POSITIVE TECHNOLOGIES

Hacking mobile network via SS7: interception, shadowing and more

Dmitry Kurbatov

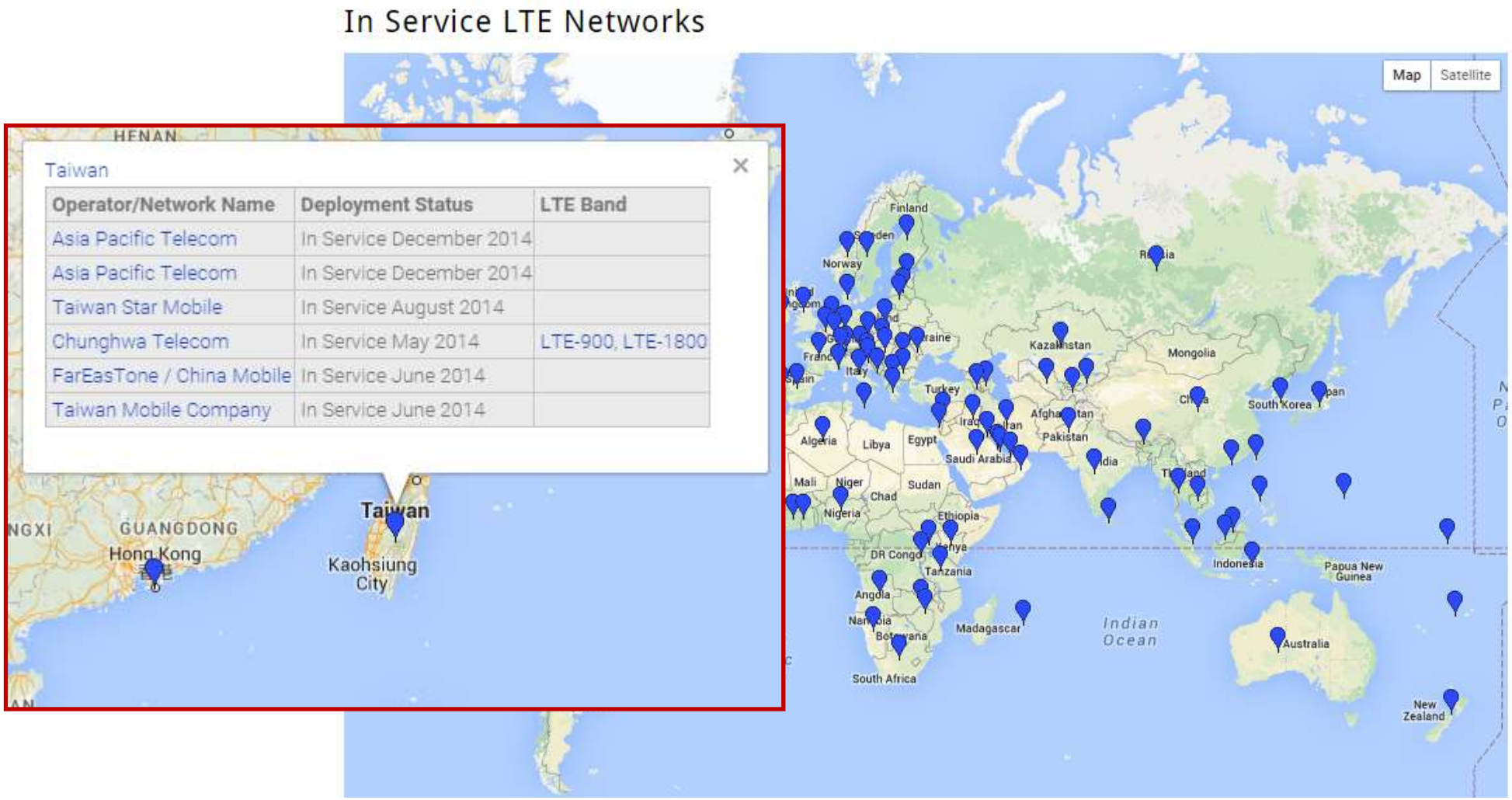
Vladimir Kropotov

Positive Research

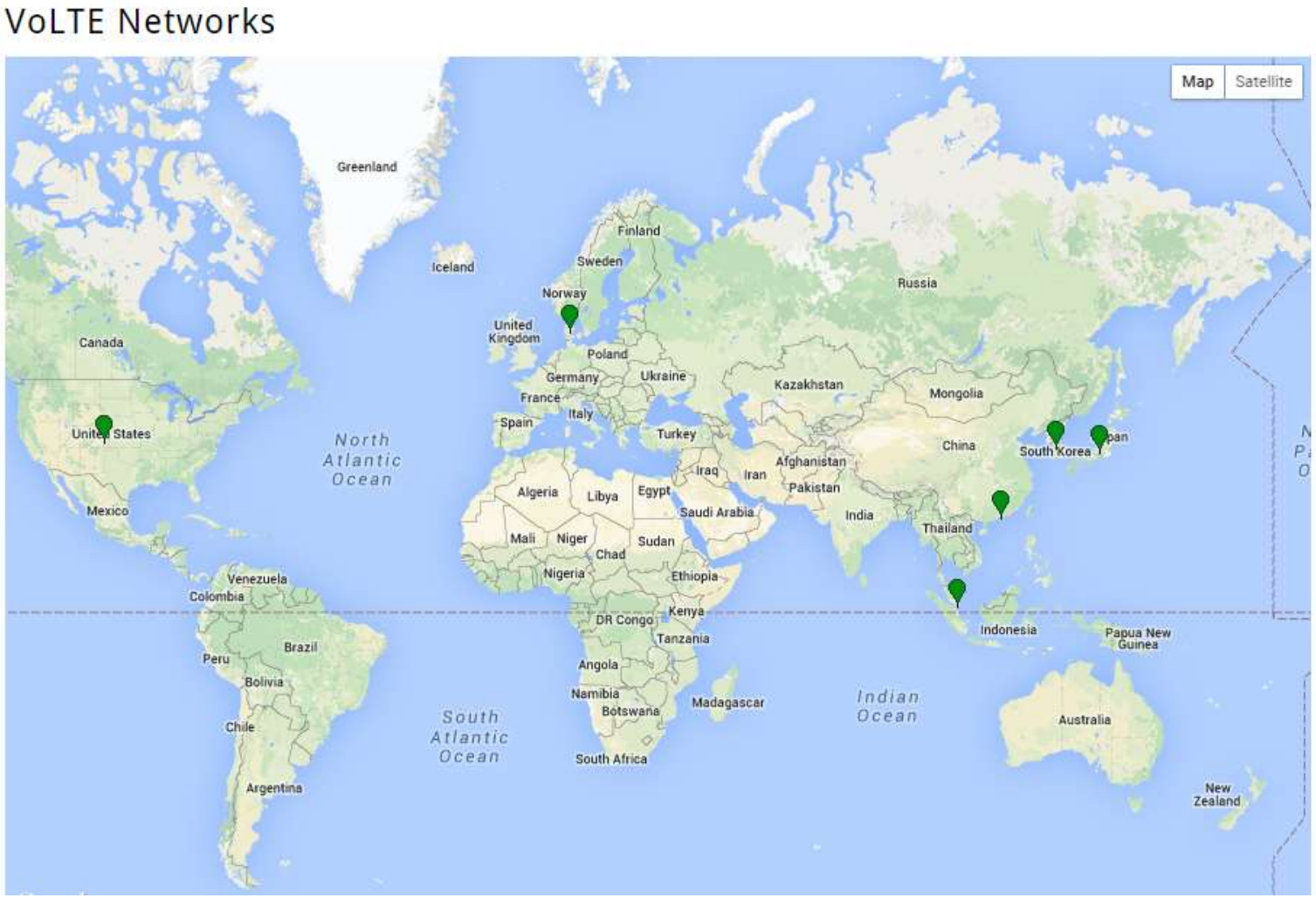
Agenda

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

In Service LTE Networks



VoLTE Networks



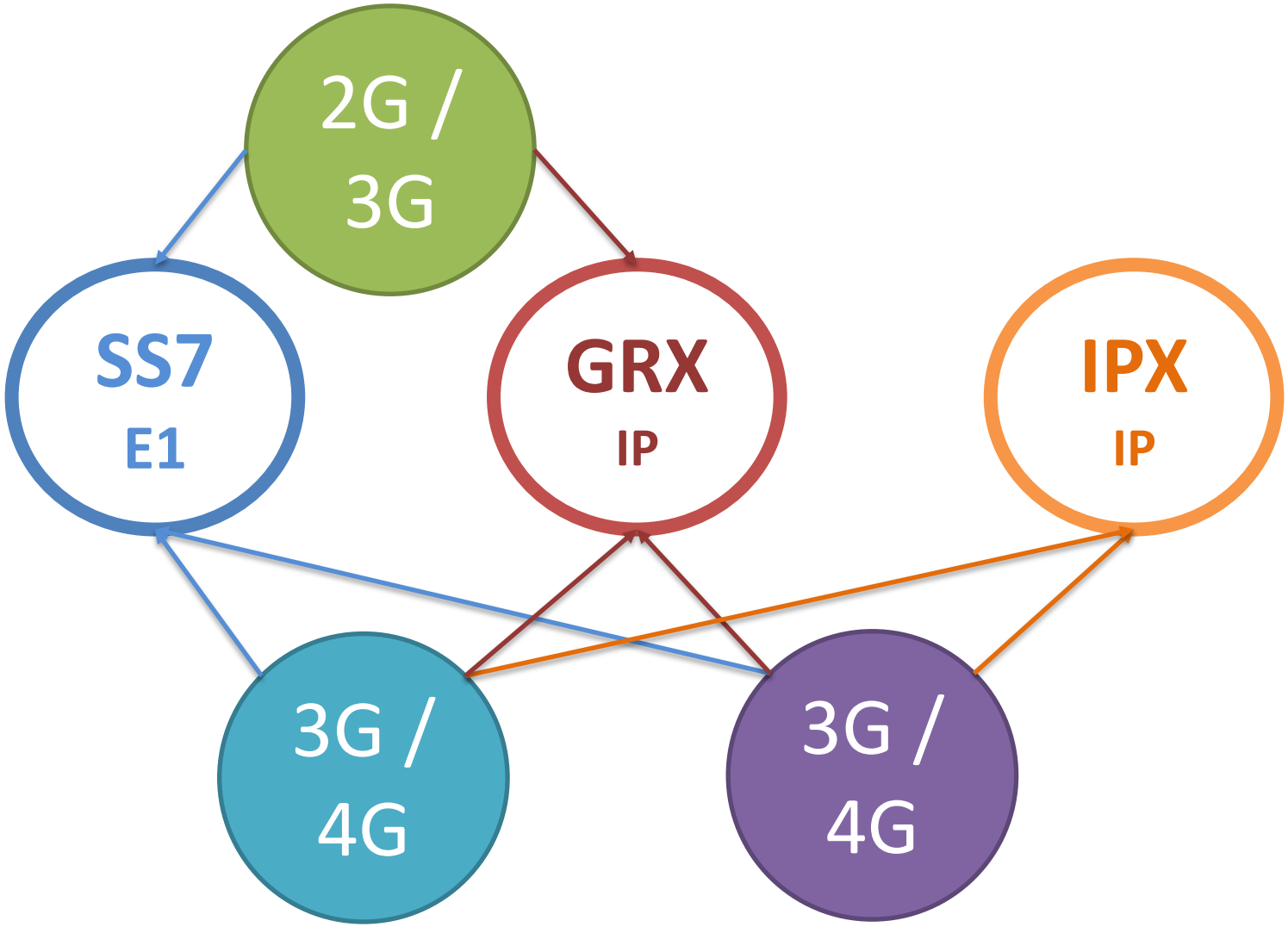
http://ltemaps.org/

The most of the world performs HANGDOVER

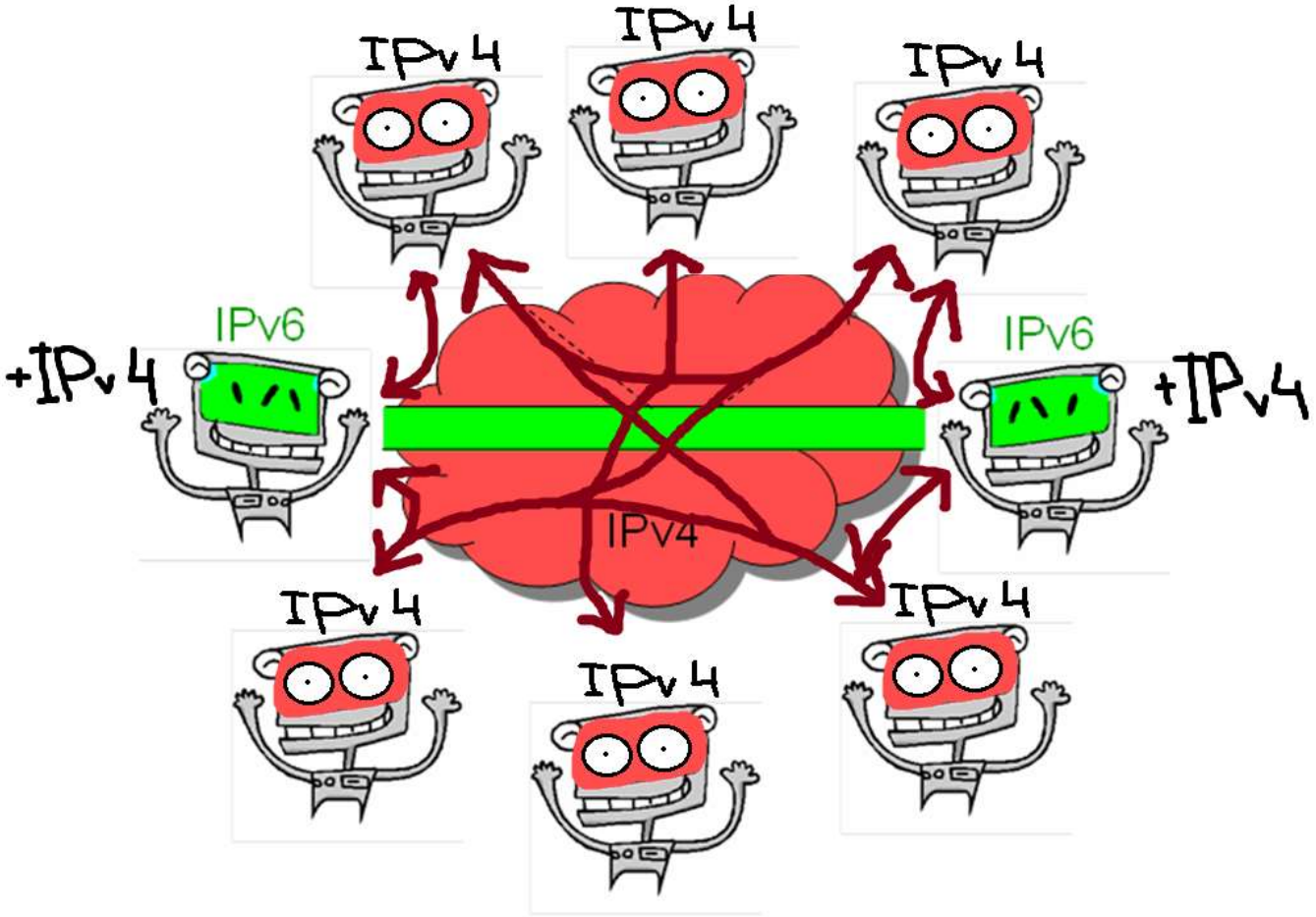
LTE only for web browsing

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

Interconnect / roaming

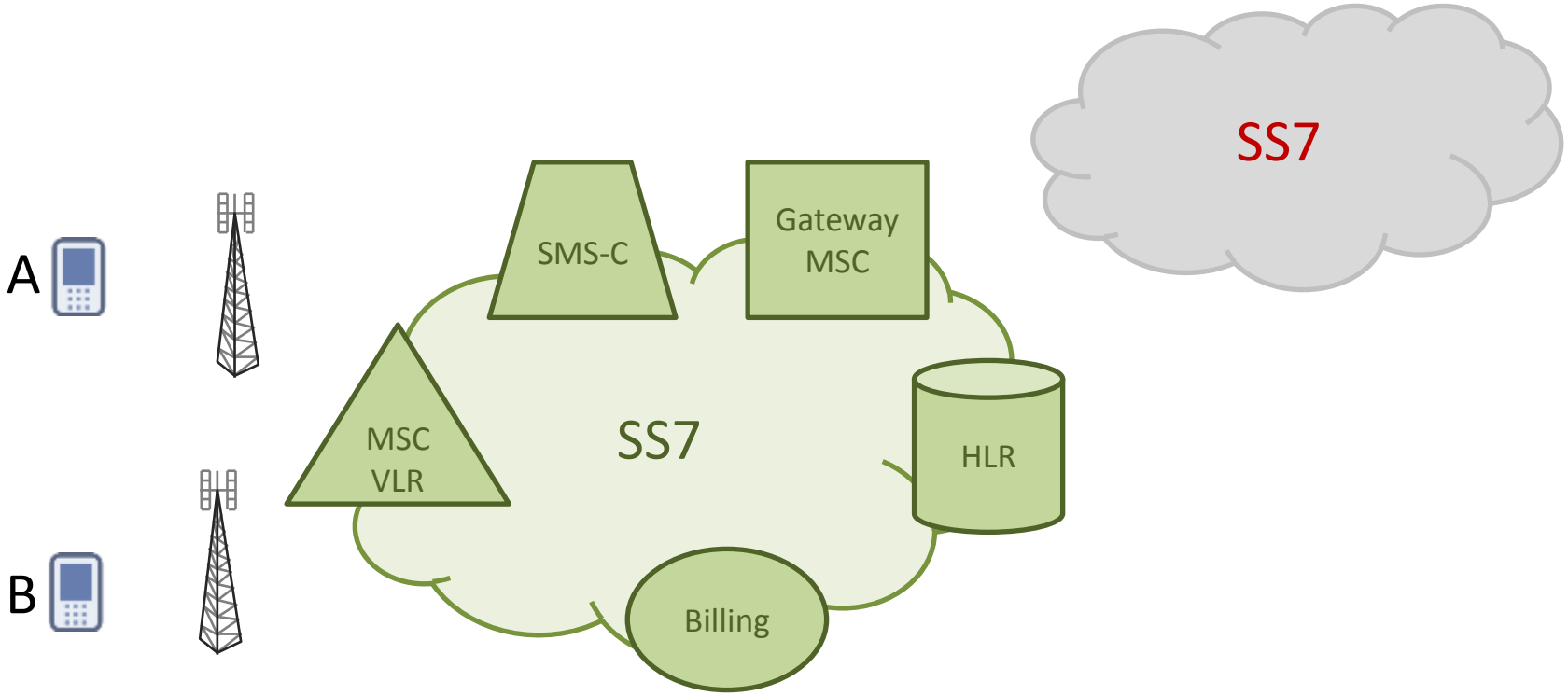


Kind of IPv4 vs IPv6 dilemma



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

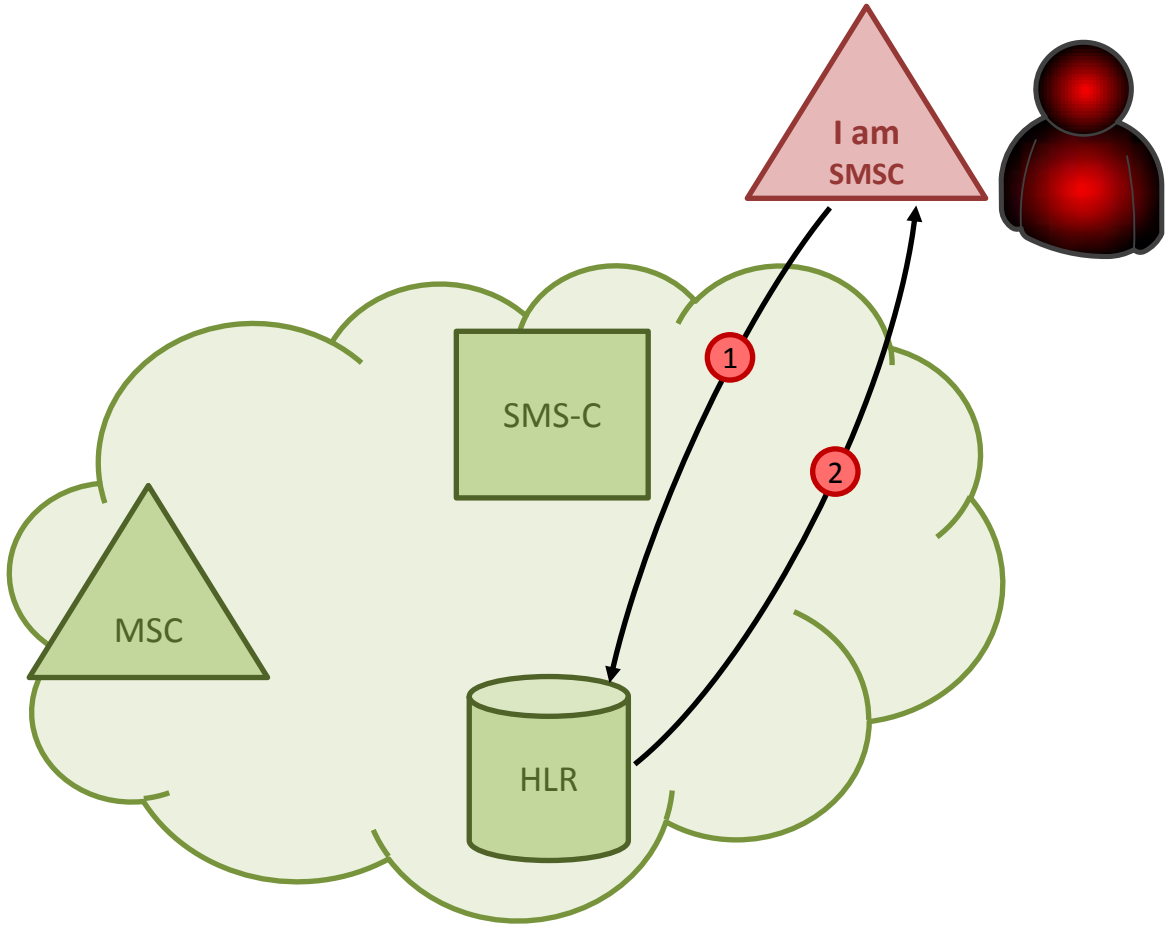
Threats to IoT

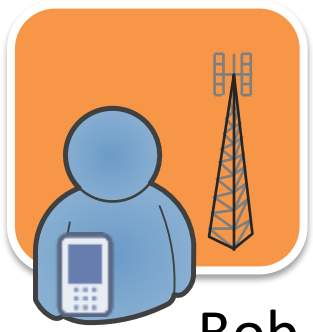
Basic Terms

- 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

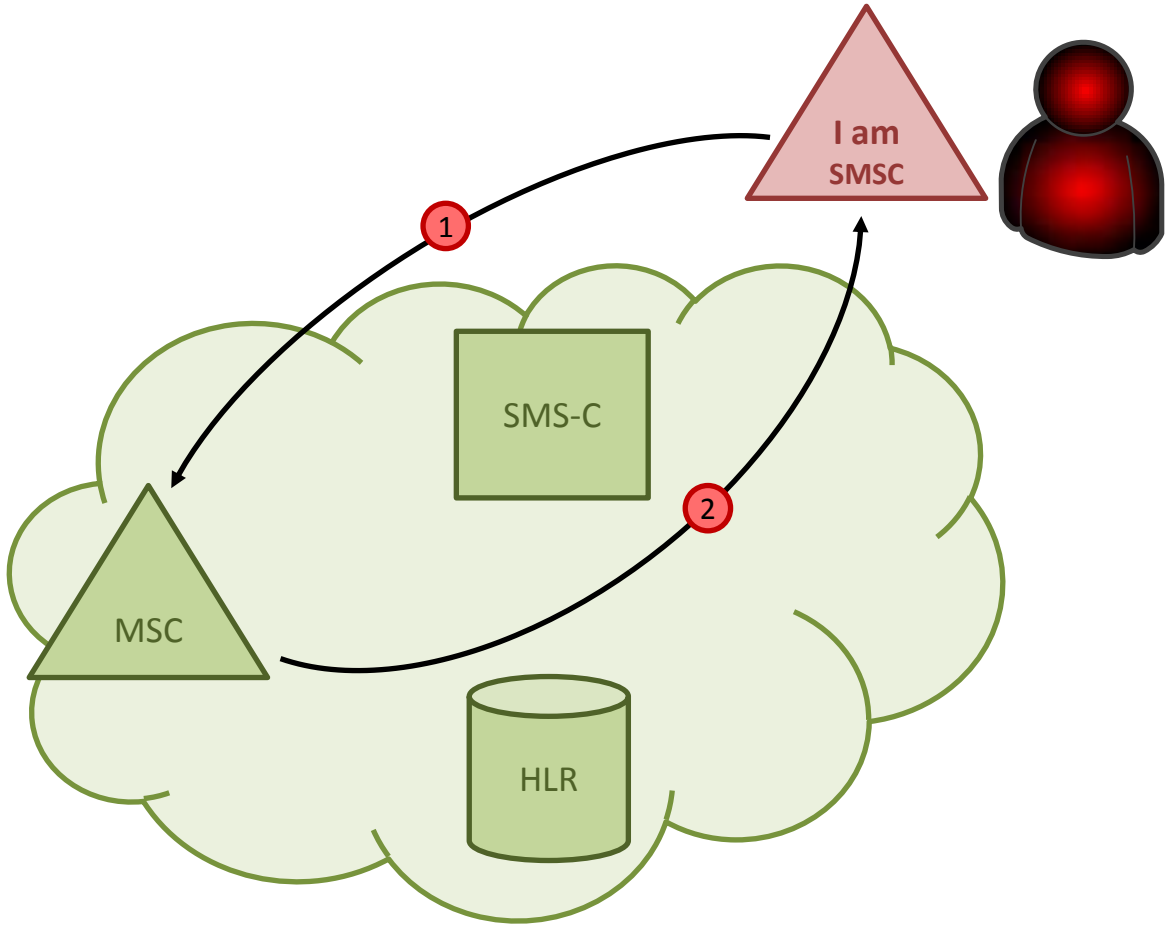


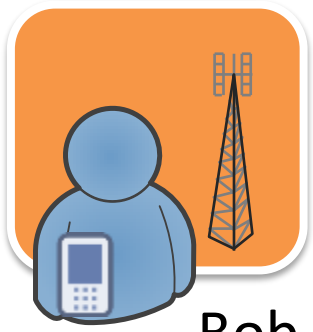


Bob

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

Get Cell ID



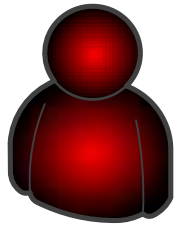


Bob

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

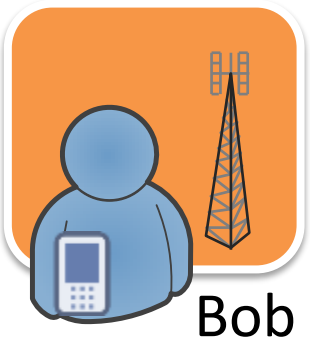
Get Location…

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



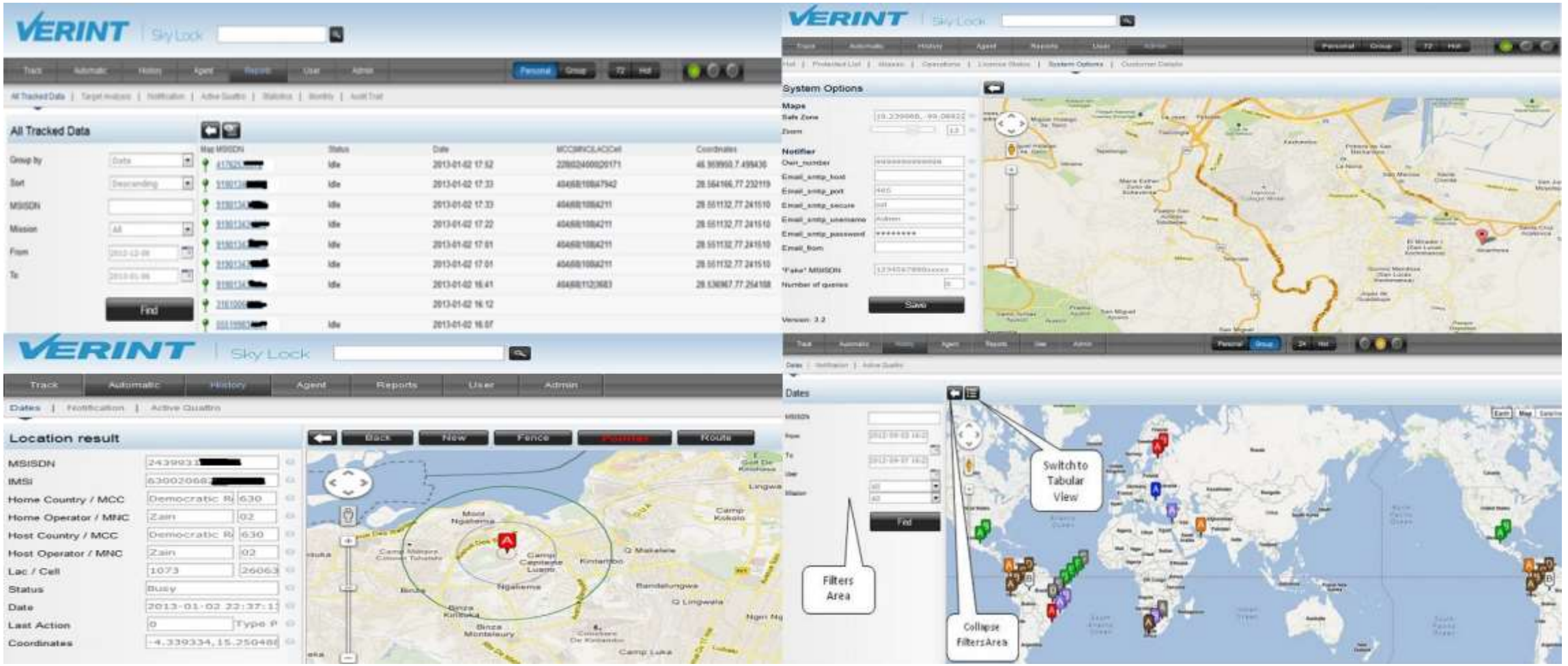
1

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



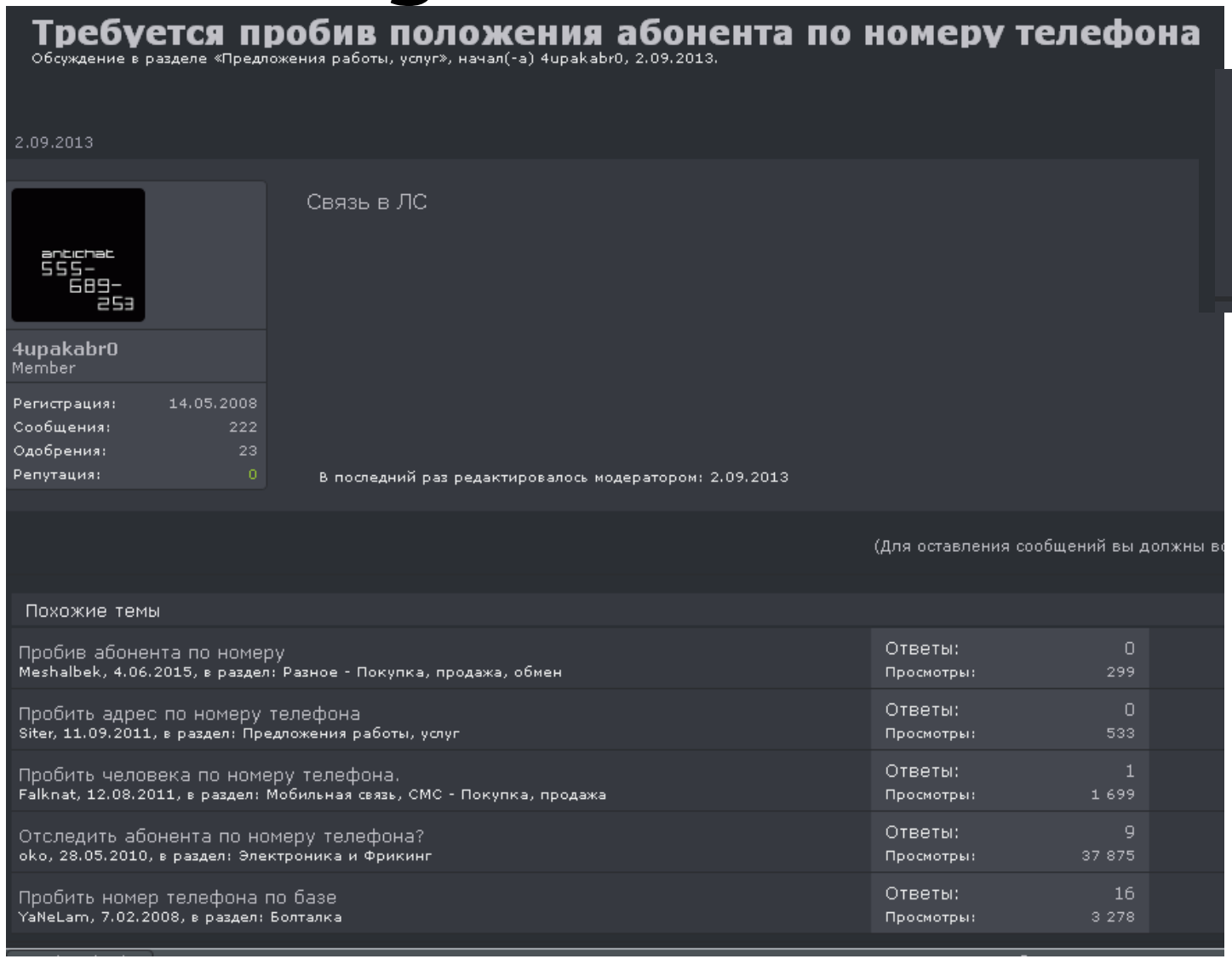
Bob

…and Track User Just Like SkyLock



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

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

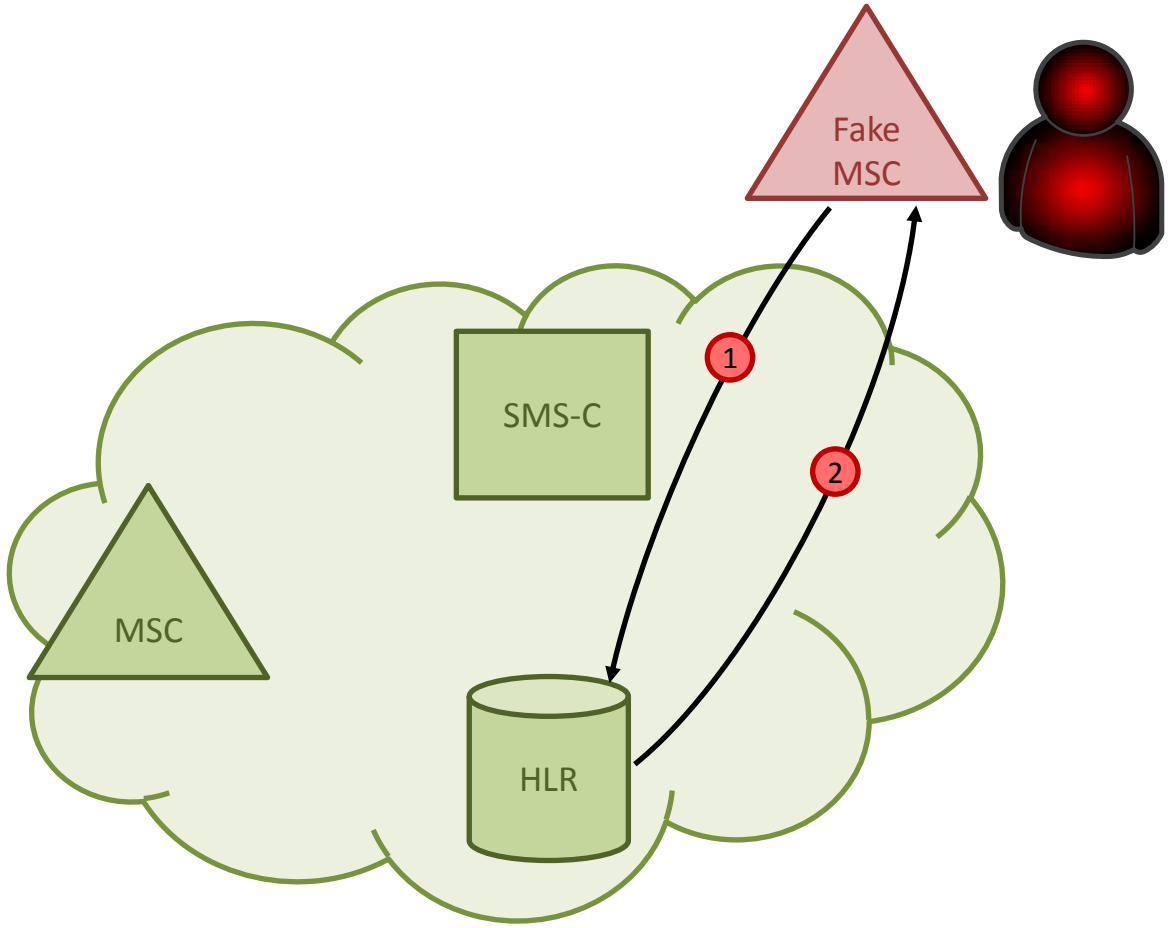
DoS / 阻斷服務攻擊

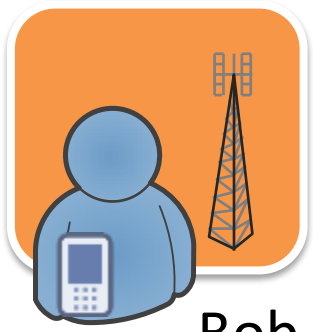
To make someone unavailable

To stop data leakage

What else?

Common Step 0 for Any Attack

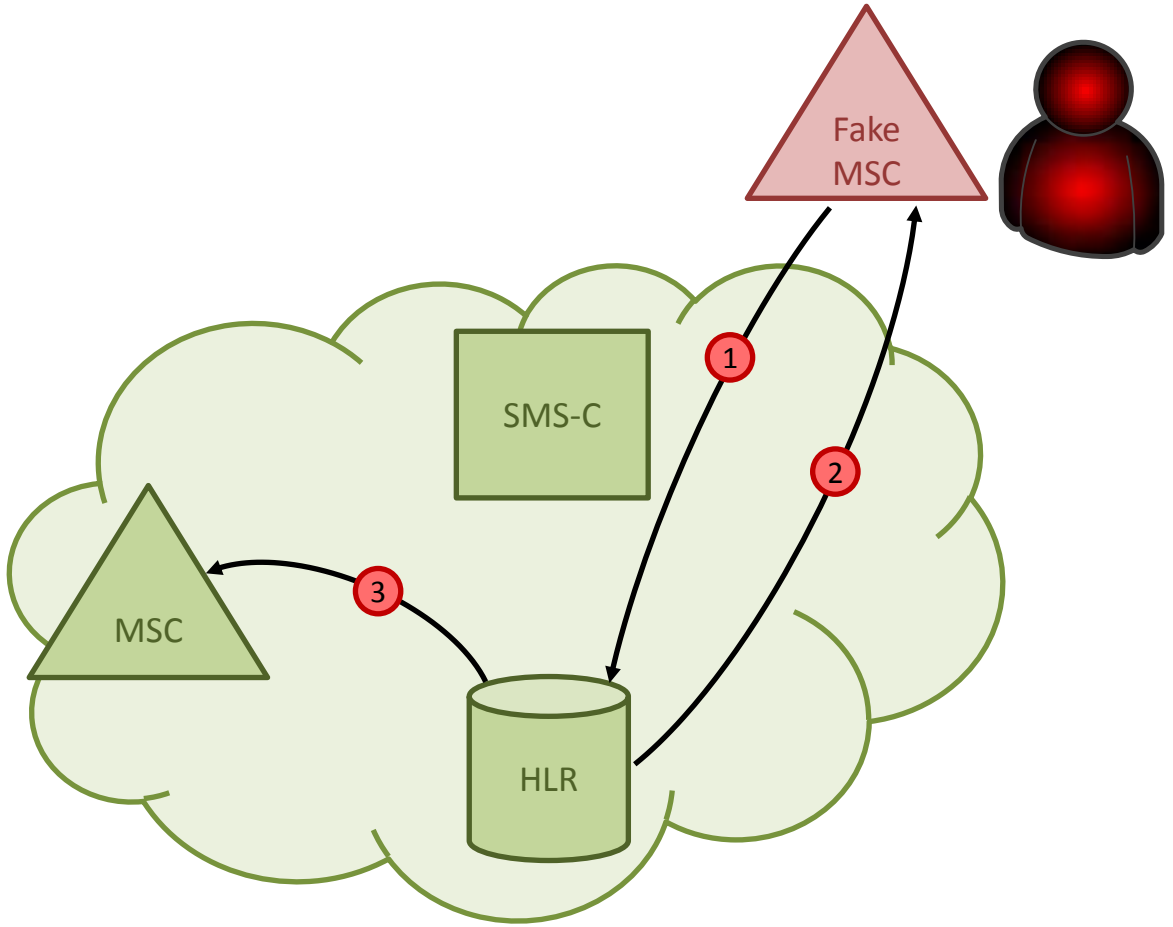




Bob

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

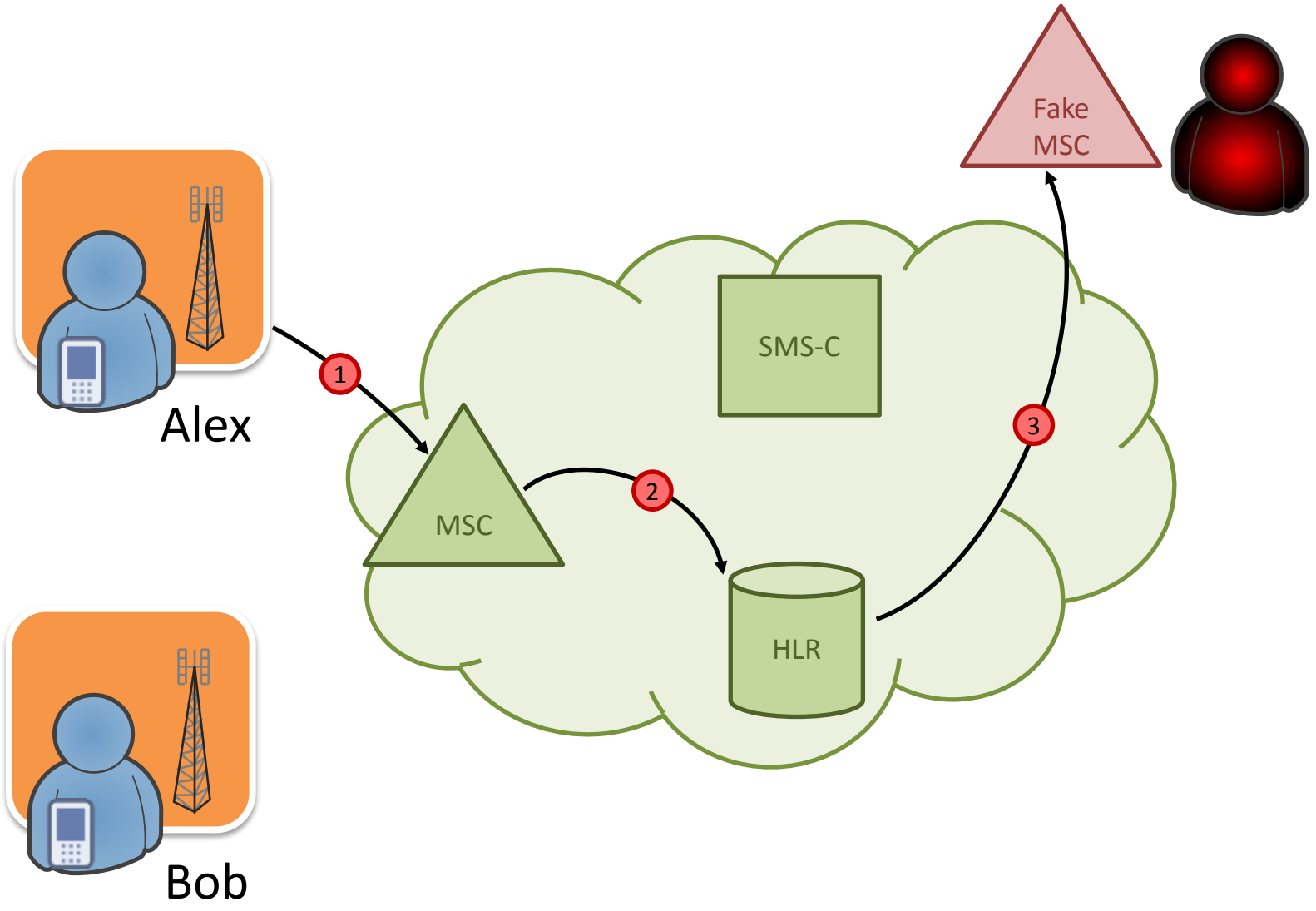
Denial of Service. Step 1



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

Bob

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

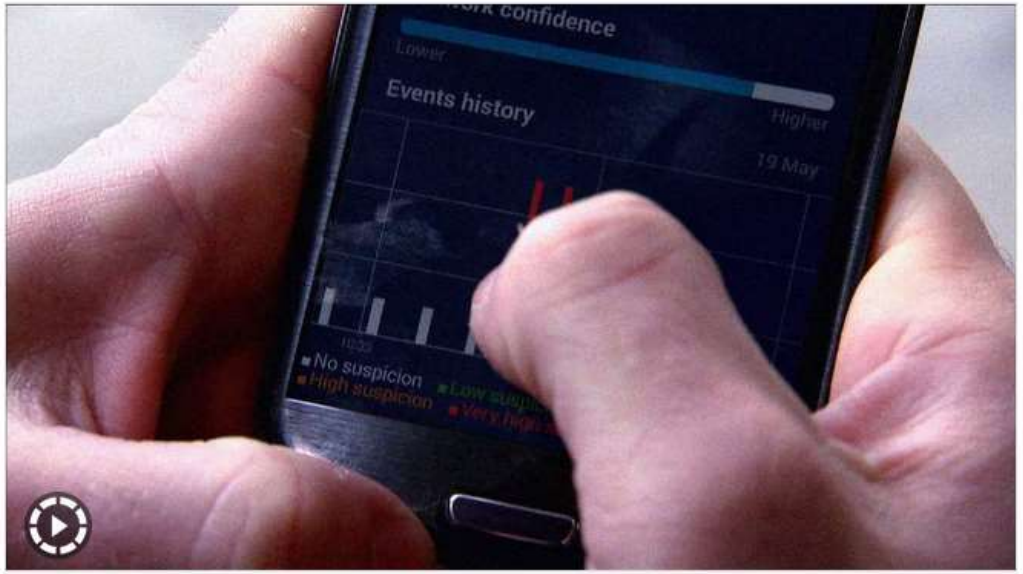
Interception / 截聽

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

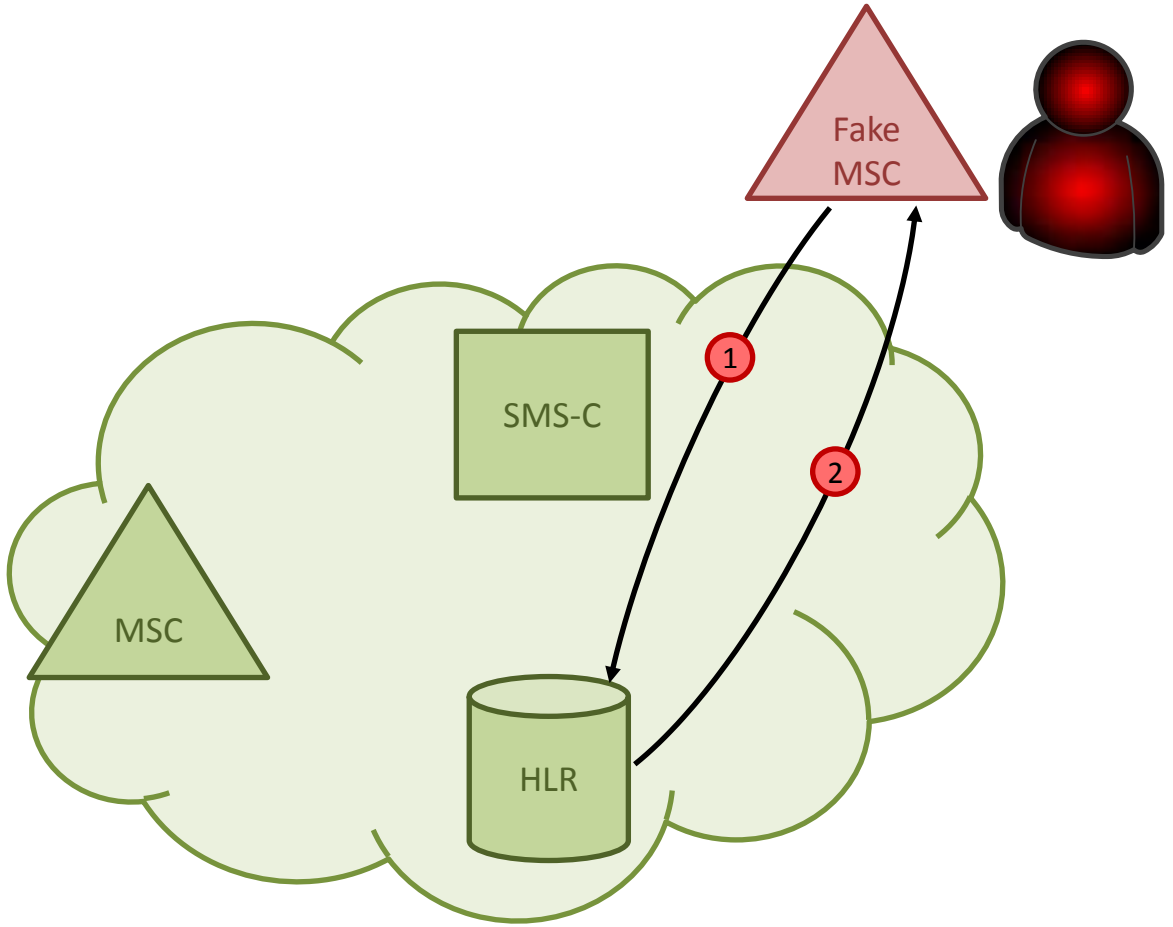
+ osmocomBB +

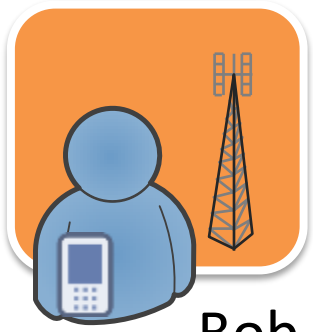
WIRESHARK

(f)or

$$7

Common Step 0 for Any Attack

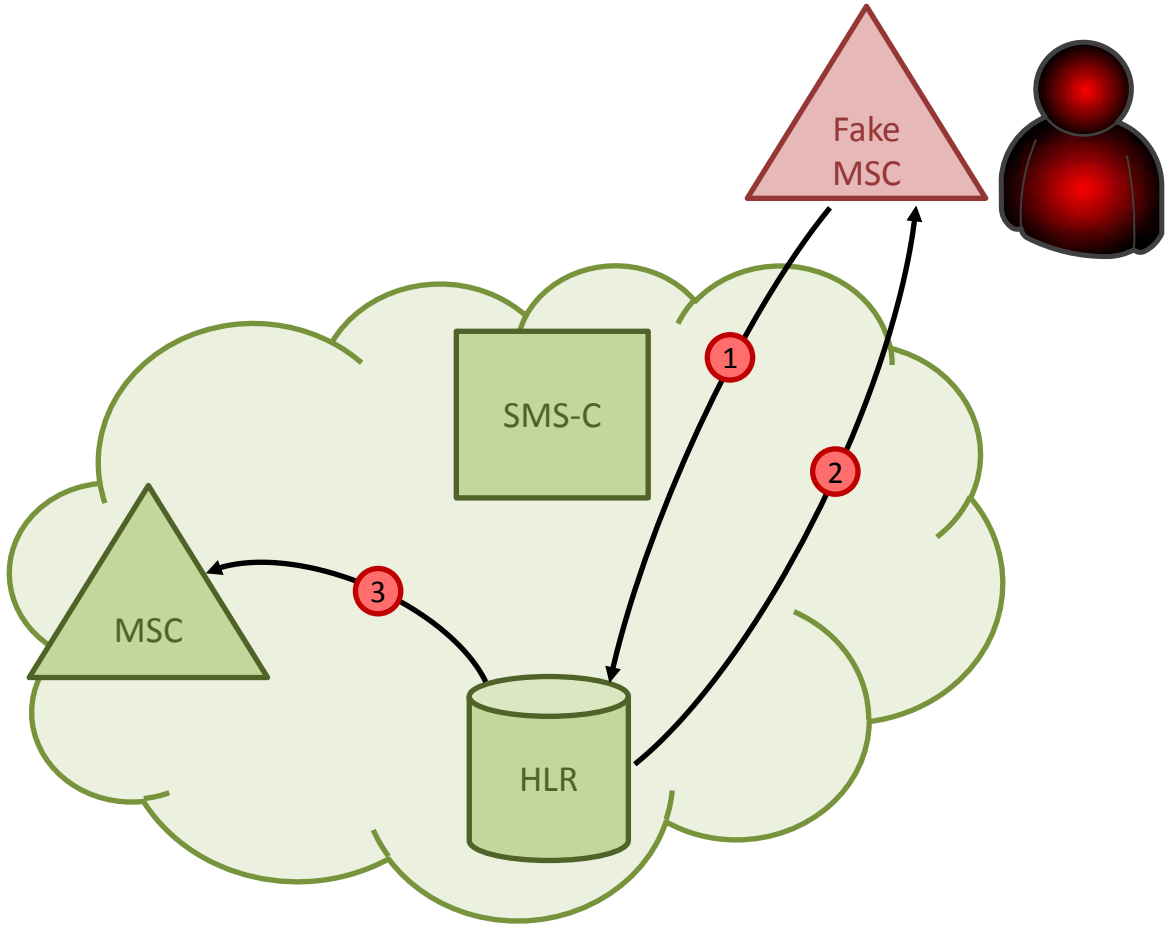




Bob

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

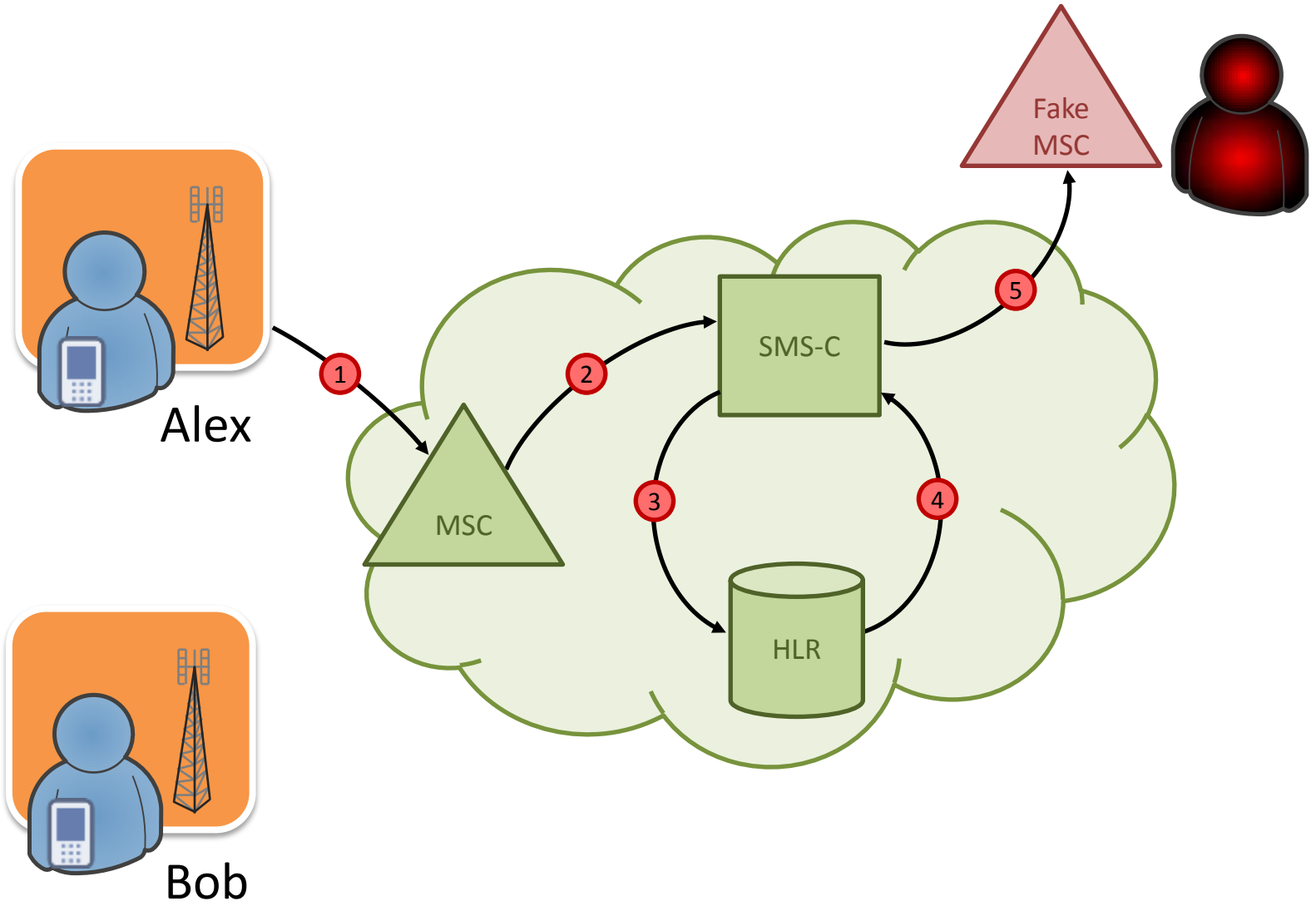
SMS Interception. Step 1



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

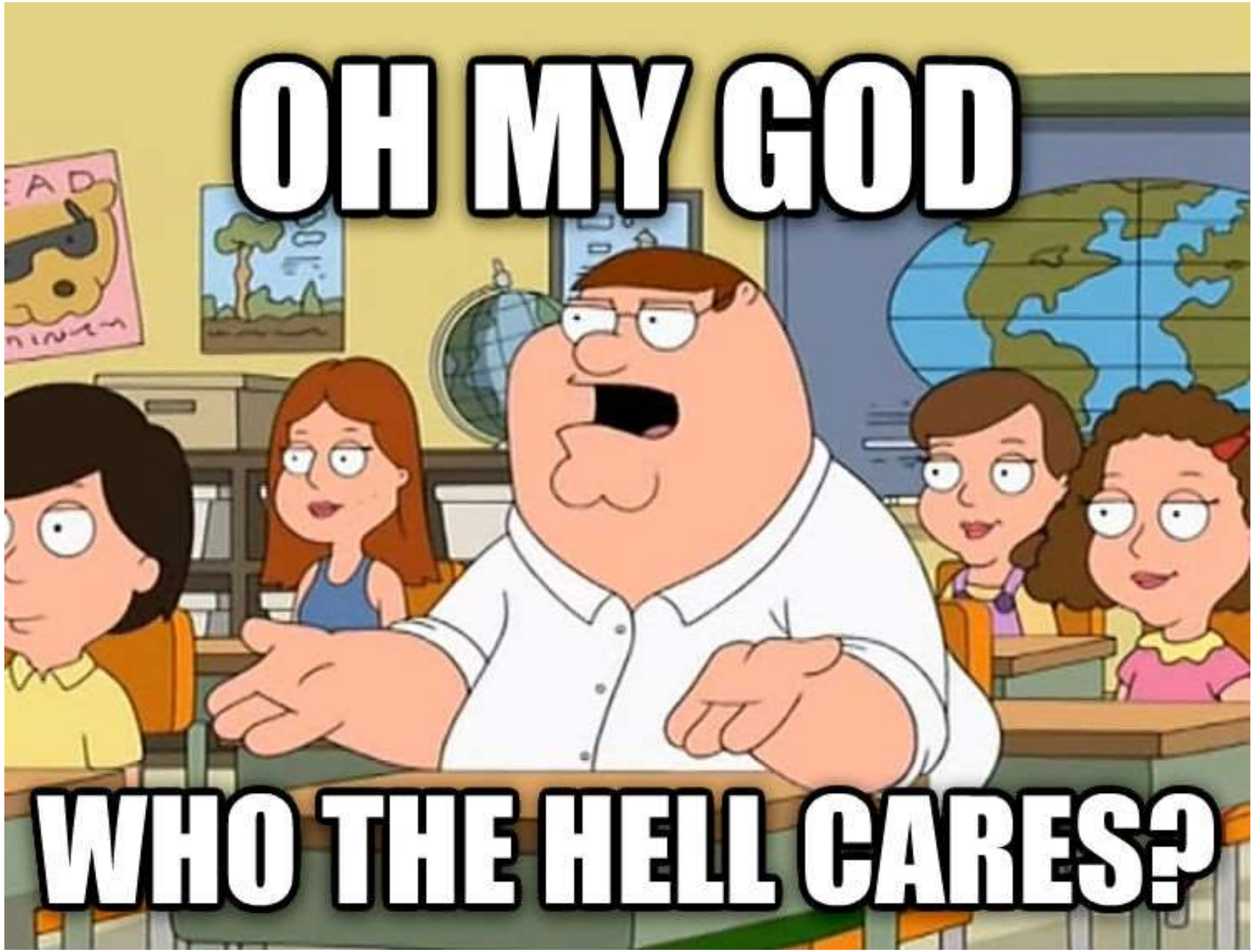
Bob

SMS Interception. Step 2



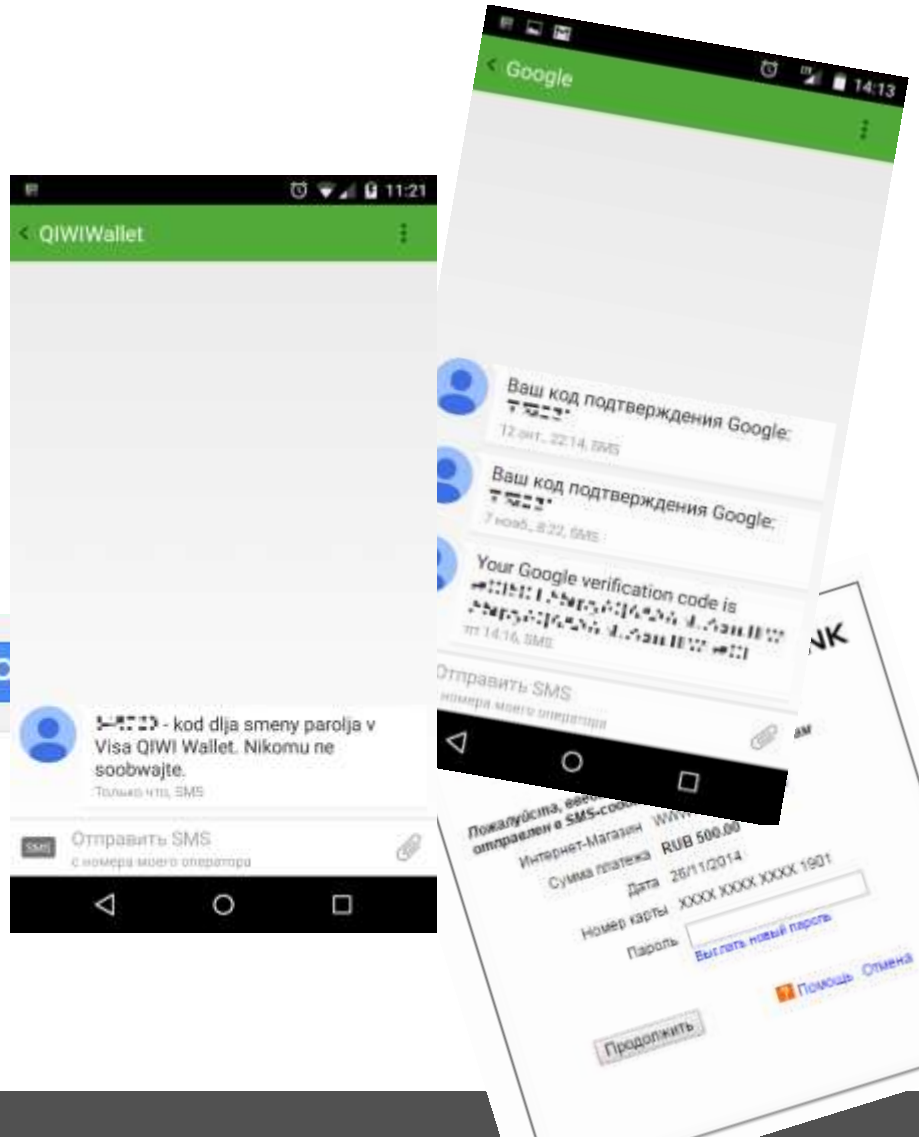
1. Alex sends SMS to Bob
2. MSC translates the SMS to SMS-C
3. SMS-C requests HLR for Bob`s location
4. HLR replies with a fake MSC address
5. SMS-C translates SMS to the fake MSC

demo


OH MY GOD
WHO THE HELL CARES?

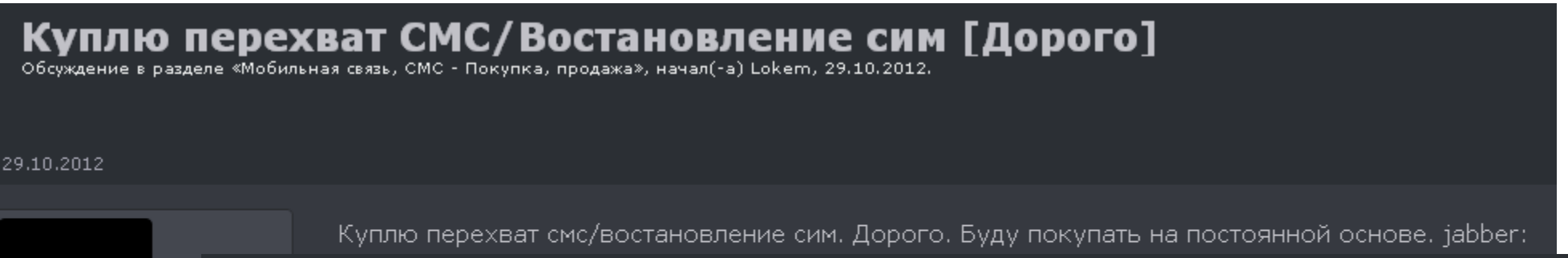
SMS Interception, We “Really Missed” You

- Access to payment service
- Recover passwords for email and social networks
- Online banking OTP

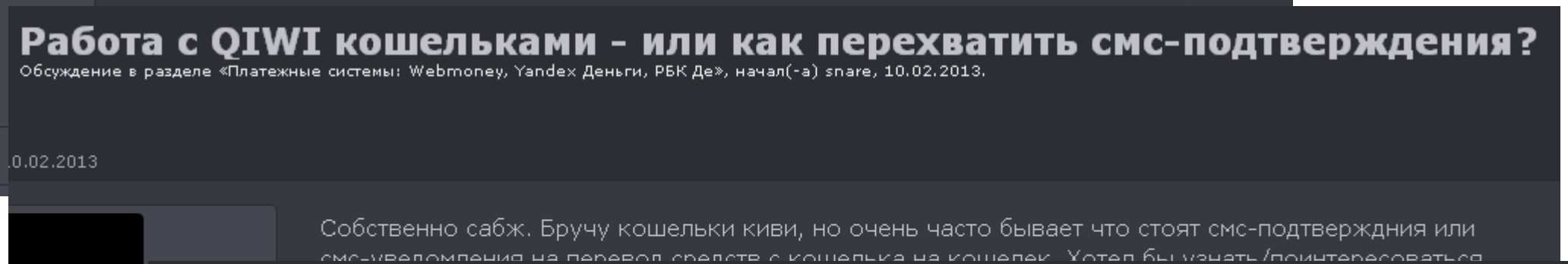


Illegal cases

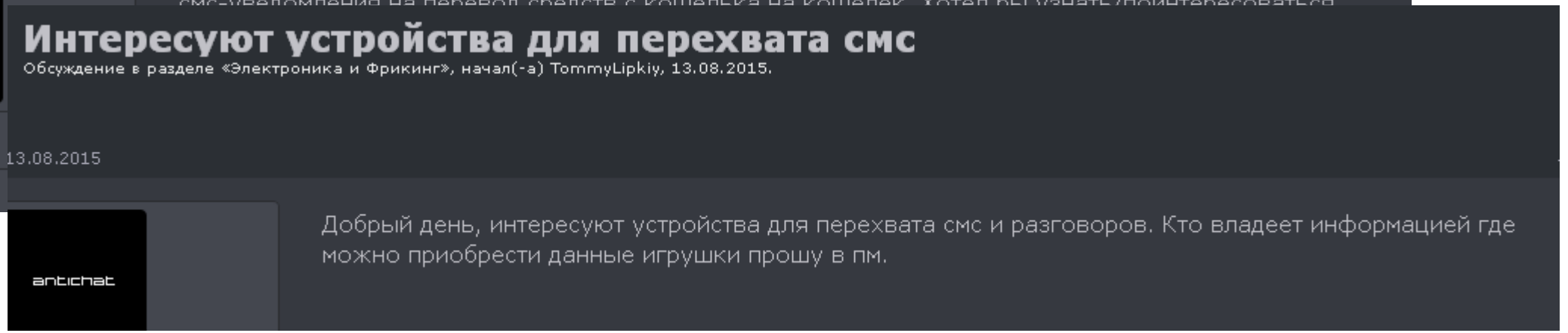
SMS Interception



Payment confirmation
SMS Interception



Devices for SMS Interception



Active actions and Impersonation

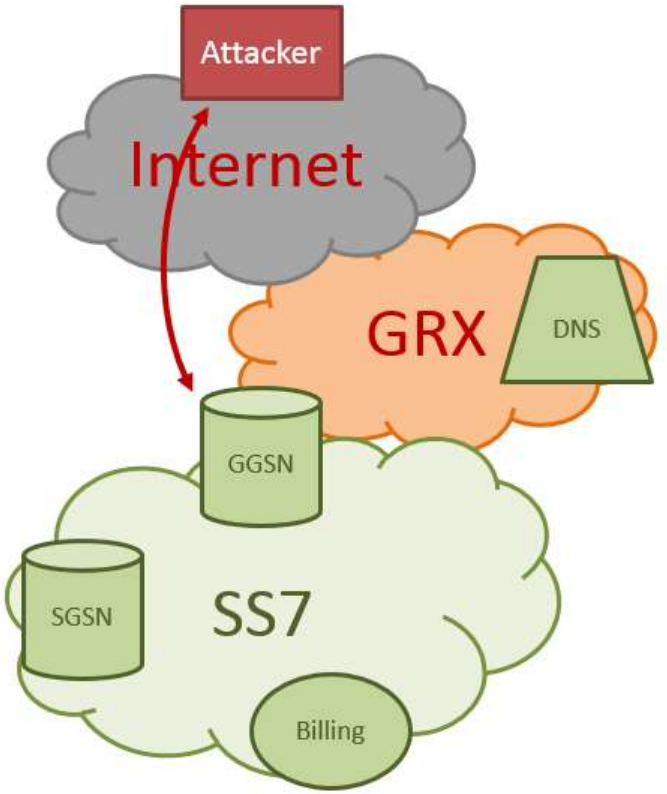
—Mobile balance transfer over USSD
—Premium Rate SMS Subscriptions
—Credit cards money transfers via phone
—Even fake calls from Victim number

How to Get Into SS7

How They Can Get Into SS7

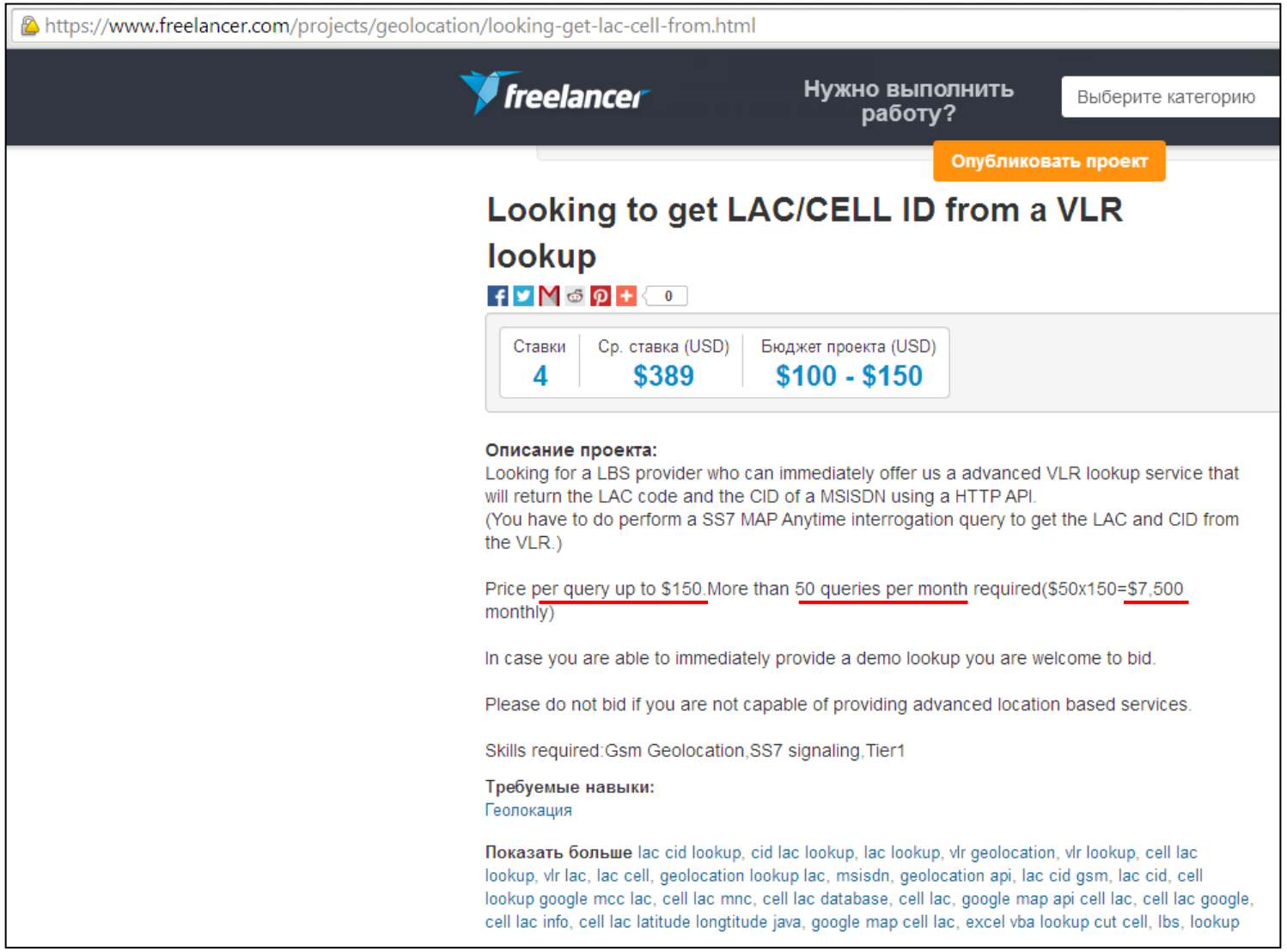
Legal with license
Semi legal without

Find a guy

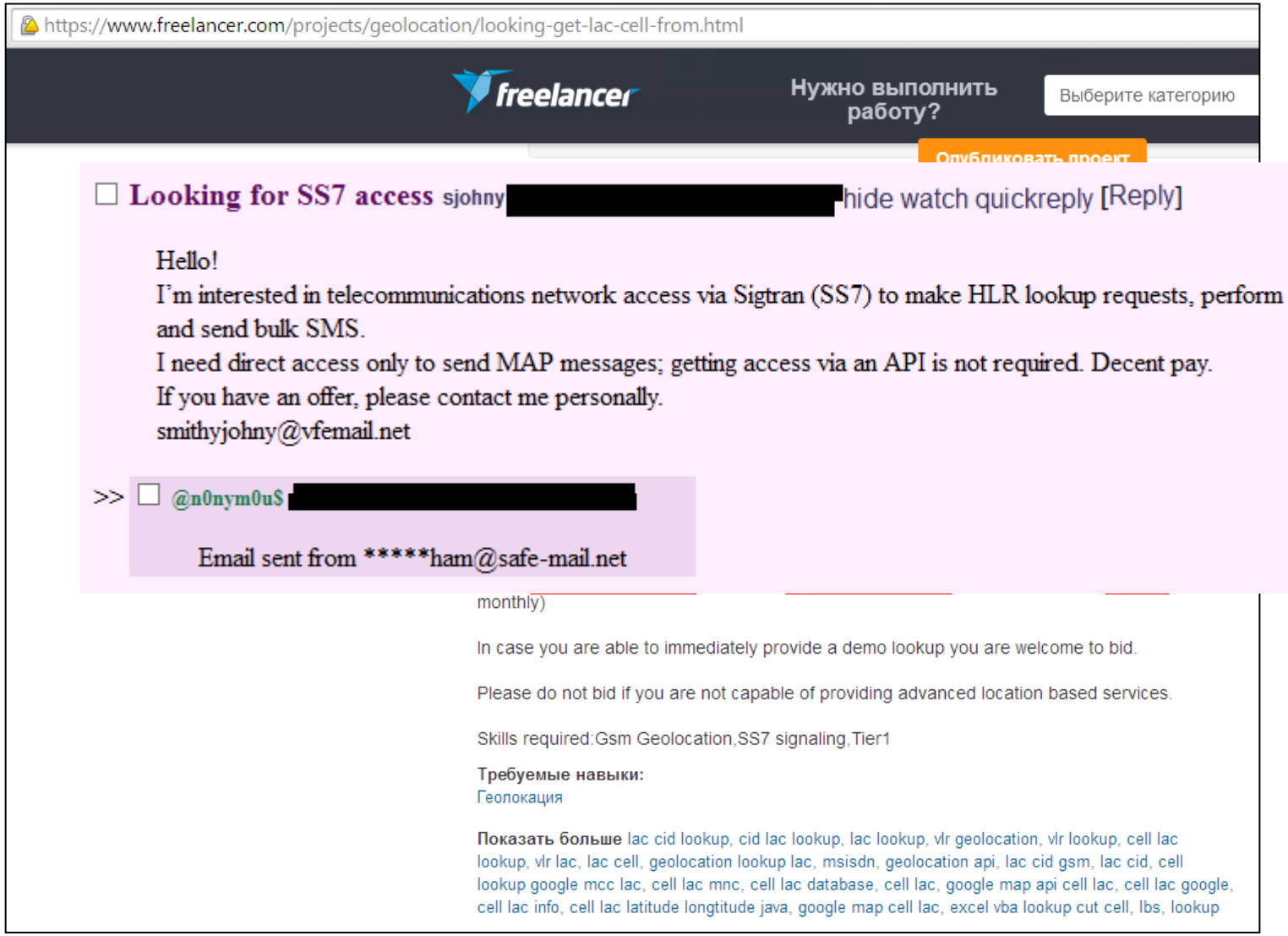


Hack border device

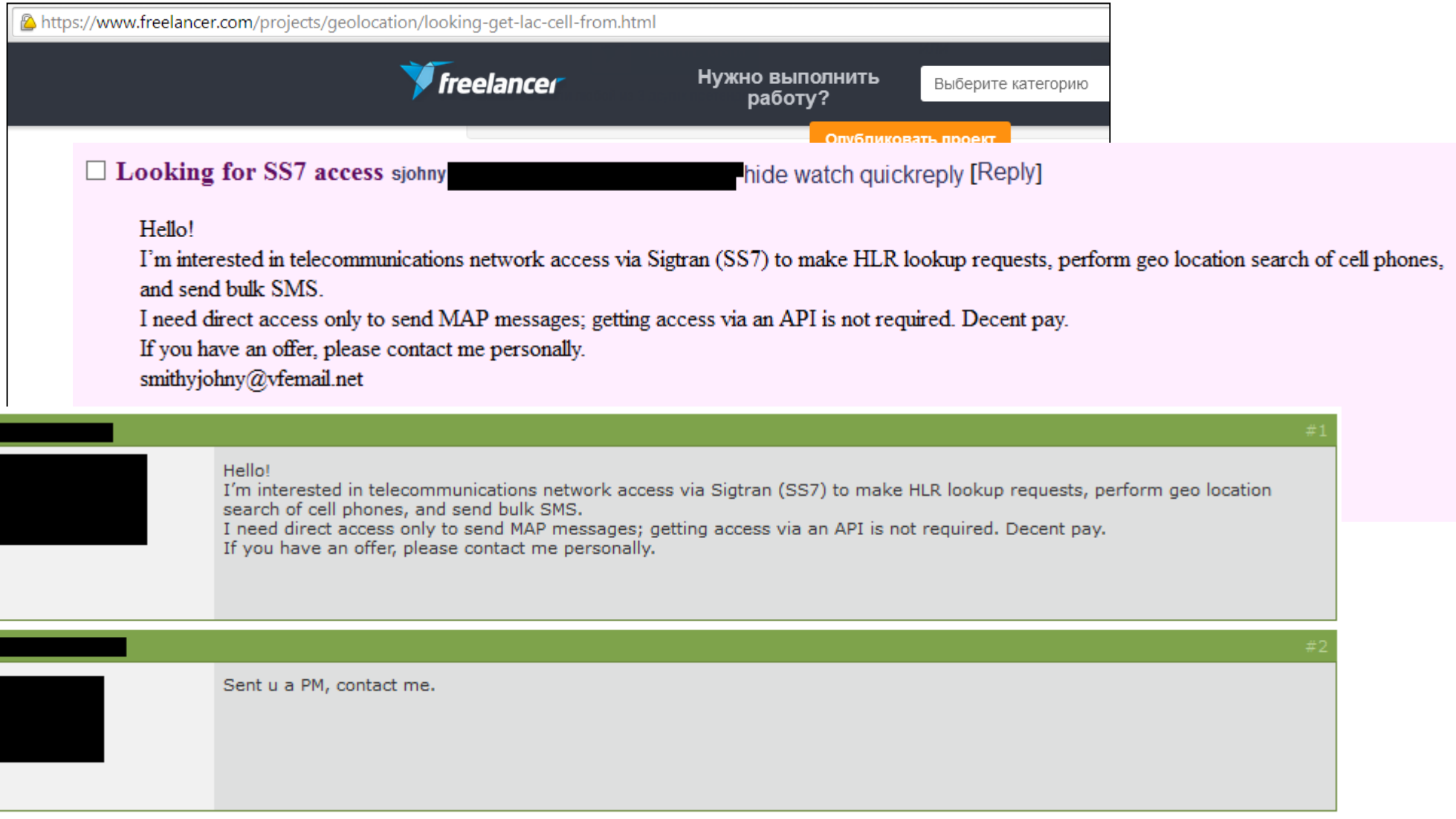
Find a Guy


https://www.freelancer.com/projects/geolocation/looking-get-lac-cell-from.html
freelancer
Нужно выполнить работу?
Выберите категорию
Опубликовать проект
Looking to get LAC/CELL ID from a VLR lookup
0
Ставки
4
Ср. ставка (USD)
$389
Бюджет проекта (USD)
$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

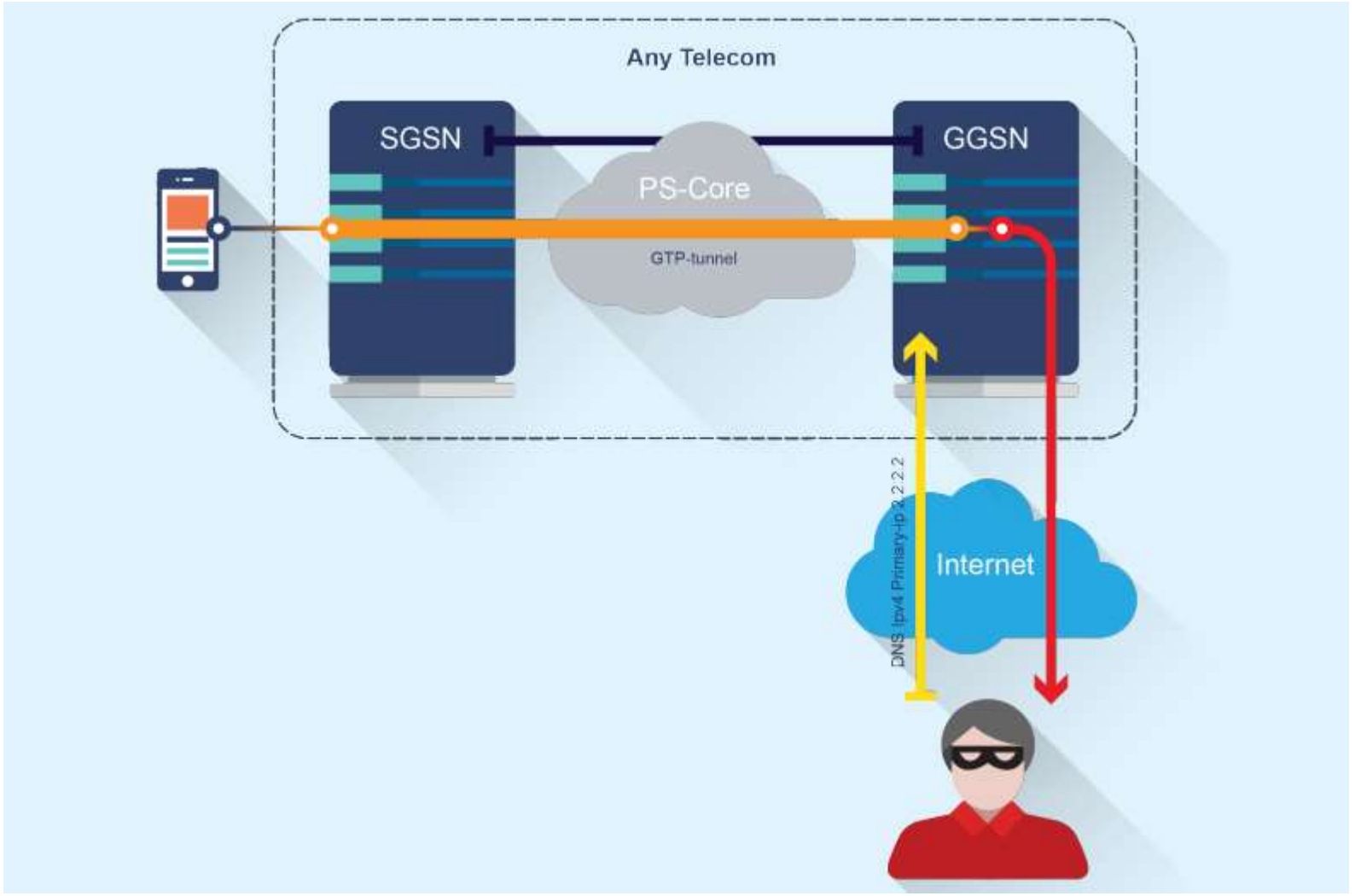
Find a Guy


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

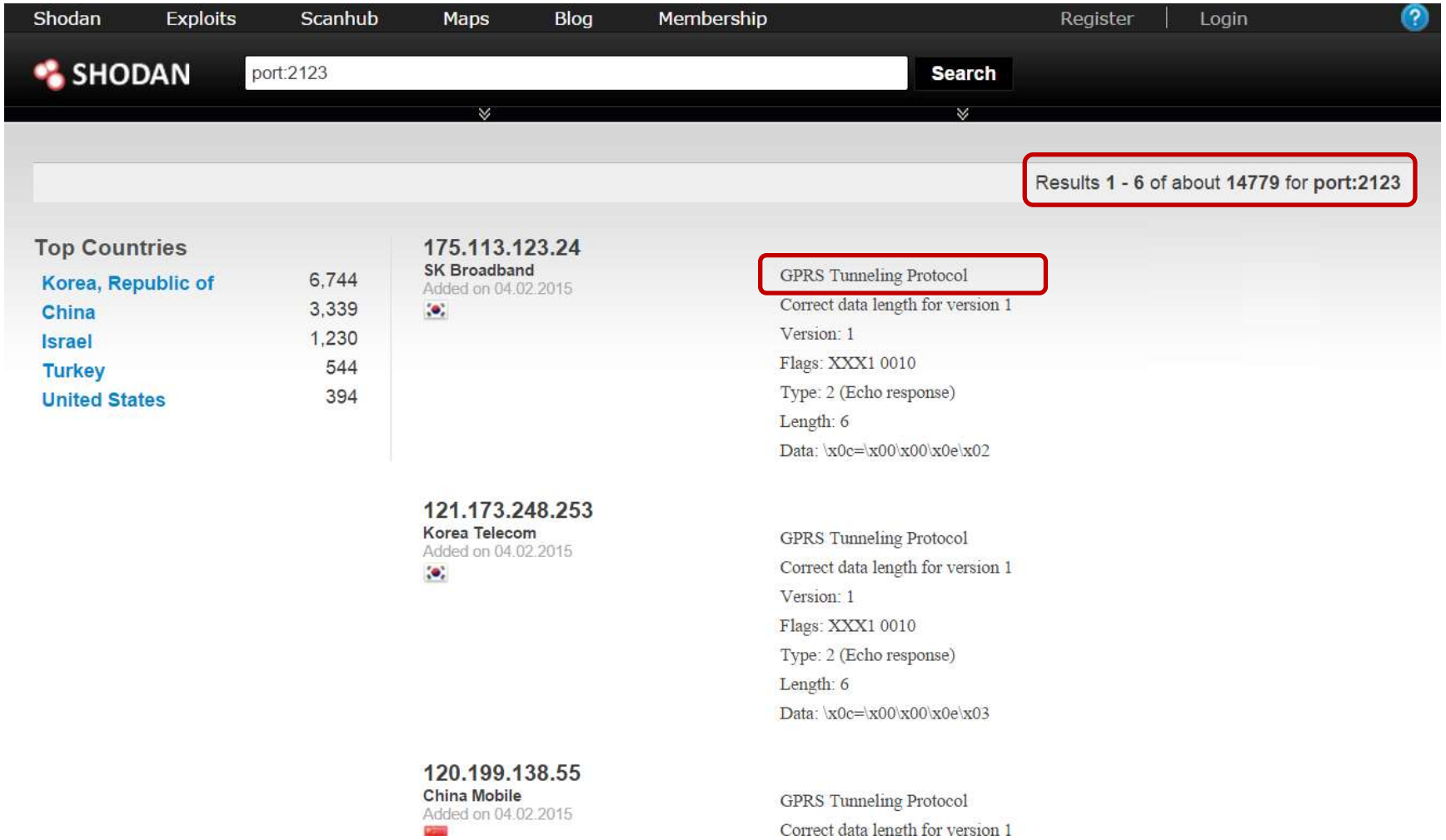
Find a Guy


https://www.freelancer.com/projects/geolocation/looking-get-lac-cell-from.html
freelancer
Нужно выполнить работу?
Выберите категорию
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
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
Offline
Sent u a PM, contact me.

Hack border device

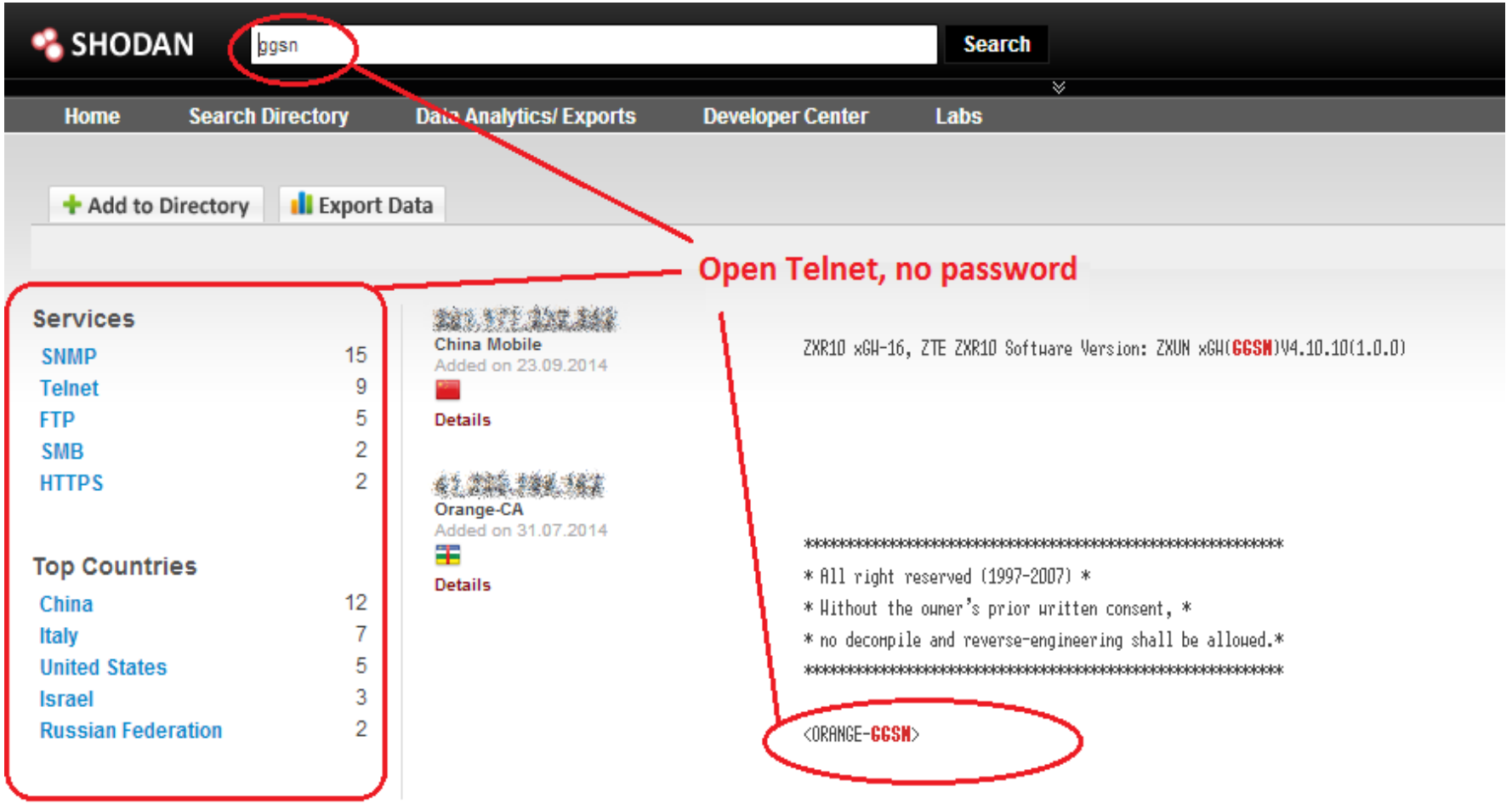


Today: IP Connectivity



Misconfiguration Example

Critical



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