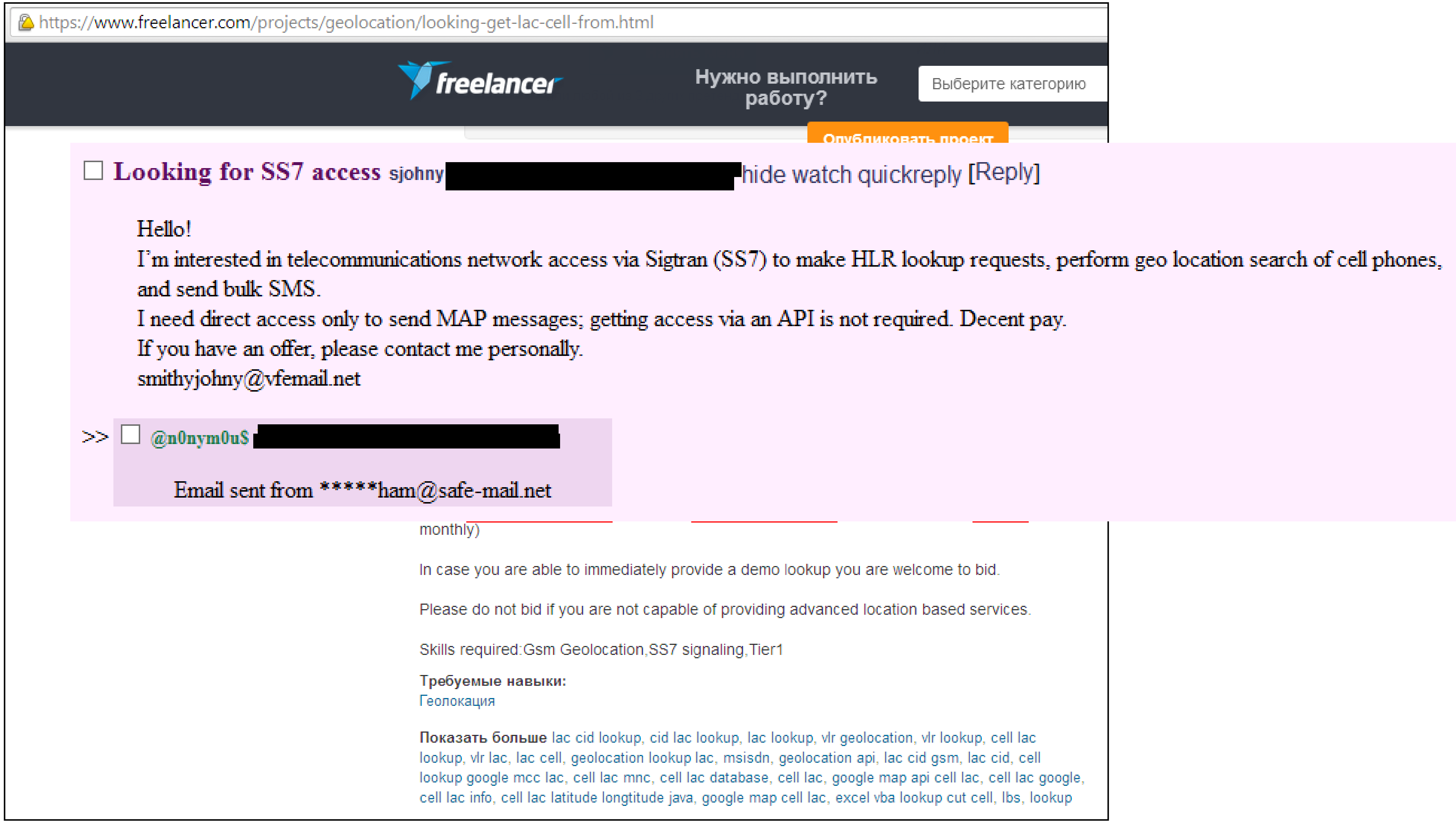
Please do not bid if you are not capable of providing advanced location based services.

Skills required:Gsm Geolocation,SS7 signaling,Tier1

Требуемые навыки:
Геолокация

Показать больше lac cid lookup, cid lac lookup, lac lookup, vlr geolocation, vlr lookup, cell lac lookup, vlr lac, lac cell, geolocation lookup lac, msisdn, geolocation api, lac cid gsm, lac cid, cell lookup google mcc lac, cell lac mnc, cell lac database, cell lac, google map api cell lac, cell lac google, cell lac info, cell lac latitude longtitude java, google map cell lac, excel vba lookup cut cell, lbs, lookup

Find a Guy



https://www.freelancer.com/projects/geolocation/looking-get-lac-cell-from.html
freelancer
Нужно выполнить работу?
Выберите категорию
Опубликовать проект

□ **Looking for SS7 access** sjohny [redacted] hide watch quickreply [Reply]

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@vfemail.net

>> □ @n0nym0u$ [redacted]

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

monthly)

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

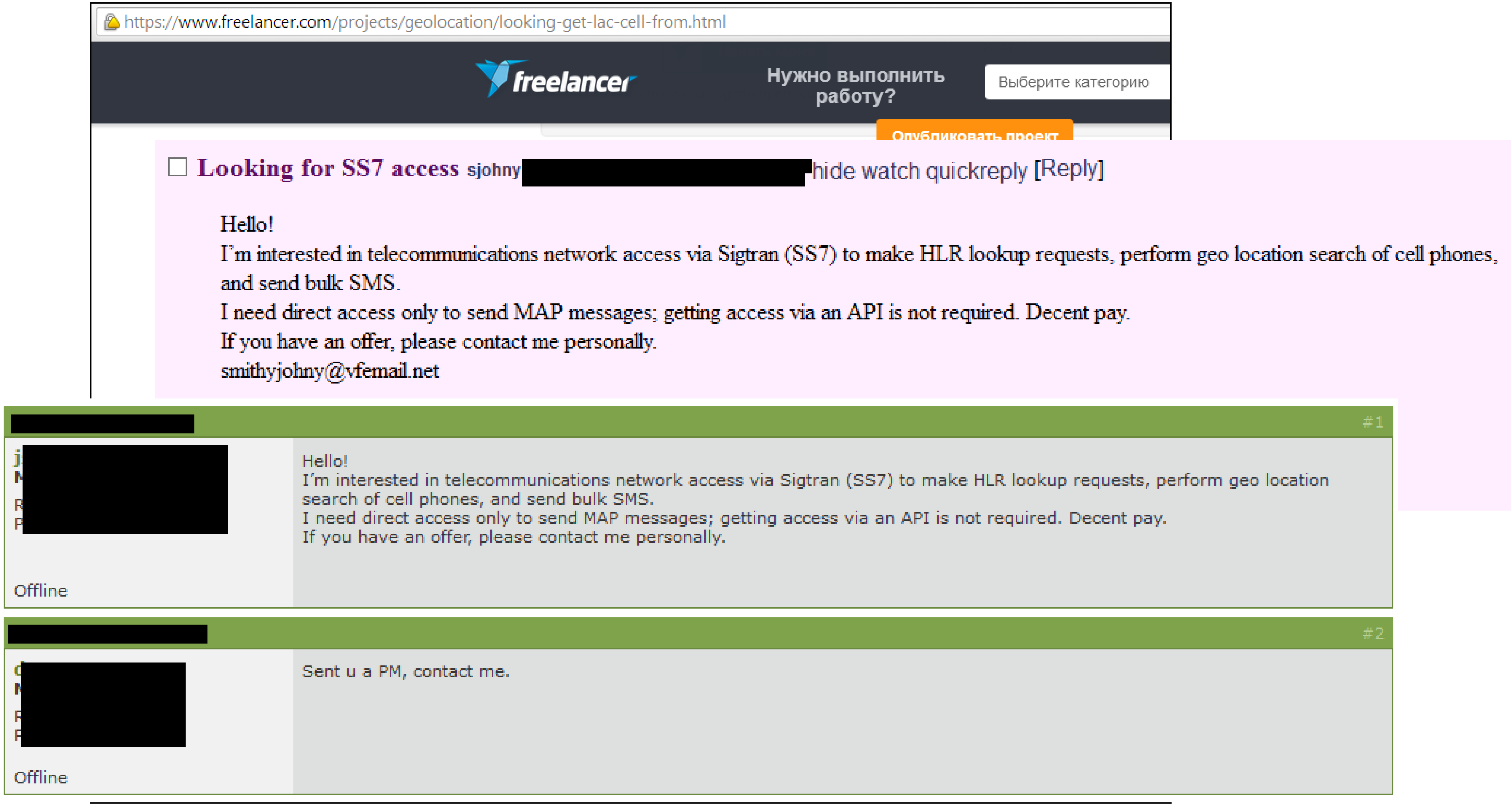
Please do not bid if you are not capable of providing advanced location based services.

Skills required:Gsm Geolocation,SS7 signaling,Tier1

Требуемые навыки:
Геолокация

Показать больше lac cid lookup, cid lac lookup, lac lookup, vlr geolocation, vlr lookup, cell lac lookup, vlr lac, lac cell, geolocation lookup lac, msisdn, geolocation api, lac cid gsm, lac cid, cell lookup google mcc lac, cell lac mnc, cell lac database, cell lac, google map api cell lac, cell lac google, cell lac info, cell lac latitude longtitude java, google map cell lac, excel vba lookup cut cell, lbs, lookup

Find a Guy


https://www.freelancer.com/projects/geolocation/looking-get-lac-cell-from.html
freelancer
Нужно выполнить работу?
Выберите категорию
Опубликовать проект

□ **Looking for SS7 access** sjohny [redacted] hide watch quickreply [Reply]

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@vfemail.net

[redacted] #1

[redacted]

Offline

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.

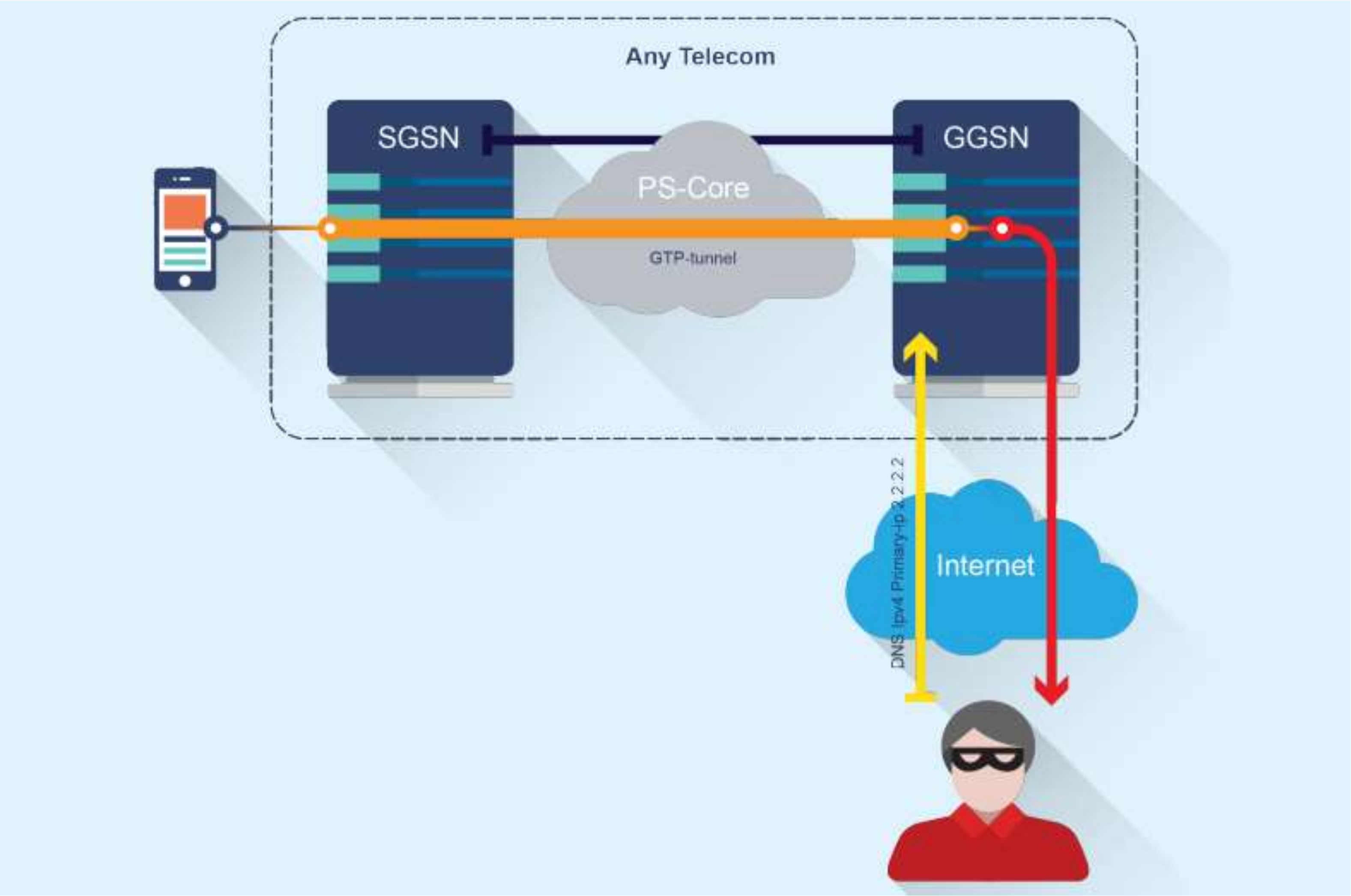
[redacted] #2

[redacted]

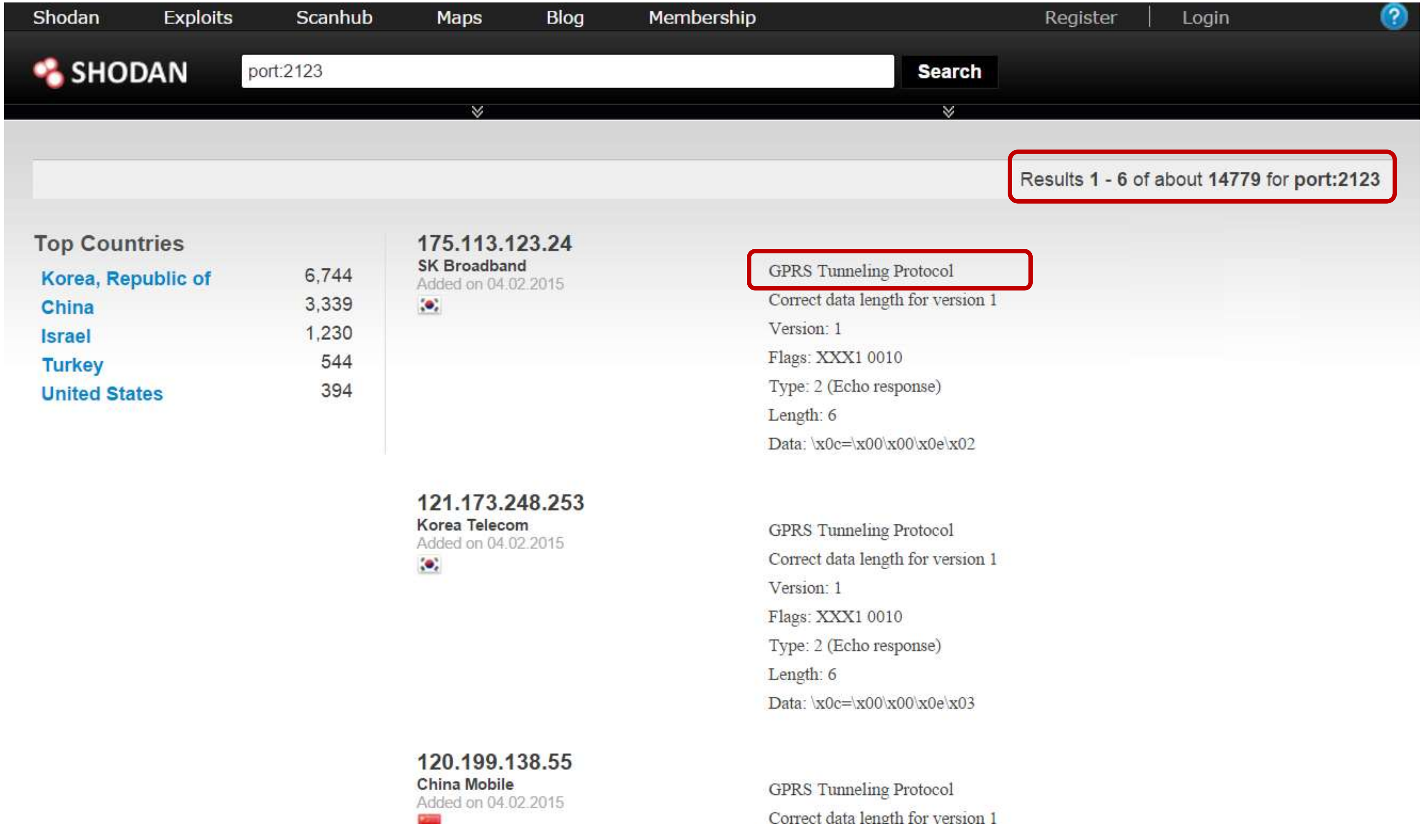
Offline

Sent u a PM, contact me.

Hack border device



Today: IP Connectivity



port:2123

Results **1 - 6** of about **14779** for **port:2123**

Top Countries

Korea, Republic of	6,744
China	3,339
Israel	1,230
Turkey	544
United States	394

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\x0e\x02
```

121.173.248.253
Korea Telecom
Added on 04.02.2015

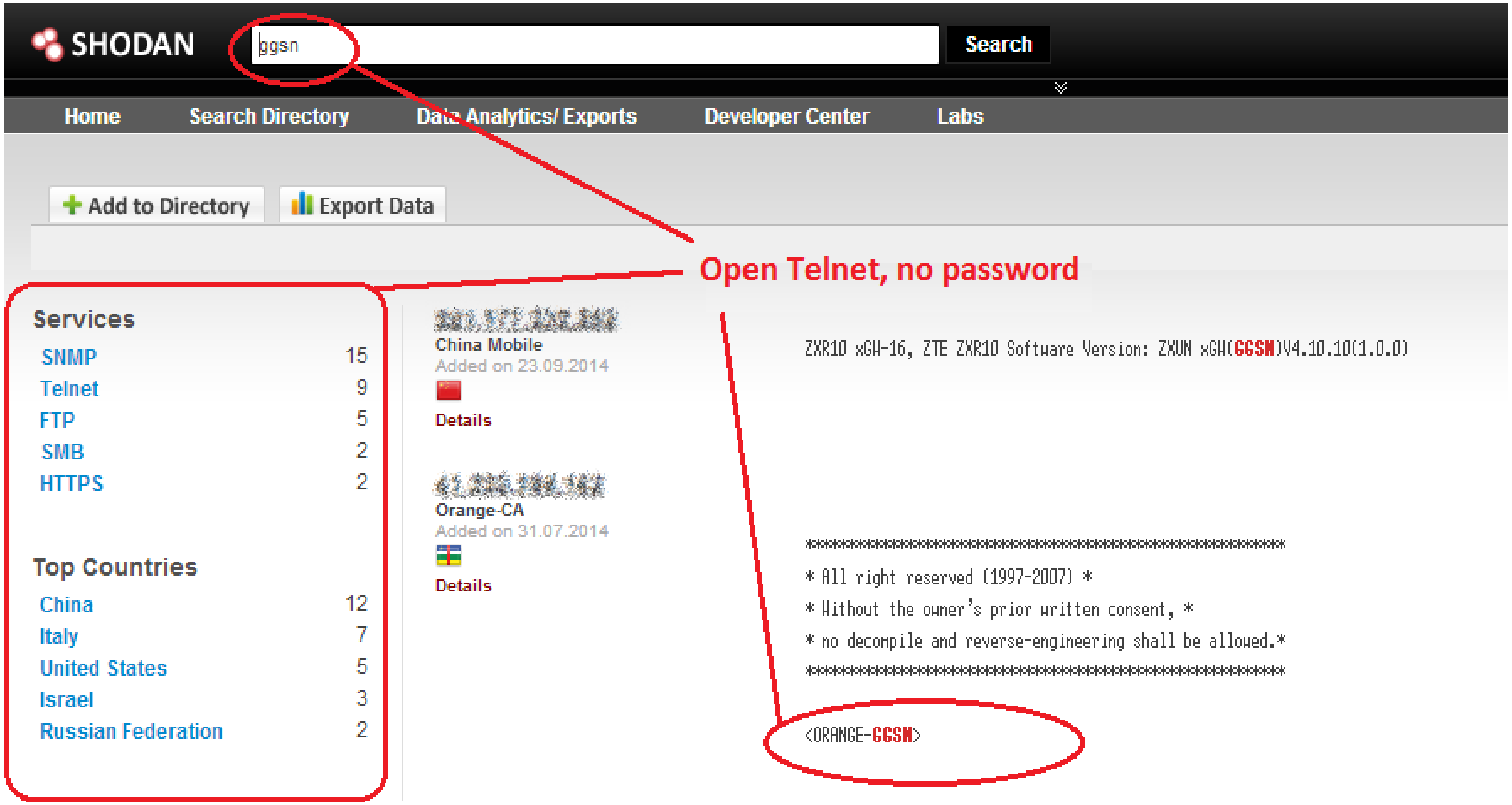
```
GPRS Tunneling Protocol
Correct data length for version 1
Version: 1
Flags: XXX1 0010
Type: 2 (Echo response)
Length: 6
Data: \x0c=\x00\x00\x0e\x03
```

120.199.138.55
China Mobile
Added on 04.02.2015

```
GPRS Tunneling Protocol
Correct data length for version 1
```

Misconfiguration Example

Critical



Open Telnet, no password

Services

SNMP	15
Telnet	9
FTP	5
SMB	2
HTTPS	2

Top Countries

China	12
Italy	7
United States	5
Israel	3
Russian Federation	2

[redacted]
China Mobile
Added on 23.09.2014
Details

```
ZXR10 xGW-16, ZTE ZXR10 Software Version: ZXUN xGW(GGSN)V4.10.10(1.0.0)
```

[redacted]
Orange-CA
Added on 31.07.2014
Details

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

<ORANGE-GGSN>
```

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