

Hacking mobile network via SS7: interception, shadowing and more

Dmitry Kurbatov
Vladimir Kropotov

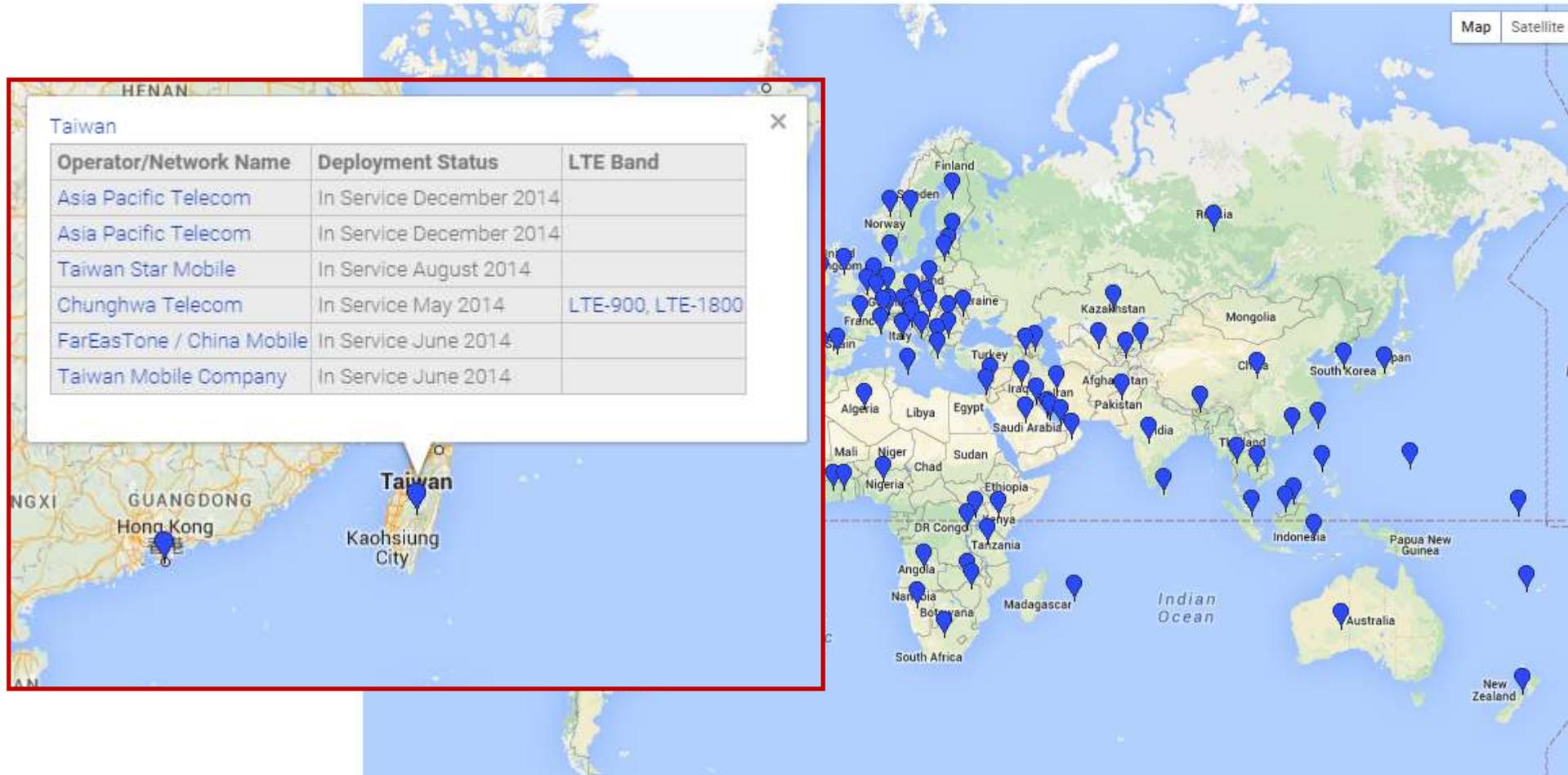
Positive Research

Agenda

- Intro
- Attacks prerequisites, costs and case studies
- Official and underground market brief
- Possible Security measures
- Forecasts

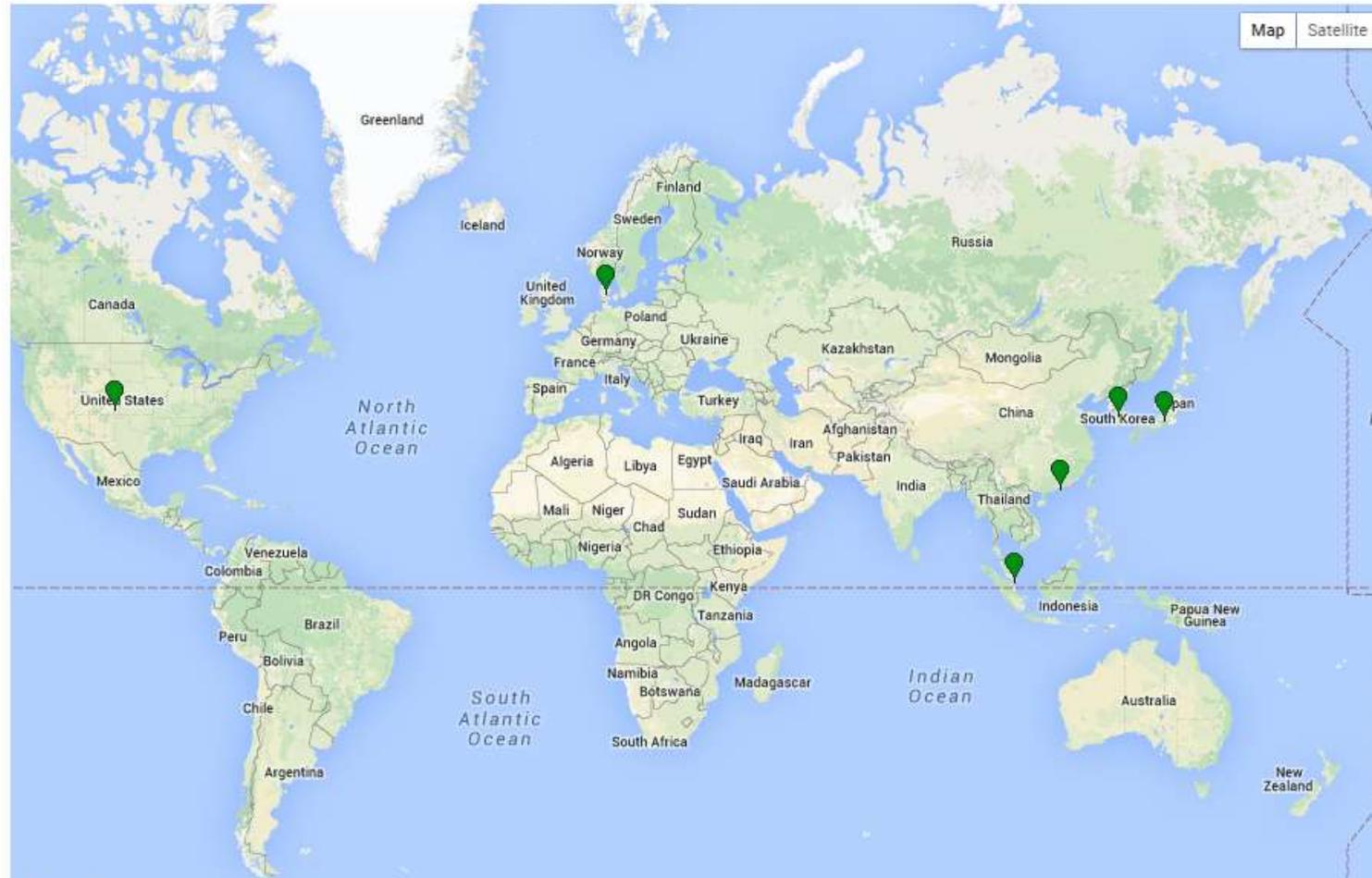
In Service LTE Networks

In Service LTE Networks



VoLTE Networks

VoLTE Networks



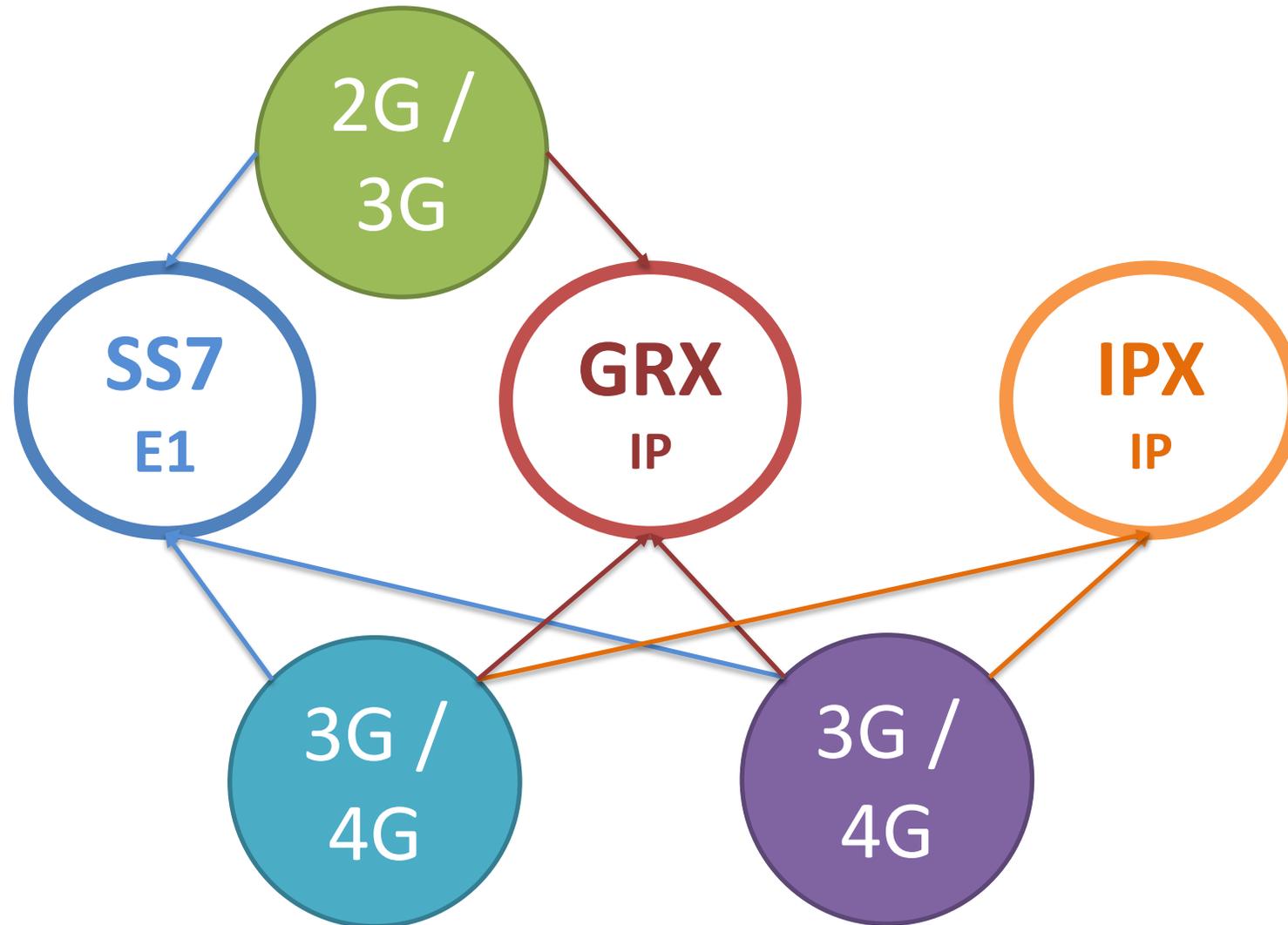
<http://itemaps.org/>

The most of the world performs HANGDOVER

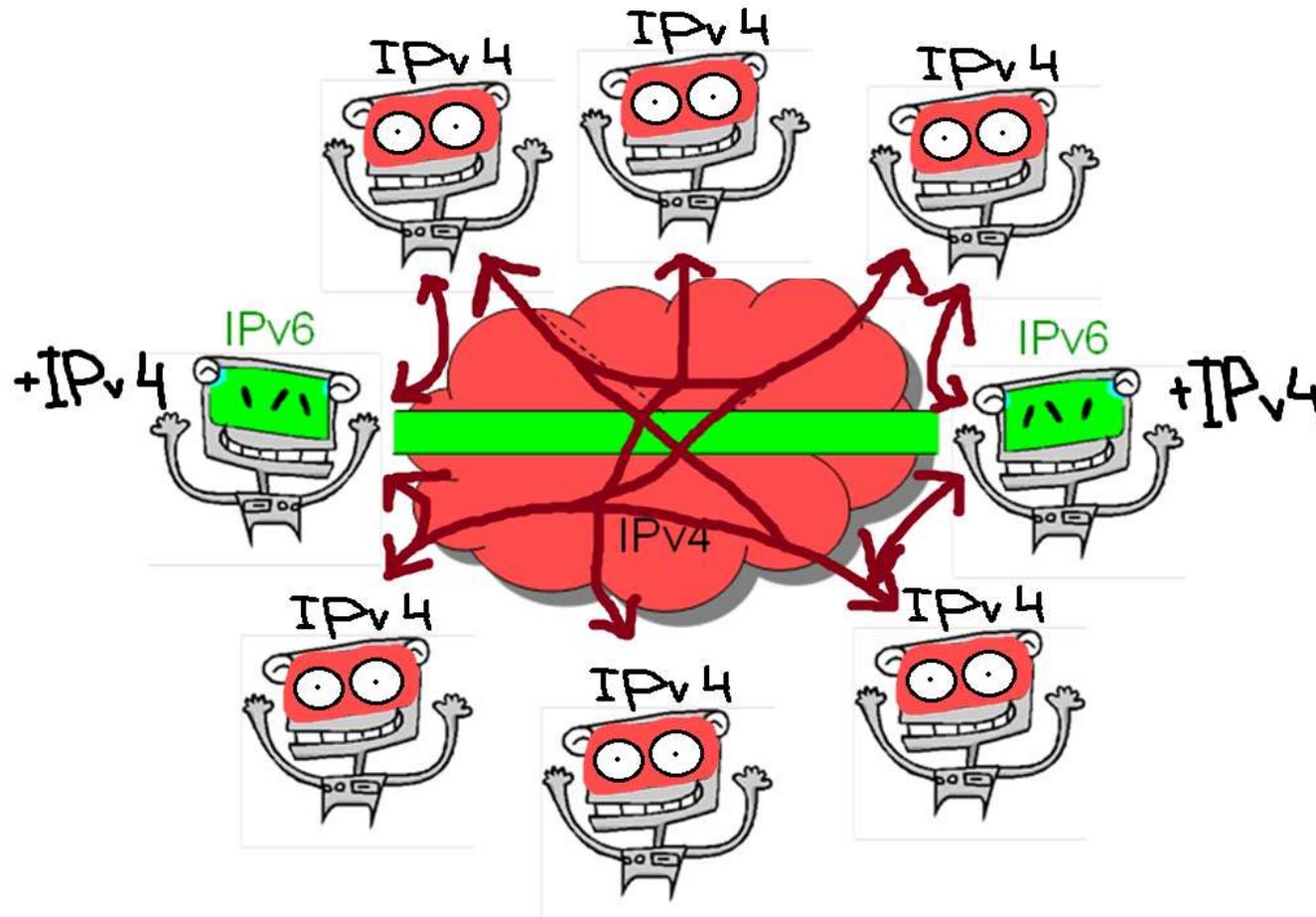
LTE only for web browsing

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

Interconnect / roaming

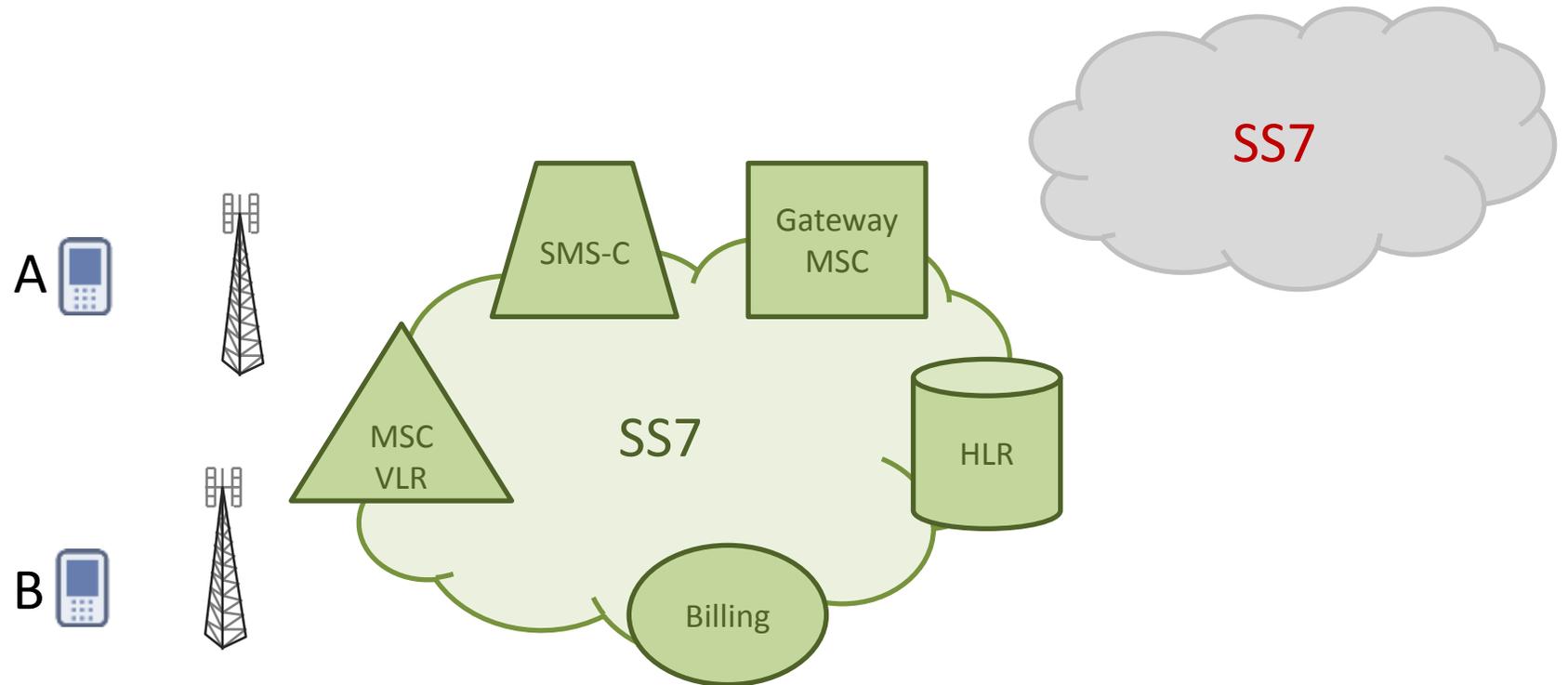


Kind of IPv4 vs IPv6 dilemma



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



EIC3

a new dawn

31st Chaos Communication Congress

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

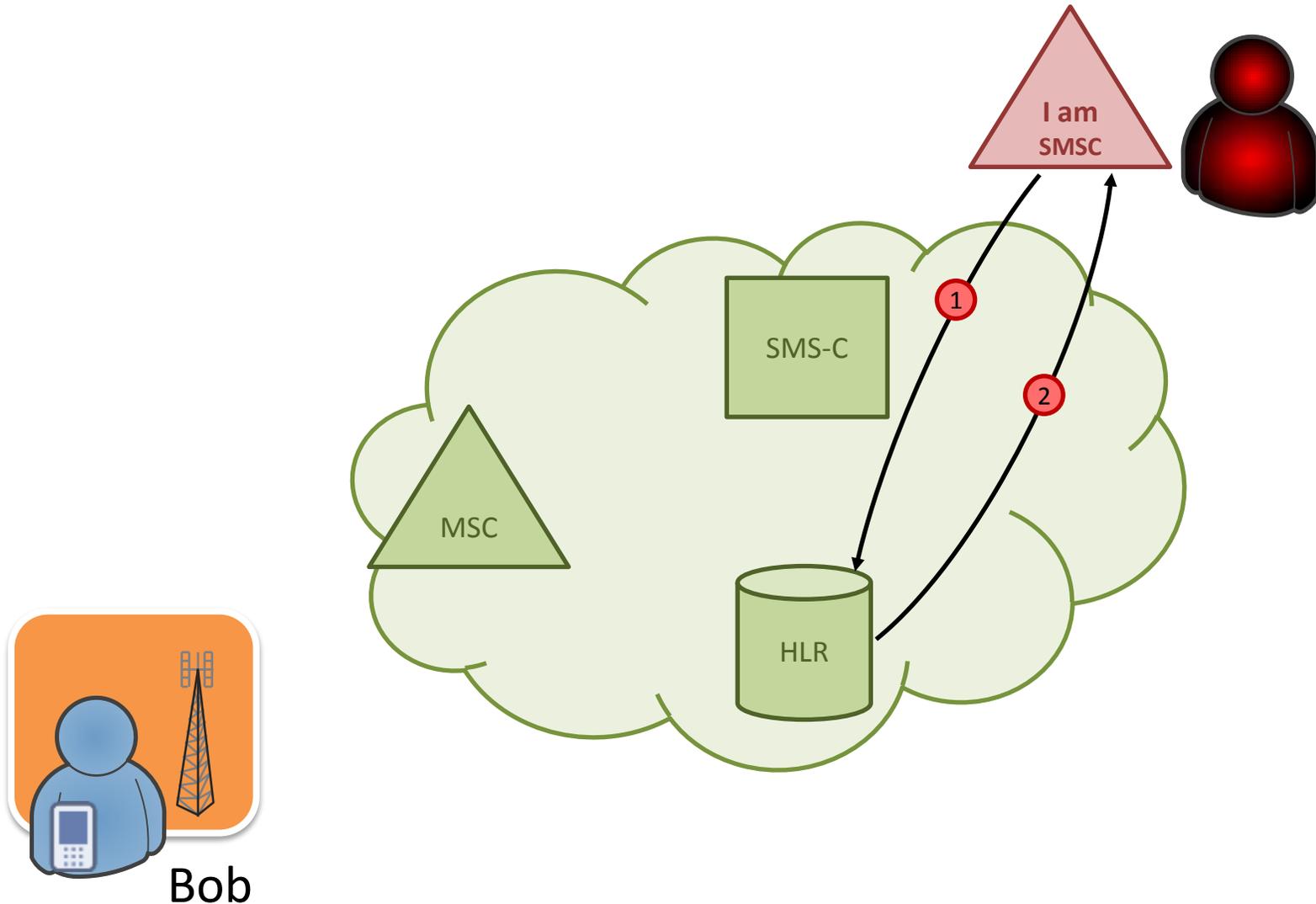
Threats to IoT

Basic Terms

- IMSI ~ SIM Card
- IMEI ~ Device
- MSISDN ~ Your Number
- HLR ~ Subscriber DB
- MSC ~ Call Processing

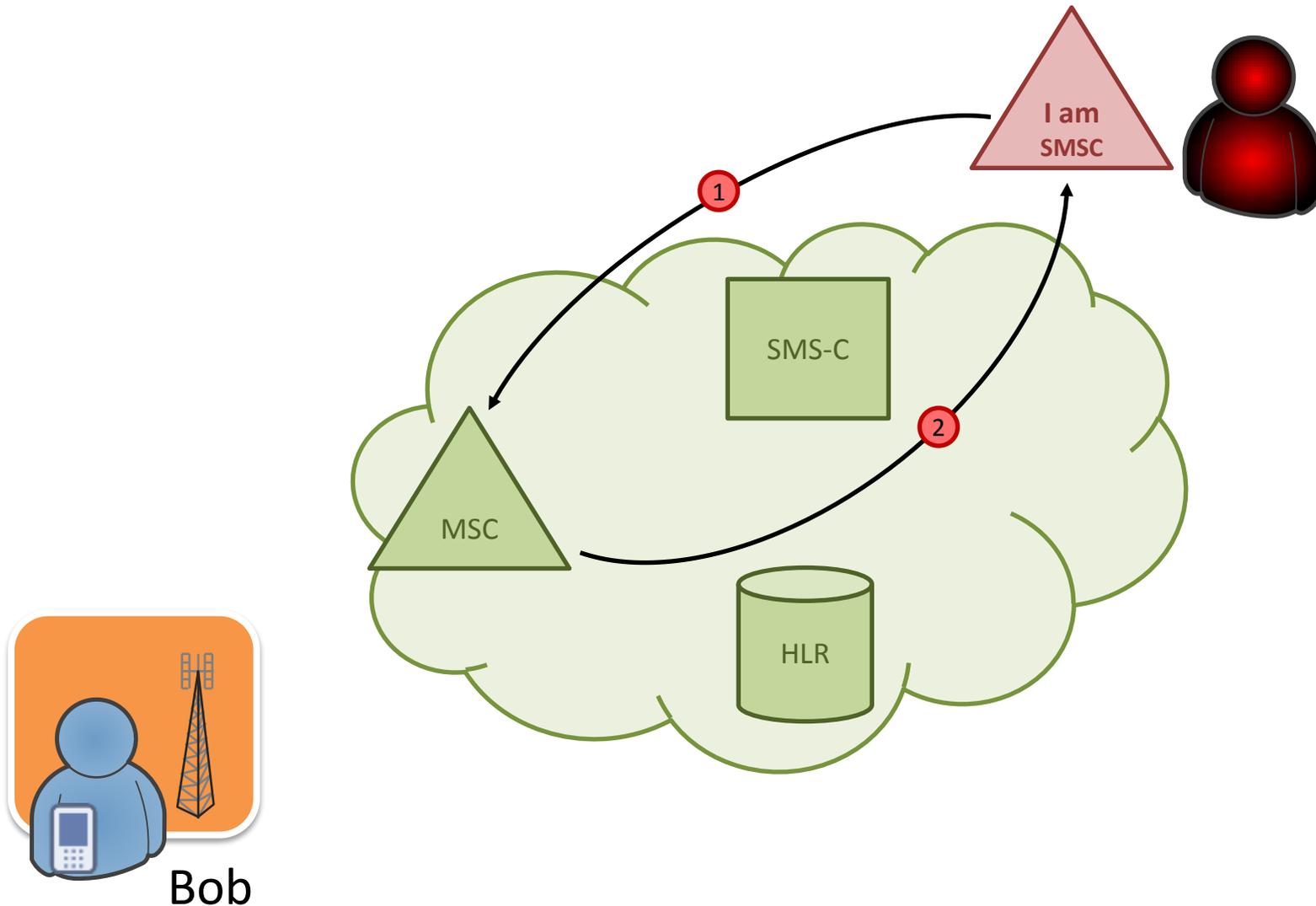
Tracking / 跟踪(位置)

Common Step 0 for Any Attack



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

Get Cell ID

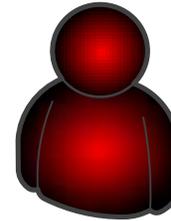


1. Attacker sends request provideSubscriberInfo addressing MAP message by IMSI and asking for subscriber location
2. MSC replies with Cell ID:
 - MCC - 250
 - MNC - 90
 - LAC 4A67
 - CID 673D

Get Location...

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

MCC: 250
MNC: 90
LAC: 4A67
CID: 673D



1



...and Track User Just Like SkyLock

The image displays two screenshots of the Verint SkyLock web application interface. The top-left screenshot shows the 'All Tracked Data' table with columns for MSISDN, Status, Date, MCC/MNC/ACCel, and Coordinates. The top-right screenshot shows the 'System Options' panel with a map of Africa and various configuration fields. The bottom-left screenshot shows the 'Location result' panel with a detailed map of a region in Africa, including a 'Filters Area' callout. The bottom-right screenshot shows a world map with a 'Filters Area' callout and a 'Switch to Tabular View' callout.

Group by	MSISDN	Status	Date	MCC/MNC/ACCel	Coordinates
Date	217201	Idle	2013-01-02 17:52	2260246050171	46.90990, 7.499430
Descending	2180131	Idle	2013-01-02 17:33	4046810047942	28.564166, 7.232119
	2180134	Idle	2013-01-02 17:33	404681004211	28.551132, 7.7241010
	2180134	Idle	2013-01-02 17:22	404681004211	28.551132, 7.7241010
	2180134	Idle	2013-01-02 17:01	404681004211	28.551132, 7.7241010
	2180134	Idle	2013-01-02 17:01	404681004211	28.551132, 7.7241010
	2181000	Idle	2013-01-02 16:41	404681123683	28.53067, 7.7264108
	2181000	Idle	2013-01-02 16:12		
	0011000	Idle	2013-01-02 16:07		

Location result

MSISDN	2439931
IMSI	63002068
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 22:37:11
Last Action	0 Type P
Coordinates	-4.339334, 15.250488

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

Underground market demands

Требуется пробив положения абонента по номеру телефона
Обсуждение в разделе «Предложения работы, услуг», начал(-а) 4upakabr0, 2.09.2013.

2.09.2013

Связь в ЛС

4upakabr0
Member

Регистрация: 14.05.2008
Сообщения: 222
Одобрения: 23
Репутация: 0

В последний раз редактировалось модератором: 2.09.2013

(Для оставления сообщений вы должны во...)

Похожие темы

Пробив абонента по номеру Meshalbek, 4.06.2015, в раздел: Разное - Покупка, продажа, обмен	Ответы: 0 Просмотры: 299
Пробить адрес по номеру телефона Siteg, 11.09.2011, в раздел: Предложения работы, услуг	Ответы: 0 Просмотры: 533
Пробить человека по номеру телефона. Falknat, 12.08.2011, в раздел: Мобильная связь, СМС - Покупка, продажа	Ответы: 1 Просмотры: 1 699
Отследить абонента по номеру телефона? око, 28.05.2010, в раздел: Электроника и Фрикинг	Ответы: 9 Просмотры: 37 875
Пробить номер телефона по базе YaNeLam, 7.02.2008, в раздел: Болталка	Ответы: 16 Просмотры: 3 278

Отследить абонента по
око, 28.05.2010, в раздел: Э

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

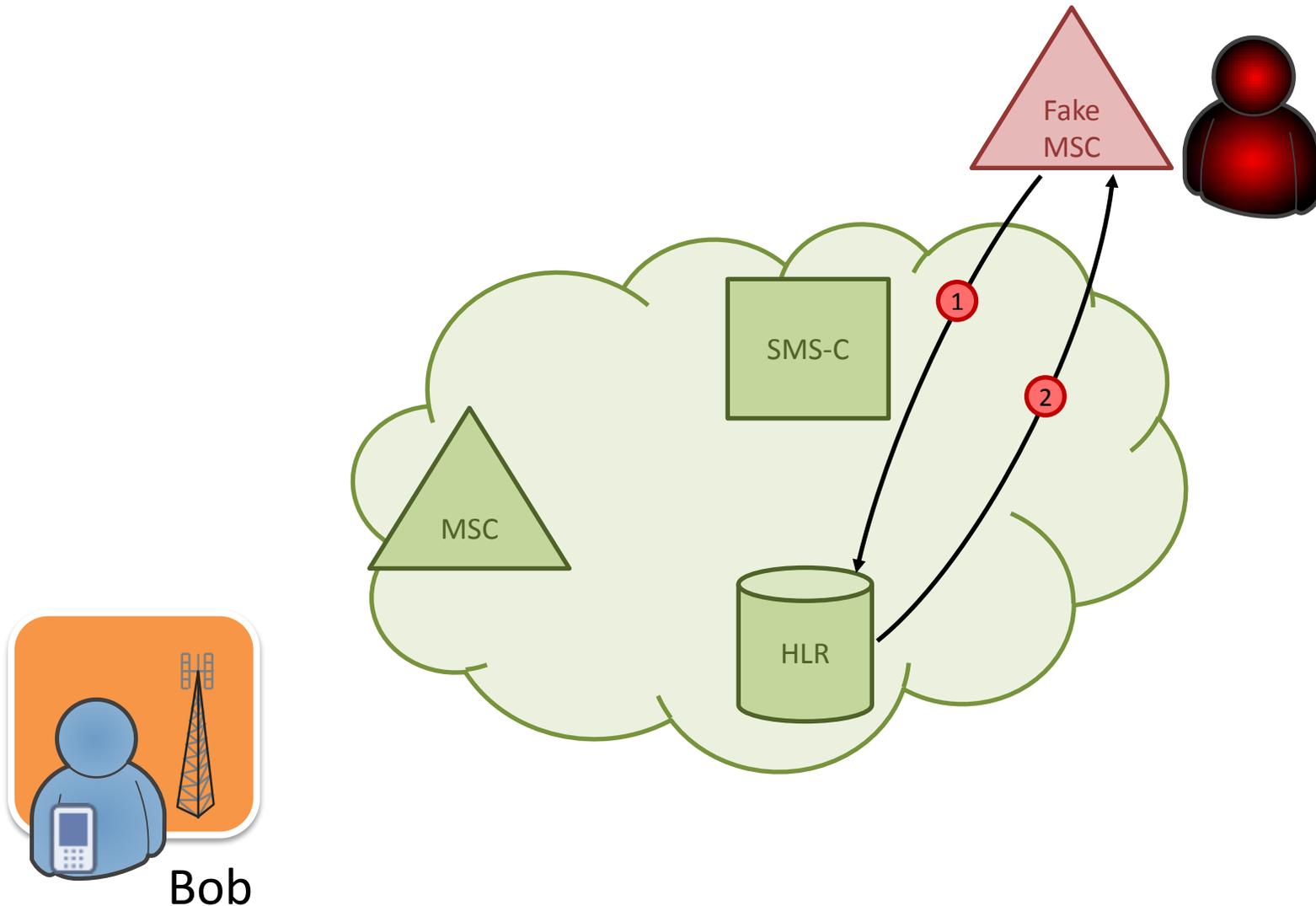
To make someone unavailable

To stop data leakage

What else?

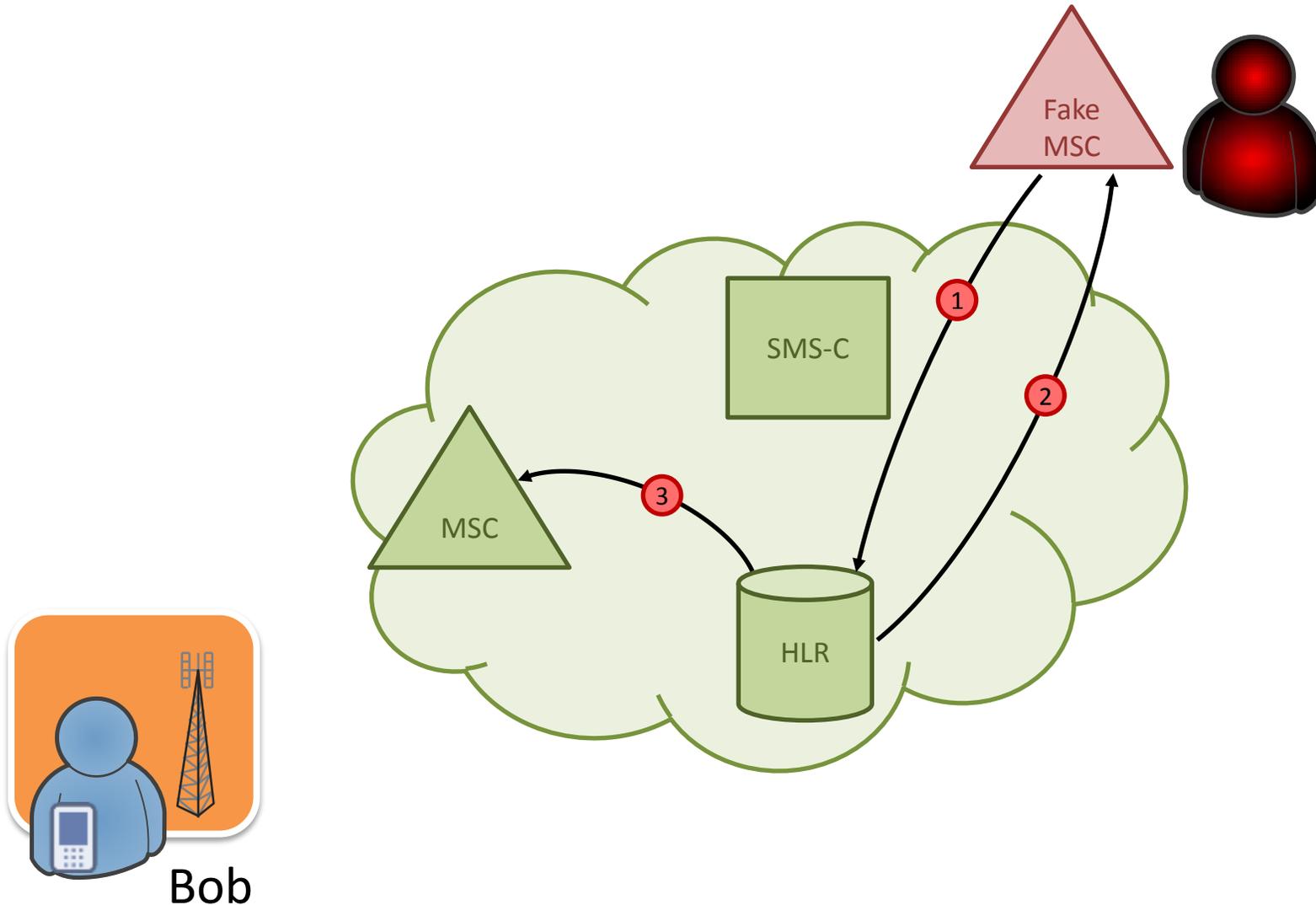


Common Step 0 for Any Attack



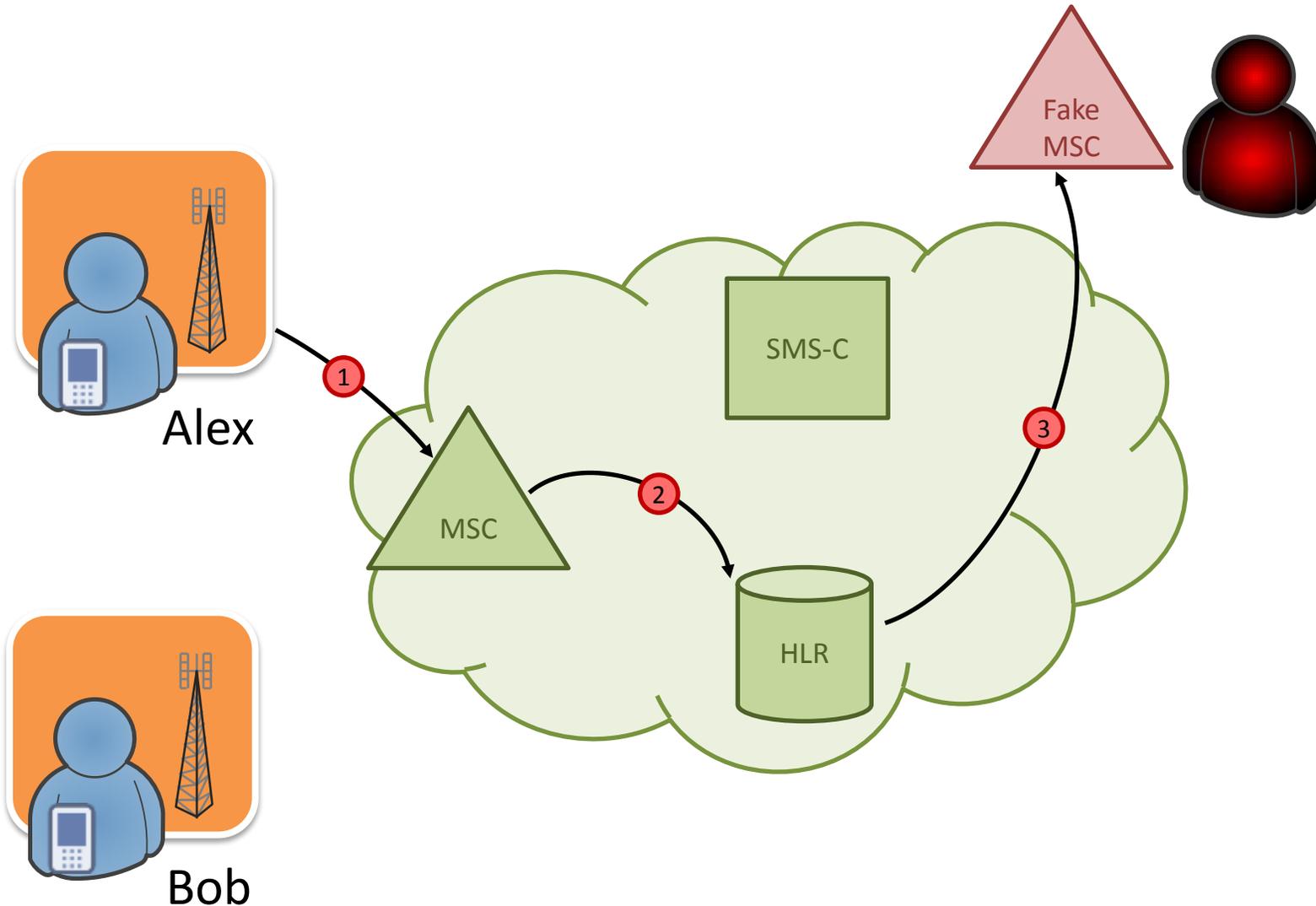
1. Attacker sends request SendRoutingInfoForSM addressing MAP message by MSISDN
2. HLR replies with:
 - own address
 - serving MSC address
 - IMSI

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.



Video: Secret Towers Tracing Your Calls



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.



ComputerWeekly.com

IT Management ▼

Industry Sectors ▼

Technology Topics

Ross Coulthart

60 Minutes Australia

16 Aug 2015 23:58

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 +

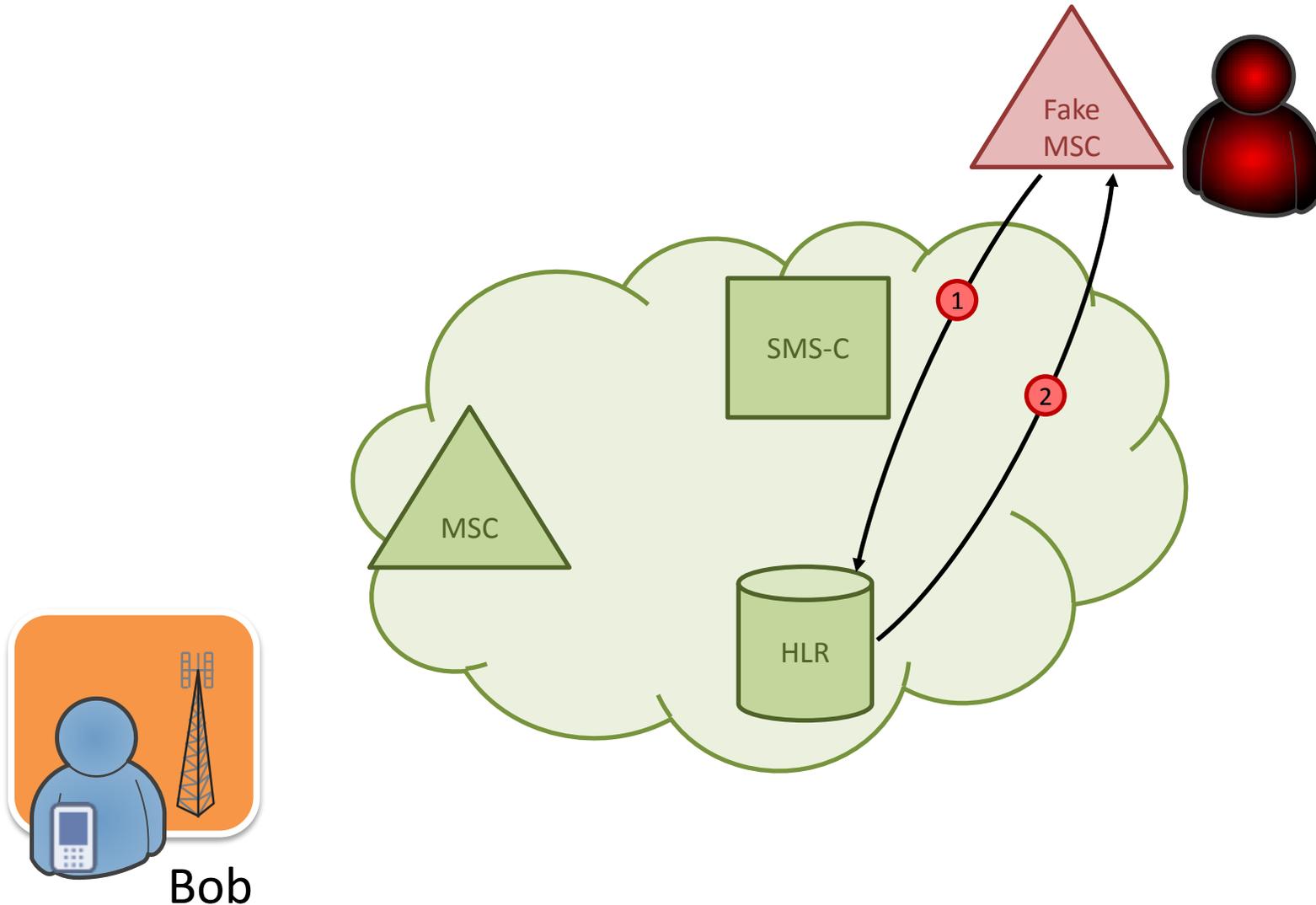
The logo for osmocomBB, featuring a stylized antenna tower icon to the left of the text "osmocomBB". The text is in a red, sans-serif font.



(f)or

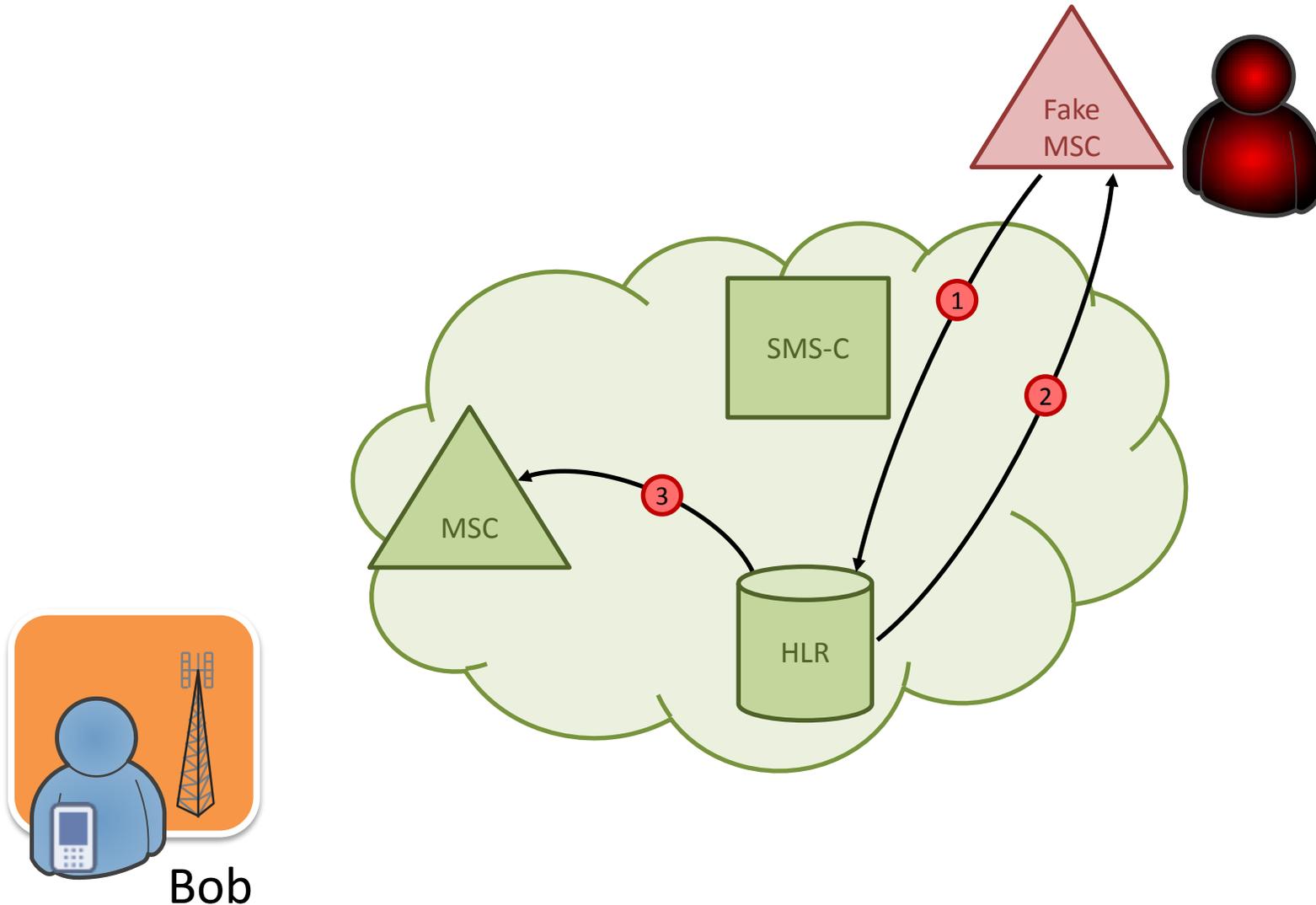
\$\$\$7

Common Step 0 for Any Attack



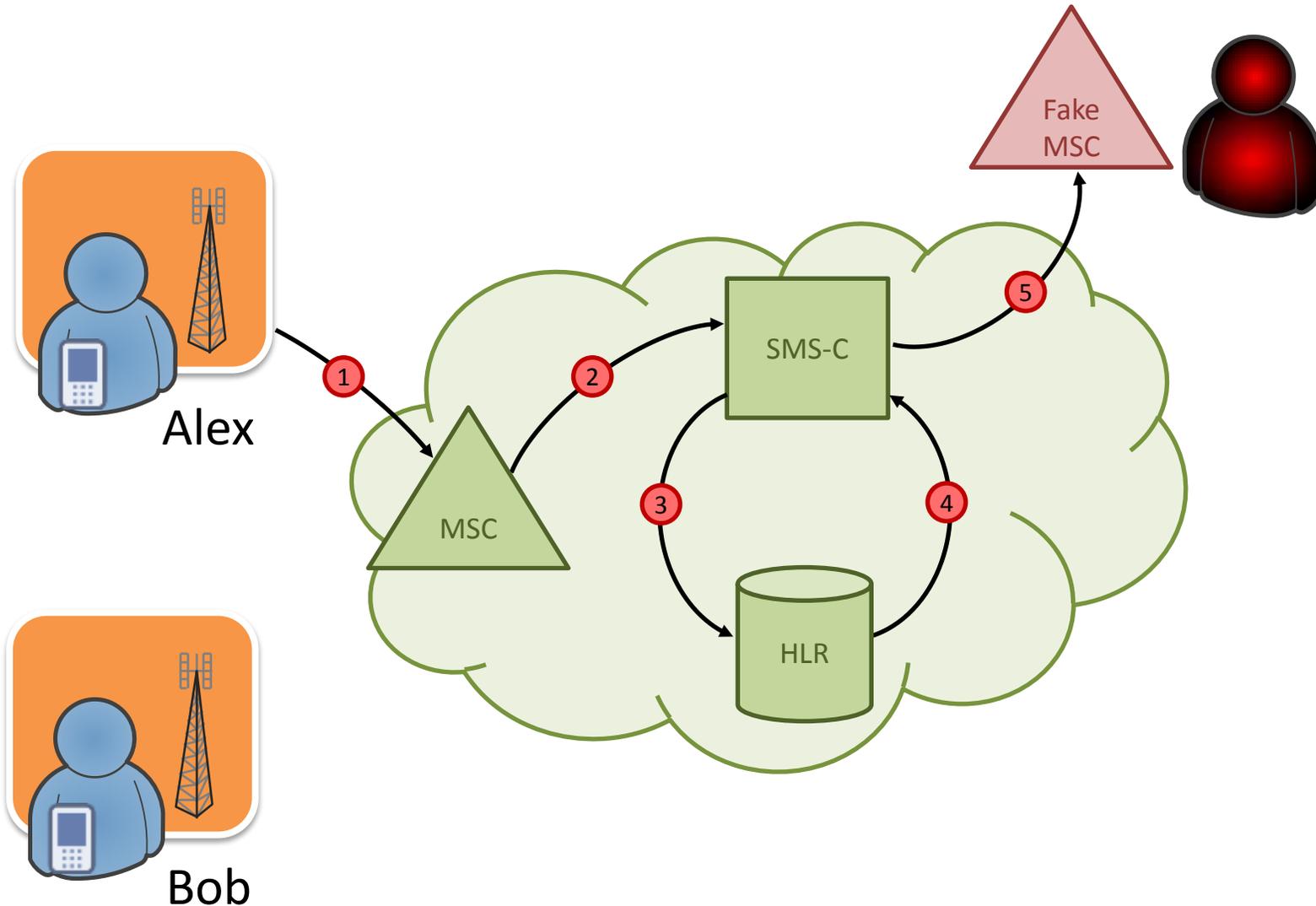
1. Attacker sends request SendRoutingInfoForSM addressing MAP message by MSISDN
2. HLR replies with:
 - own address
 - serving MSC address
 - IMSI

SMS Interception. Step 1



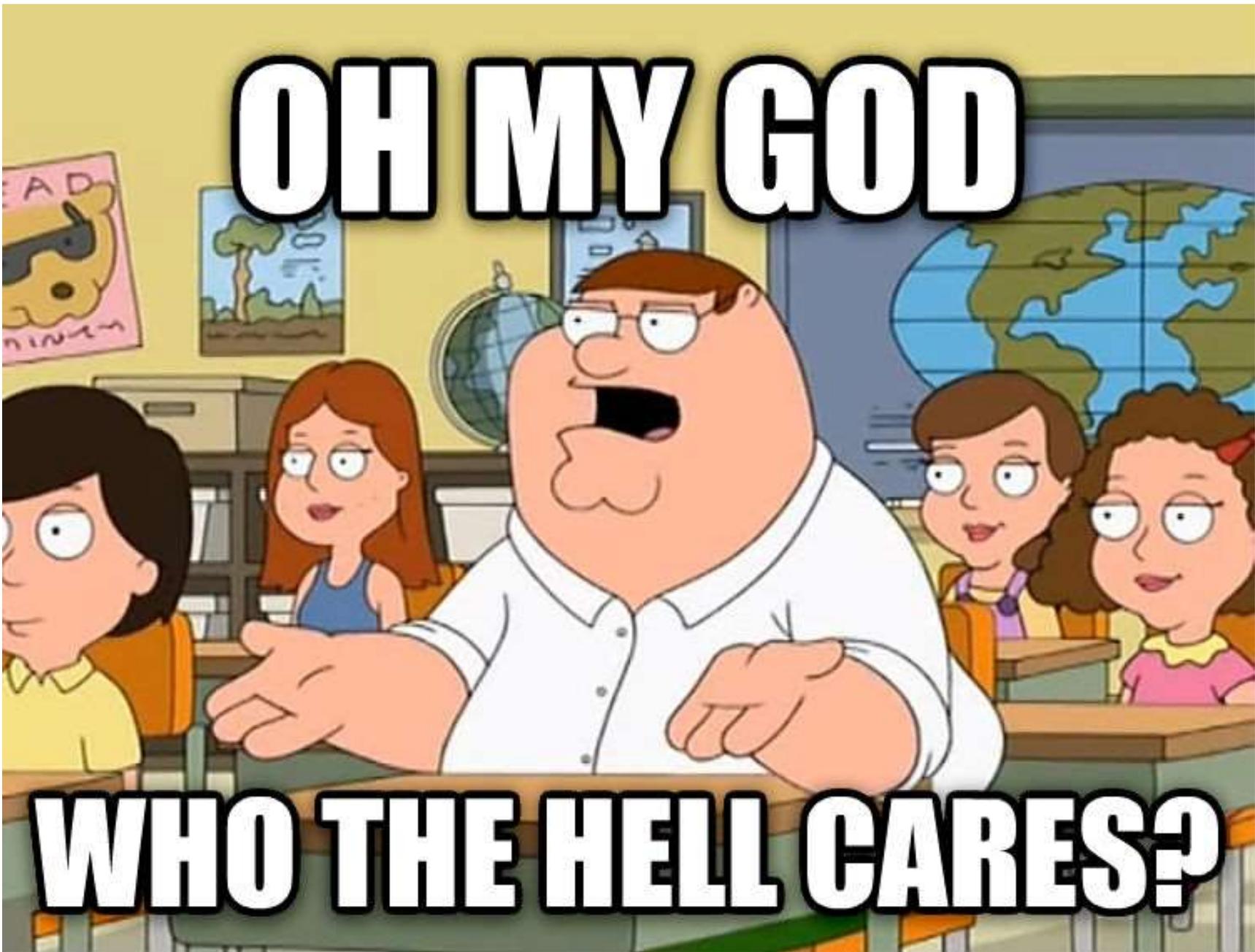
1. Attacker registers Bob on the fake MSC
2. HLR sets up new location for Bob
3. HLR asks real MSC to release a memory

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



Illegal cases

SMS Interception

Куплю перехват СМС/Восстановление сим [Дорого]

Обсуждение в разделе «Мобильная связь, СМС - Покупка, продажа», начал(-а) Lokem, 29.10.2012.

29.10.2012

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

Payment confirmation
SMS Interception

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

Обсуждение в разделе «Платежные системы: Webmoney, Яндекс Деньги, РБК Де», начал(-а) snare, 10.02.2013.

Lokem
New Member

10.02.2013

Собственно сабж. Брочу кошельки киви, но очень часто бывает что стоят смс-подтверждения или смс-уведомления на перевод средств с кошелька на кошелек. Хотел бы узнать/поинтересоваться

Интересуют устройства для перехвата смс

Обсуждение в разделе «Электроника и Фрикинг», начал(-а) TommyLipkiy, 13.08.2015.

snare
New Member

13.08.2015

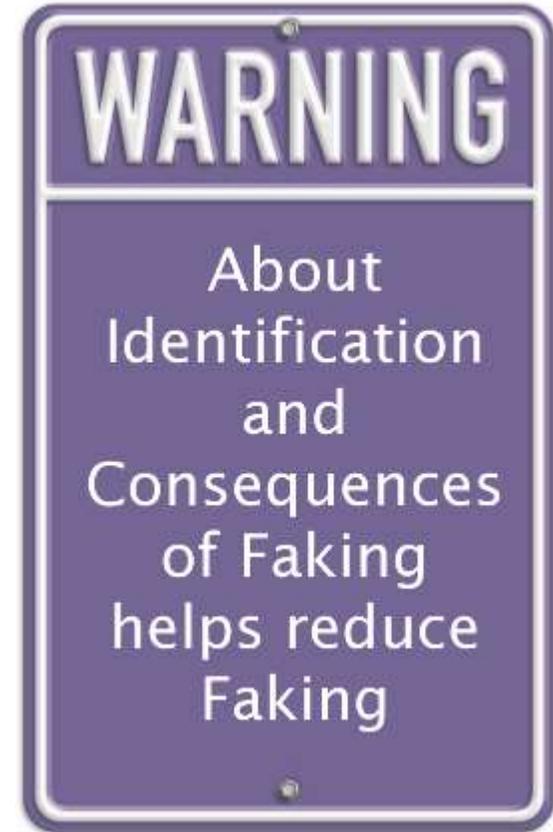
регистрация:

Добрый день, интересуют устройства для перехвата смс и разговоров. Кто владеет информацией где можно приобрести данные игрушки прошу в пм.

Devices for
SMS Interception

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

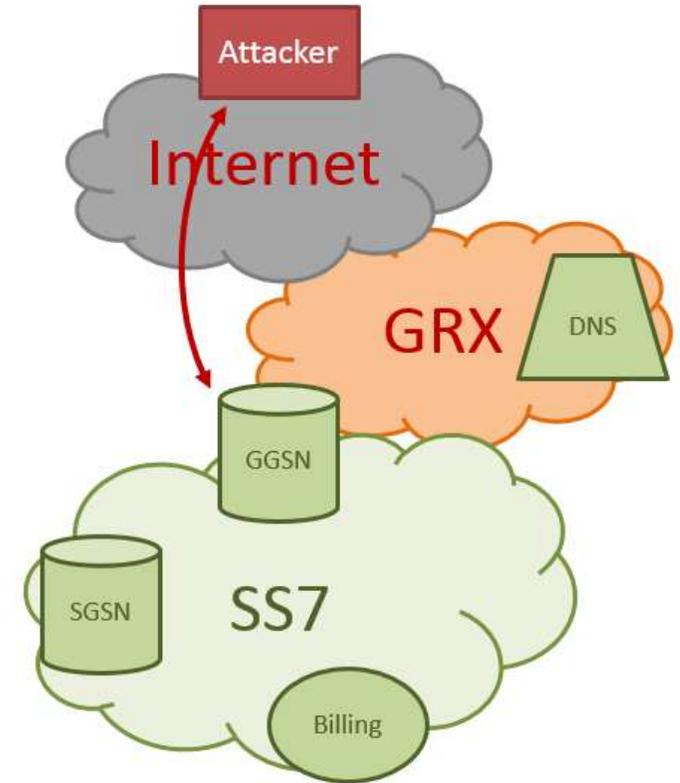
How They Can Get Into SS7



Legal with license
Semi legal without



Find a guy



Hack border device

Find a Guy

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

 Нужно выполнить работу?

[Опубликовать проект](#)

Looking to get LAC/CELL ID from a VLR lookup

[f](#) [t](#) [M](#) [e](#) [p](#) [+](#) 0

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 longitude 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

 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 longitude 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

 Нужно выполнить работу? Выберите категорию

[Опубликовать проект](#)

Looking for SS7 access sjohnny [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.
smithyjohnny@vfemail.net

[redacted] #1

 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.

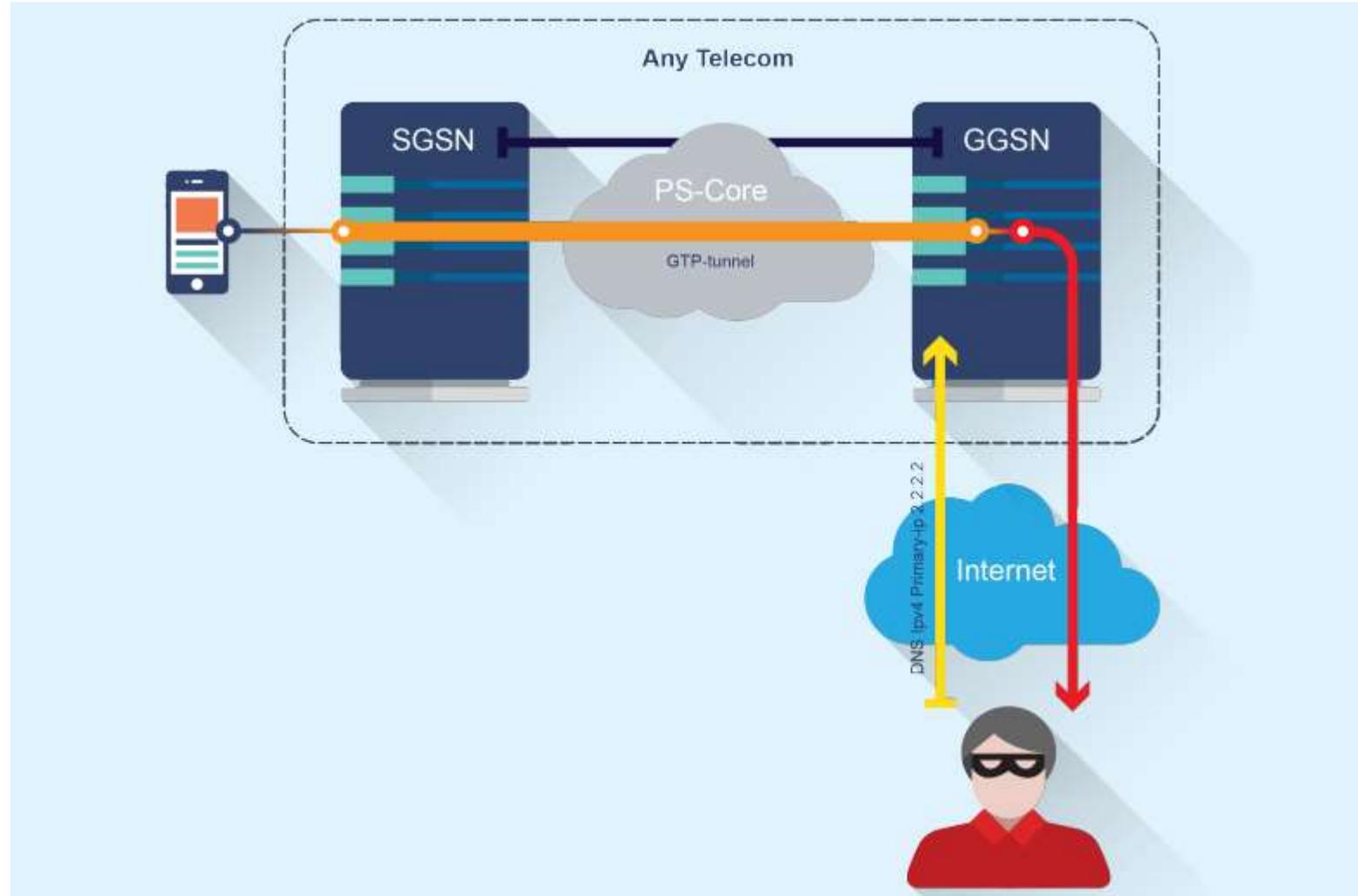
Offline

[redacted] #2

 Sent u a PM, contact me.

Offline

Hack border device



Today: IP Connectivity

The screenshot shows the Shodan search engine interface. At the top, there is a navigation bar with links for Shodan, Exploits, Scanhub, Maps, Blog, Membership, Register, and Login. Below this is a search bar containing the query 'port:2123' and a 'Search' button. A red box highlights the search results summary: 'Results 1 - 6 of about 14779 for port:2123'. On the left side, there is a 'Top Countries' section with a list of countries and their corresponding result counts. The main content area displays three search results, each with an IP address, provider name, and a red box highlighting the service name 'GPRS Tunneling Protocol'. The first result is for IP 175.113.123.24 (SK Broadband), the second for 121.173.248.253 (Korea Telecom), and the third for 120.199.138.55 (China Mobile). Each result also includes details such as 'Correct data length for version 1', 'Version: 1', 'Flags: XXX1 0010', 'Type: 2 (Echo response)', 'Length: 6', and 'Data: \x0c=\x00\x00\x0e\x02'.

Shodan Exploits Scanhub Maps Blog Membership Register Login

SHODAN port:2123 Search

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

SHODAN Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

+ Add to Directory Export Data

Critical

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

China Mobile
Added on 23.09.2014

Details

Orange-CA
Added on 31.07.2014

Details

Open Telnet, no password

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

```
*****  
* 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/>



Questions?

Dmitry Kurbatov

dkurbatov@ptsecurity.com

Vladimir Kropotov

vkropotov@ptsecurity.com