Attacks on Telecom Operators and Mobile Subscribers via SS7

Dmitry Kurbatov
Security specialist
Positive Research
Yesterday: Closed Ecosystems
Today: Unified Technologies
Today: Common Interfaces
Today: IP Connectivity
Tomorrow: virtualization
Time Machine

Through SIGTRAN back to 1970’s
2014 was a good year for SS7 security

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
Topics

- USSD Money Transfer
- Short Message Interception
- DoS on Mobile Switching Center
- Fraud in SS7 network

- Hot for everyone
- Hot for mobile network operators
SS7 Network
Radio Part

Cell Phone
Base Transceiver Station
Base Station Controller
MSC/VLR
Mobile Switching Center
Visitor Location Register

SS7

Gateway MSC
SMS-C
HLR
Billing

MSC VLR

A
B
Gateway MSC
Gateway Mobile Switching Center

SS7

A

B

MSC VLR

Gateway MSC

SMS-C

HLR

Billing
SMS-C
Short Message Service Center
HLR
Homey Location Register
Billing
IDs

GT – Global Title  0 123 4567890
IDs

GT – Global Title  0 123 4567890

MSISDN – A or B mobile numbers  0 123 4567890
IDs

GT – Global Title  0 123 4567890

MSISDN – A or B mobile numbers  0 123 4567890

MSRN – Mobile Subscriber Roaming Number  0 123 4567890
IDs

GT – Global Title 0 123 4567890

MSISDN – A or B mobile numbers 0 123 4567890

MSRN – Mobile Subscriber Roaming Number 0 123 4567890

IMSI – International Mobile Subscriber Identity 15 digits
How to get in?
Core Networks
Access Networks

- LTE
- Wi-Fi
- WiMAX
- PON
- DSL
- Femto

UTRAN

Gateway MSC

SMS-C

MSC VLR

HLR

Billing

CS Core

PS Core

IMS

SS7

Access Networks

UTRAN

Gateway MSC

SMS-C

MSC VLR

HLR

Billing

CS Core

PS Core

IMS

SS7
Exchange Points

LTE
Wi-Fi
WiMAX
PON
DSL
Femto

UTRAN

MSC
VLR

Gateway
MSC

SMS-C

HLR

Billing

CS Core

GRX/IPX

SS7

PS Core

IMS
Support

LTE
Wi-Fi
WiMAX
PON
DSL
Femto

UTRAN

GRX/IPX

OAM
Remote support

SS7

Gateway
MSC

SMS-C

MSC
VLR

HLR

Billing

CS Core

PS Core

IMS

POSITIVE TECHNOLOGIES

A

B

Support
Threat

Attacker

OAM Remote support

IT network

GRX/IPX

Attacker

LTE

Wi-Fi

WiMAX

PON

DSL

Femto

Attacker

LTE

Wi-Fi

WiMAX

PON

DSL

Femto

Attacker

CS Core

MSC

VLR

MSC

VLR

UNTRAN

Gateway
MSC

SMS-C

HLR

Billing

PS Core

Internet

IMS

GRX/IPX

Remote support

OAM

Attacker

IT network

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker

Internet

Attacker
SMS Interception
Collect info

We know
B-Number 0 123 4567802
Collect info

We know
B-Number 0 123 4567802

sendRoutingInfoForSM
I am SMSC.
My GT 1 321 4567801.
Where is Subscriber-B MSISDN 0 123 4567802?

A

B
Collect info

We know

**B-Number 0 123 4567802**

---

**sendRoutingInfoForSM**

I am HLR 0 123 4567800

MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits
Collect info

We know
B-Number 0 123 4567802
HLR 0 123 4567800
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits

sendRoutingInfoForSM
I am SMSC.
My GT 1 321 4567801.
Where is Subscriber-B MSISDN 0 123 4567802?

sendRoutingInfoForSM
I am HLR 0 123 4567800
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits
Spoof MSC

updateLocation
I am MSC/VLR.
My GT 1 321 4567801.
I serve Subscriber-B IMSI 15 digits.

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits
Spoof MSC

Attacker serves Subscriber-B

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits

HLR stores
Subscriber-B IMSI 15 digits
MSC/VLR 1 321 4567801
SMS interception

“Hi, meet at 8pm at Baker Street”
SMS interception

“Hi, meet at 8pm at Baker Street”

sendRoutingInfoForSM
I am SMSC.
My GT 0 123 4567804.
Where is Subscriber-B MSISDN 0 123 4567802?
Hi, meet at 8pm at Baker Street

sendRoutingInfoForSM
I am HLR 0 123 4567800
MSC/VLR 1 321 4567801
Subscriber-B IMSI 15 digits

HLR sends Attacker address instead of real MSC!

sendRoutingInfoForSM
I am SMSC.
My GT 0 123 4567804.
Where is Subscriber-B MSISDN 0 123 4567802?
SMS interception

"Hi, meet at 8pm at Baker Street"

sendRoutingInfoForSM
I am HLR 0 123 4567800
MSC/VLR 1 321 4567801
Subscriber-B IMSI 15 digits

SMS-C routes this SMS to the received address.

sendRoutingInfoForSM
I am SMSC.
My GT 0 123 4567804.
Where is Subscriber-B MSISDN 0 123 4567802?
SMS interception

“Hi, meet at 8pm at Baker Street”

sendRoutingInfoForSM
I am HLR 0 123 4567800
MSC/VLR 1 321 4567801
Subscriber-B IMSI 15 digits

SMS-C routes this SMS to the received address.

sendRoutingInfoForSM
I am SMSC.
My GT 0 123 4567804.
Where is Subscriber-B MSISDN 0 123 4567802?
SMS interception

1. SMS chats
2. One time passwords
3. Notifications
4. Password recovery
Money Transfer
Using USSD
Collect info

We know

B-Number 0 123 4567802
Collect info

We know
B-Number 0 123 4567802

sendRoutingInfoForSM
I am SMSC.
My GT 1 321 4567801.
Where is Subscriber-B MSISDN 0 123 4567802?

A

B

SS7

Attacker as SMSC

SRI4SM

Gateway MSC

MSC VLR

HLR
Collect info

We know
B-Number 0 123 4567802
HLR 0 123 4567800
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits

sendRoutingInfoForSM
I am SMSC.
My GT 1 321 4567801.
Where is Subscriber-B MSISDN 0 123 4567802?

sendRoutingInfoForSM
I am HLR 0 123 4567800
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits
Send USSD 1

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits

*100#
Send USSD 1

processUnstructuredSS-Request
I am MSC/VLR.
Request how much money has subscriber with IMSI 15 digits?

processUnstructuredSS-Request
Subscriber’s account is $$$$$.

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits
Account info.
Send USSD 1

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits
Account info.

processUnstructuredSS-Request
I am MSC/VLR.
Request how much money has

processUnstructuredSS-Request
Subscriber’s account is $$$$$.

B
Send USSD 2

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits
Account info.

*123*01238765400*100#
Send USSD 2

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits
Account info.

processUnstructuredSS-Request
I am MSC/VLR.
Transfer money from IMSI 15 digits to my mobile account.
Send USSD 2

processUnstructuredSS-Request
I am MSC/VLR.
Transfer money from IMSI 15 digits to my mobile account.

Real account info.

Subscriber B does not get SMS notification if Attacker combines this attack and the previous one.
Send USSD 2

processUnstructuredSS-Request
I am MSC/VLR.
Transfer money from IMSI 15 digits to my mobile account.

Subscriber B does not get SMS notification if Attacker combines this attack and the previous one.
Mobile Switching Center DoS
Collect info

We know
B-Number 0 123 4567802
Collect info

sendRoutingInfoForSM
I am SMSC.
My GT 1 321 4567801.
Where is Subscriber-B MSISDN 0 123 4567802?

We know
B-Number 0 123 4567802
Collect info

We know
B-Number 0 123 4567802
HLR 0 123 4567800
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits

sendRoutingInfoForSM
I am HLR 0 123 4567800
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits
Make it starve

SS7

We know
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits

provideRoamingNumber
I am HLR.
My GT 1 321 4567801.
Provide MSRN for
Subscriber-B IMSI 15 digits.
Make it starve

We know
MSC/VLR  0 123 4567803
Subscriber-B IMSI 15 digits
MSRN 0 123 4560001
Make it starve

Default timeouts for MSRN:
- Ericsson – 30 sec
- Huawei – 45 sec

We know
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits
MSRN 0 123 4560001

provideRoamingNumber
MSRN 0 123 4560001
Make it starve

We know
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits
MSRN 0 123 4560001
...
MSRN 0 123 4569999
Make it starve

We know
MSC/VLR  0 123 4567803
Subscriber-B IMSI 15 digits
MSRN 0 123 4560001
...
MSRN 0 123 4569999

provideRoamingNumber
I am HLR.
My GT 1 321 4567801.
Provide MSRN for Subscriber-B IMSI 15 digits.
Make it starve

We know
MSC/VLR  0 123 4567803
Subscriber-B IMSI 15 digits
MSRN 0 123 4560001
...
MSRN 0 123 4569999

noRoamingNumberAvailable
Make it starve

We know
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits
MSRN 0 123 4560001
...
MSRN 0 123 4569999

noRoamingNumberAvailable
DoS

SS7
Attacker as HLR
Real HLR

10k – 500k

MSC
VLR

Gateway
MSC

HLR

POSITIVE TECHNOLOGIES
DoS

provideRoamingNumber
I am HLR.
My GT 13214568701.
Provide MSRN for
Subscriber-ANY IMSI 15 digits.

10k – 500k

SS7

Attacker as HLR

Real HLR

PRN

MSC

VLR

Gateway MSC

HLR
DoS

SS7
Attacker as HLR

Real HLR

PRN 3

noRoamingNumberAvailable
DoS

No incoming calls

10k – 500k

SS7

Attacker as HLR

Real HLR

PRN 3

MSC

Gateway MSC

VLR

HLR

Sad calling party

No incoming calls

10k – 500k
Fraud in SS7
SS7 interconnection

Trusted environment
Leadership team

CSO  CEO  CMO  CLO  CCO

Gateway  MSC  VLR  MSC
    SMS-C
    HLR
    Billing
Leadership team

Really?!
Trust them?
Uncharged calls
Collect info

We know
B-Number 0 123 4567802
Collect info

We know
B-Number 0 123 4567802

sendRoutingInfoForSM
I am SMSC.
My GT 1 321 4567801.
Where is Subscriber-B MSISDN 0 123 4567802?
Collect info

We know
B-Number 0 123 4567802
HLR 0 123 4567800
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits

sendRoutingInfoForSM
I am HLR 0 123 4567800
MSC/VLR 0 123 4567803
Subscriber-B IMSI 15 digits
Spoof MSC

updateLocation
I am MSC/VLR.
My GT 1 321 4567801.
I serve Subscriber-B IMSI 15 digits.

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits
**Spoof MSC**

**updateLocation**
I am MSC/VLR.
My GT 1 321 4567801.
I serve Subscriber-B IMSI 15 digits.

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits
Spoof MSC

Attacker serves Subscriber-B

We know
HLR 0 123 4567800
Subscriber-B IMSI 15 digits

HLR stores
Subscriber-B IMSI 15 digits
MSC/VLR 1 321 4567801
Forward a call

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

Gateway MSC knows nothing
Forward a call

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

sendRoutingInfo
Where is Subscriber-B MSISDN 0 123 4567802 =
Where is Subscriber-B located?
Forward a call

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

provideSubscriberInfo
I am HLR.
My GT 0 123 4567800.
Provide location for the Subscriber-B.
Forward a call

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

provideSubscribedInfo
Subscriber-B is in the Home network.
Forward a call

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

GatewayMSC knows that Subscriber-B is at home.

This information will be sent to a billing platform.
Forward a call

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

sendRoutingInfo
Where is Subscriber-B MSISDN 0 123 4567802 located =
What is MSRN for Subscriber-B?
Forward a call

SS7

Attacker as MSC

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

provideRoamingNumber
I am HLR.
My GT 0 123 4567800.
Provide MSRN for Subscriber-B IMSI 15 digits.
Forward a call

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

provideRoamingNumber MSRN 39 0 654832169
Forward a call

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

Gateway MSC knows
Subscriber-B
MSRN 39 0 654832169

A

B
Forward a call to... Italy

HLR stores
Subscriber-B
MSISDN 0 123 4567802
IMSI 15 digits
MSC/VLR 1 321 4567801

GatewayMSC knows
Subscriber-B
MSRN 39 0 654832169
Forward a call to...

**HLR stores**
- **Subscriber-B**
  - MSISDN: 0 123 4567802
  - IMSI: 15 digits
- **MSC/VLR**: 1 321 4567801

**Gateway MSC knows**
- **Subscriber-B**
  - MSRN: 39 0 654832169
Demo
Who pays?

Call from A to B while at “home” = ₽ 1,60

Call from A to Italy = ₽ 30,00
Who pays?

Call from A to B while at “home” = ₽ 1,60

Call from A to Italy = ₽ 30,00

₽ 30,00 - ₽ 1,60 = ₽ 28,40 – Attacker profit
Who pays?

Call from A to B while at “home” = ₽ 1,60

Call from A to Italy = ₽ 30,00

International calls on 5.3% of original price

₽ 30,00 - ₽ 1,60 = ₽ 28,40 – Attacker’s profit

How much does a mobile operator lose?
To Do:
SS7 Firewall or IDS with evolution to IPS?
IDS Scheme

SS7 National

SS7 International

SS7 Other PLMNs

SS7 taps

Duplicate traffic

SS7 IDS & Event correlation

STP

Duplicate traffic

Duplicate traffic

SS7 taps
Research Updates

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

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

Dmitry Kurbatov
dkurbatov@ptsecurity.com