Dmitry Kurbatov

Sergey Puzankov

Vladimir Kropotov

Fractured Backbones – Incidents Detection and Forensics in Telco Networks

POSITIVE TECHNOLOGIES

ptsecurity.com

About us

POSITIVE TECHNOLOGIES

Joint research of Incident Response and Telco Security Teams

Introduction

Technologies behind telco networks

What we use today and
what technology lies
at the heart of it

Mobile internet
Social networks
Messengers
Online banking
Internet of Things

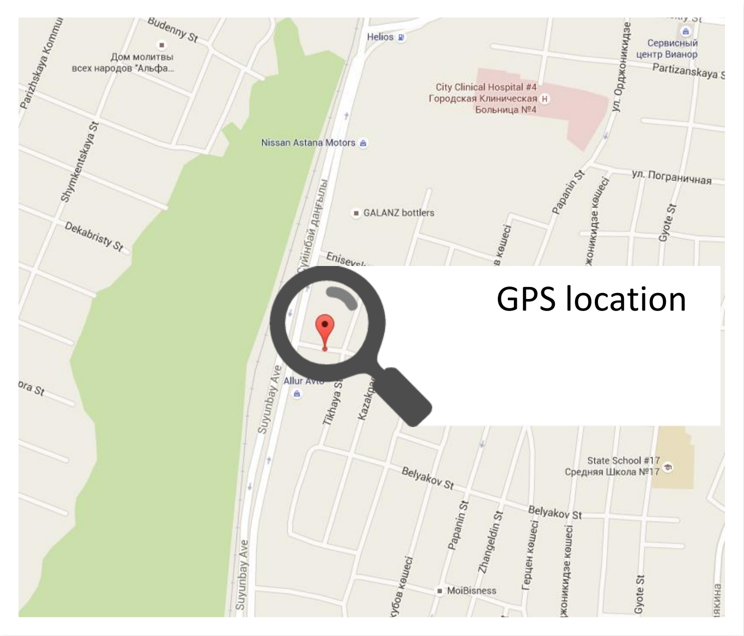
Mobile communication
developed in the 2000s

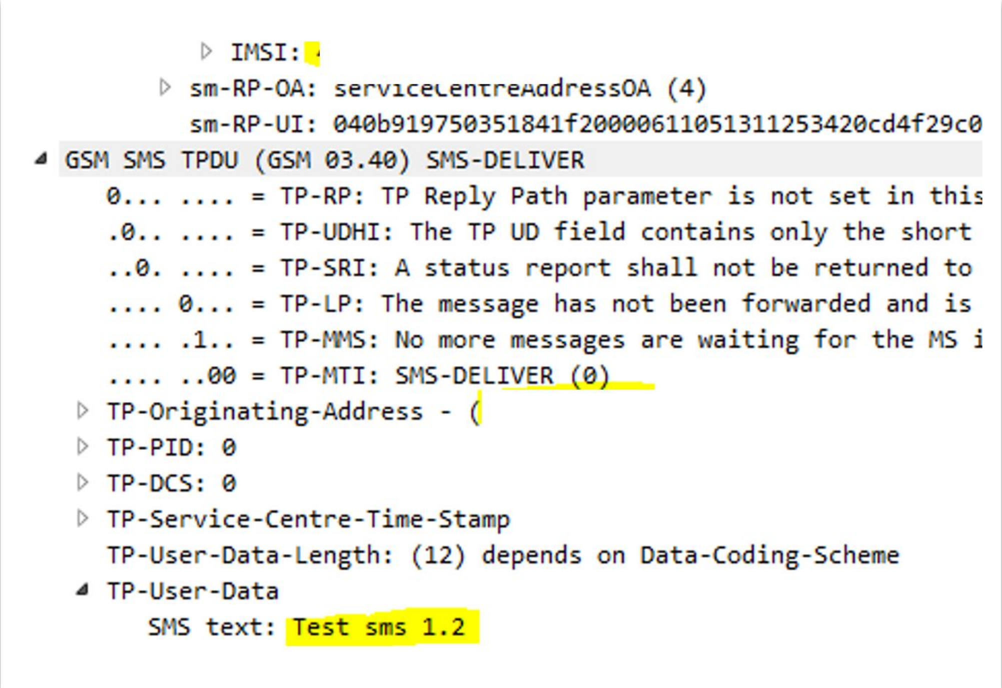
SS7 network
developed in the 1970s – 1990s

Types of Incidents

- Subscriber location tracking
- Call interception (wiretapping)
- SMS interception and spoofing
- DoS, including balance DoS
- Other Fraudulent activities

Phone number
+7 777 5555555

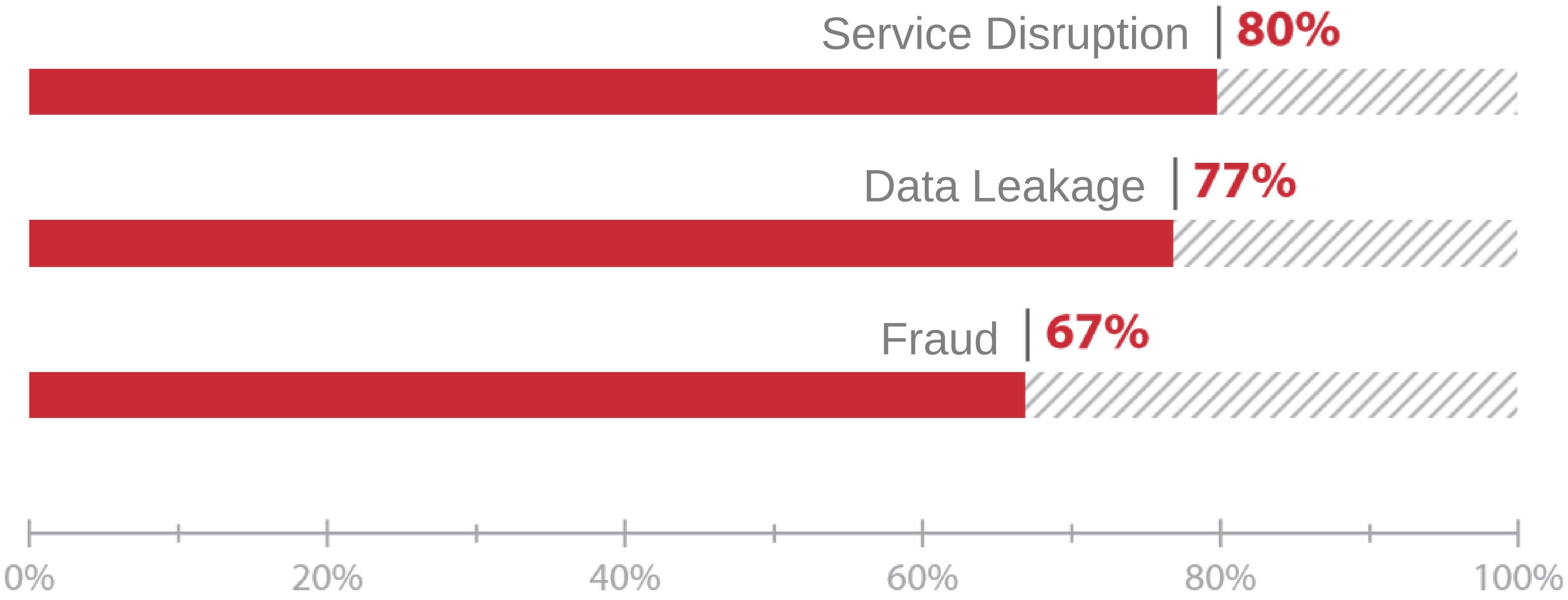




```
            ▷ IMSI:
        ▷ sm-RP-OA: serviceCentreAddressOA (4)
          sm-RP-UI: 040b919750351841f200006110513112534 20cd4f29c0
◢ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this
    .0.. .... = TP-UDHI: The TP UD field contains only the short
    ..0. .... = TP-SRI: A status report shall not be returned to
    .... 0... = TP-LP: The message has not been forwarded and is
    .... .1.. = TP-MMS: No more messages are waiting for the MS i
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (
  ▷ TP-PID: 0
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (12) depends on Data-Coding-Scheme
  ◢ TP-User-Data
      SMS text: Test sms 1.2
```

Incidents statistics. Major threats

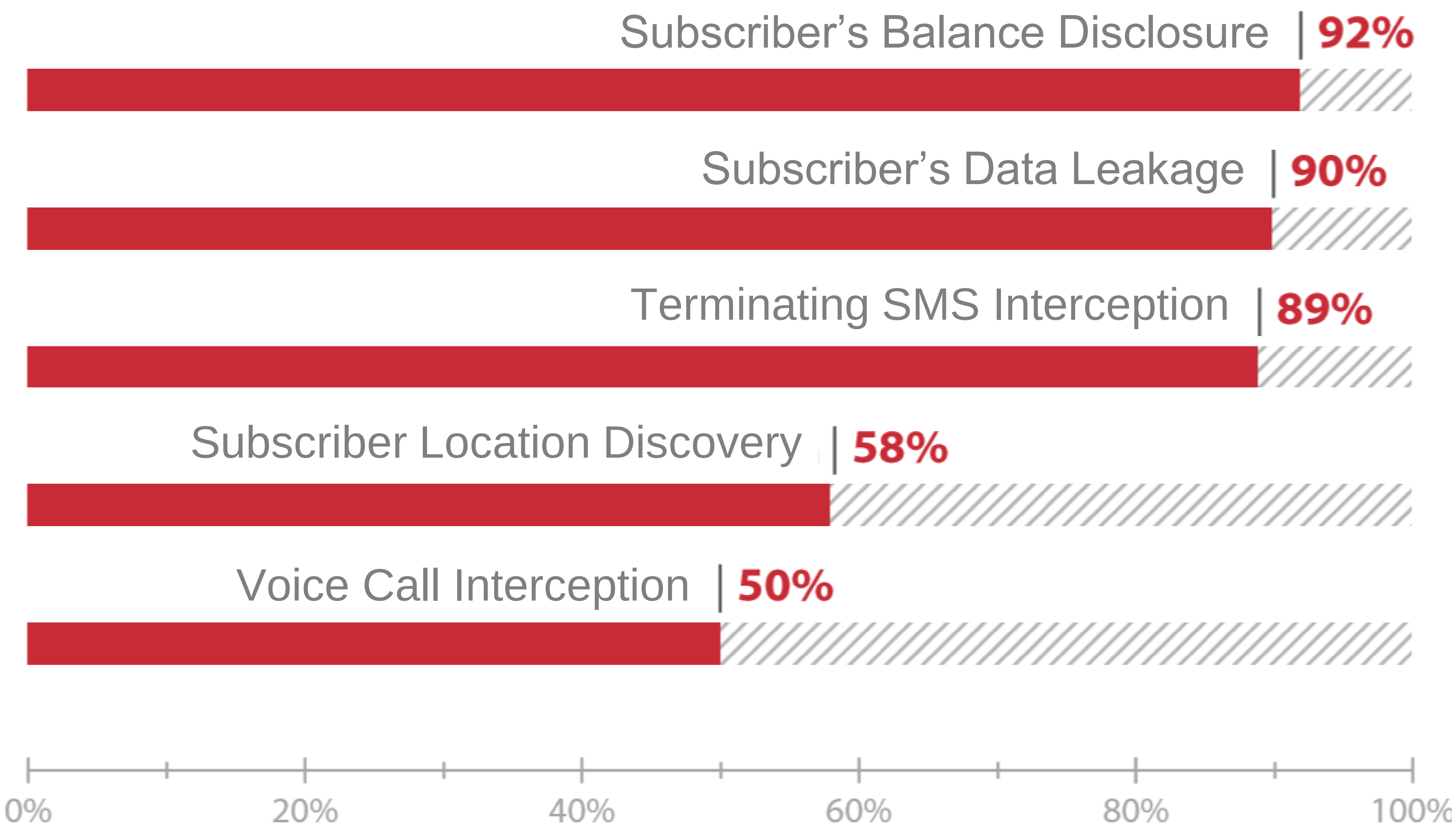
POSITIVE TECHNOLOGIES



Percentage of vulnerable networks

Incidents statistics. Data leakage

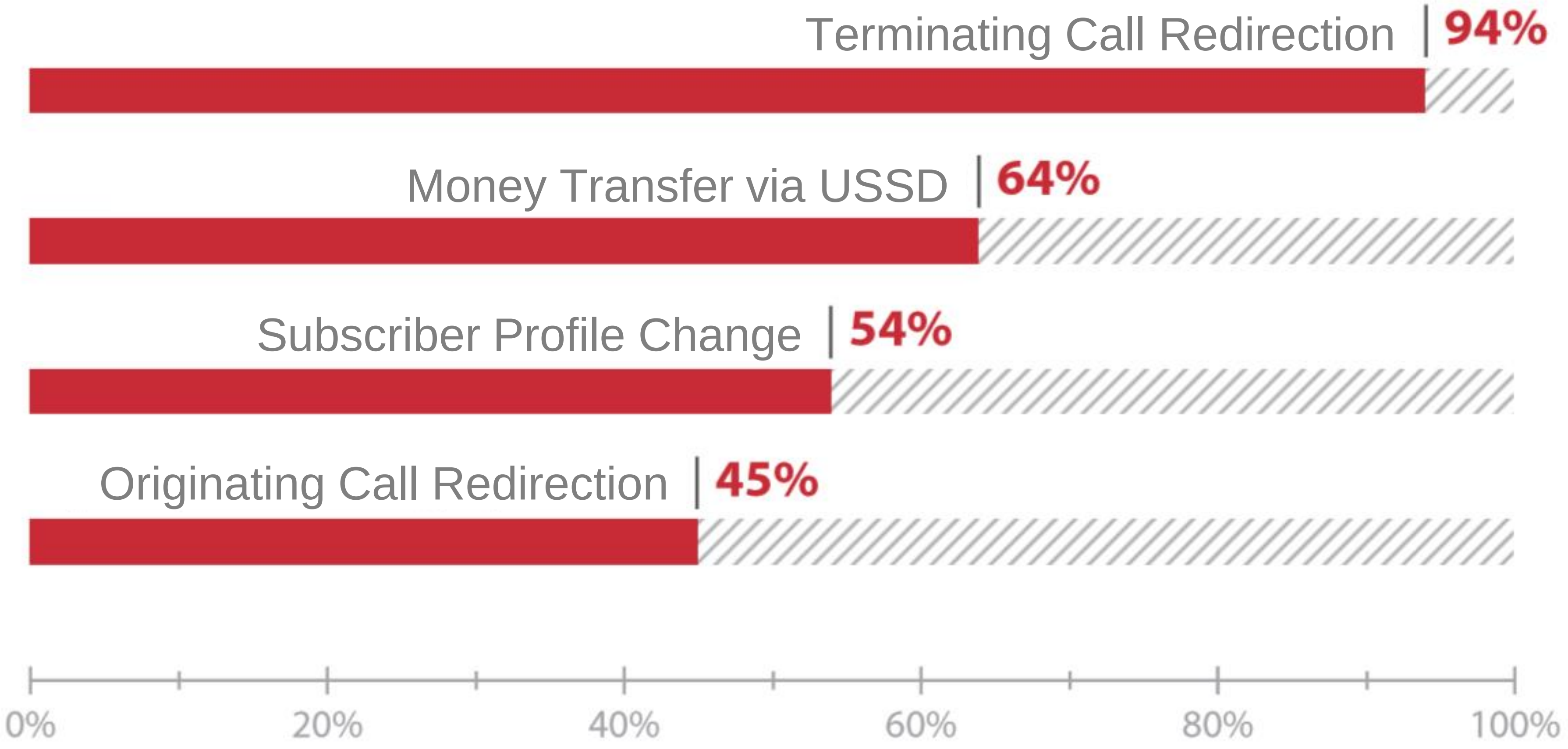
POSITIVE TECHNOLOGIES



Percentage of vulnerable networks

Incidents statistics. Fraud

POSITIVE TECHNOLOGIES



Percentage of vulnerable networks

Incident victims

- Mobile operator subscribers
- Mobile operator
- Other Mobile operators and their subscribers
- Third parties (often Banks and Their clients)

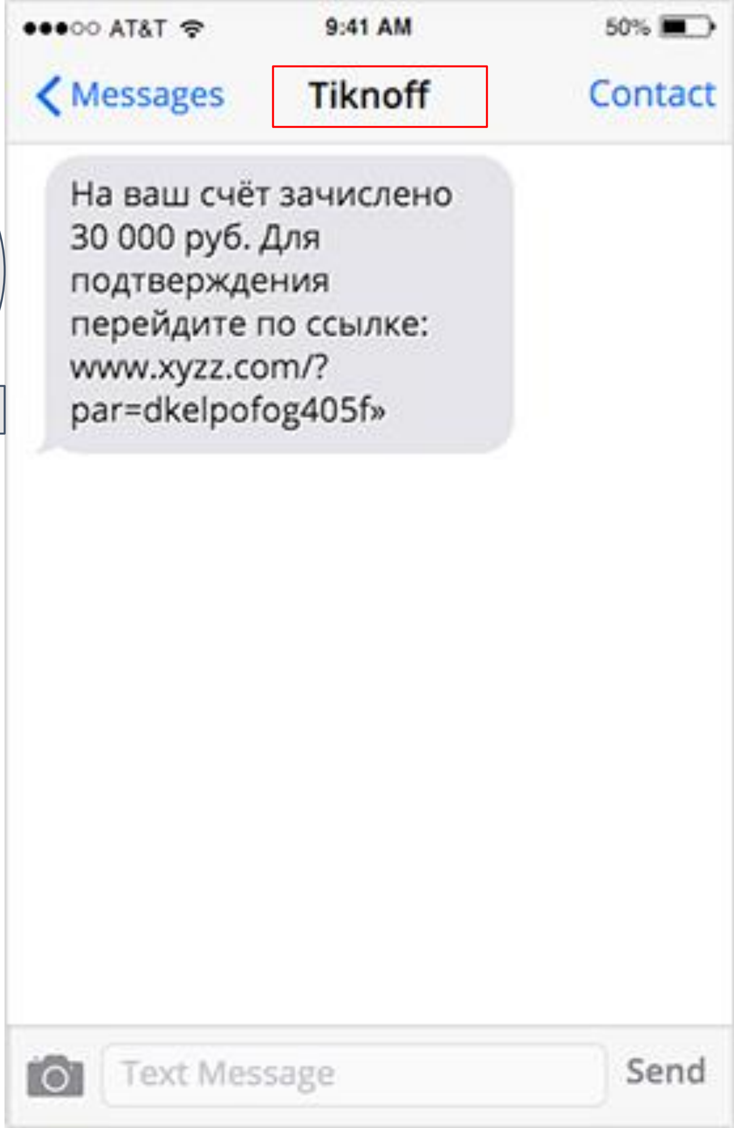
Prerequisites of attacks

- Internal intruder or Staff initiated attacks
- Level0 (almost) Kiddies - attacks that not require deep technical knowledge
  - SMS fraud as preliminary stage of malware based attacks
  - Fraud with social engineering (direct target is victim)
  - Proxified fraud with social engineering
- Level1(Locally initiated) - attacks that require technical knowledge about Radio Access Network protocols
  - IMSI Catcher
  - Bluetooth
  - Calls and SMS from the subscriber located nearby
- **Level2 (Global impact) - attacks that require technical knowledge about telco infrastructure and protocols**

Lightweight scenarios (Level0)

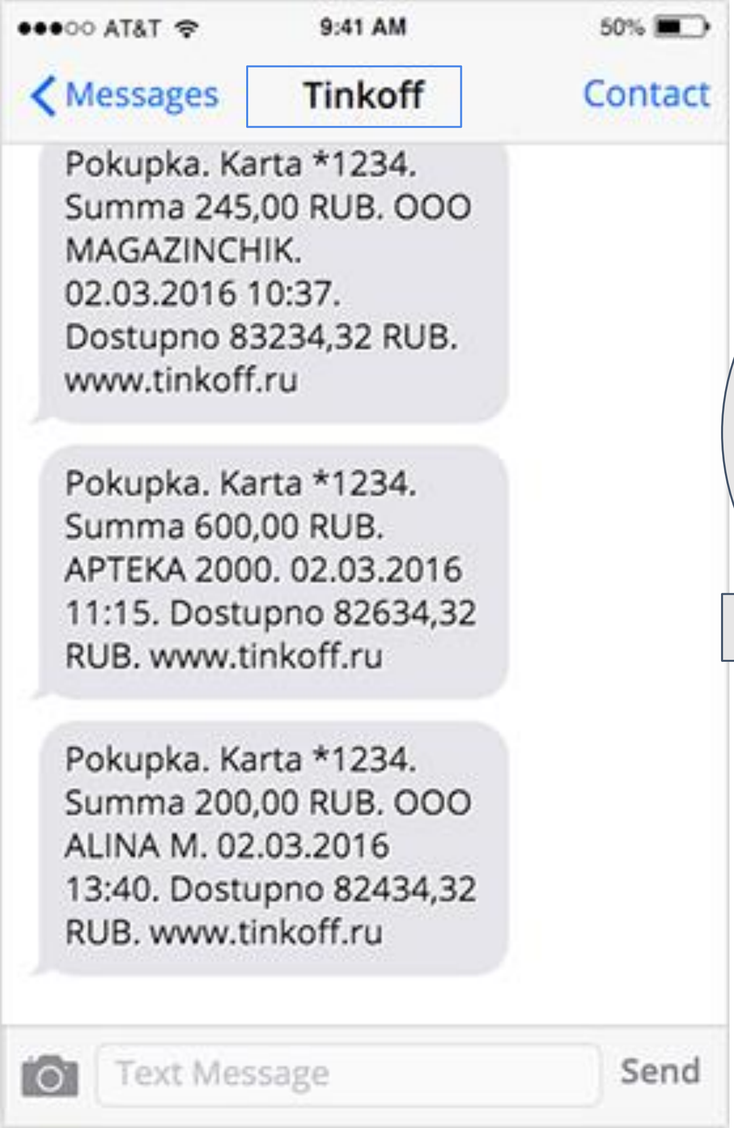
Kiddies fraud examples Typosquatting works well even here

You received 30000 RUB, please follow the link for confirmation



На ваш счёт зачислено 30 000 руб. Для подтверждения перейдите по ссылке: www.xyzz.com/?par=dkelpofog405f»

Not legit



Pokupka. Karta *1234. Summa 245,00 RUB. OOO MAGAZINCHIK. 02.03.2016 10:37. Dostupno 83234,32 RUB. www.tinkoff.ru

Pokupka. Karta *1234. Summa 600,00 RUB. APTEKA 2000. 02.03.2016 11:15. Dostupno 82634,32 RUB. www.tinkoff.ru

Pokupka. Karta *1234. Summa 200,00 RUB. OOO ALINA M. 02.03.2016 13:40. Dostupno 82434,32 RUB. www.tinkoff.ru

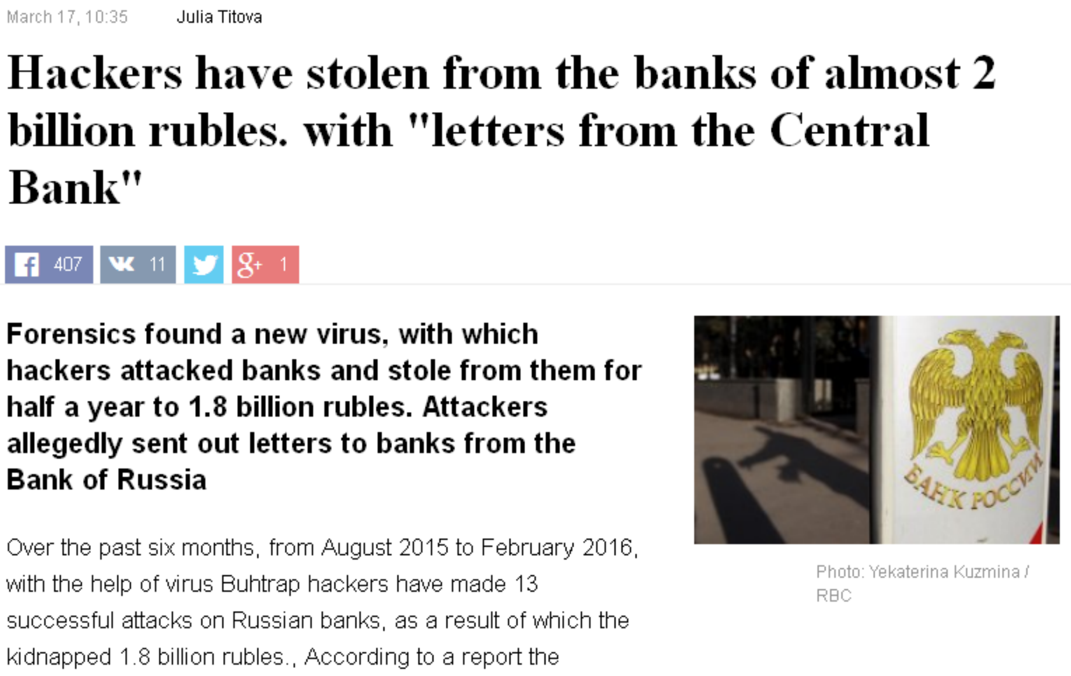
Legit

Purchase. Card *1234. Ammount 600 RUB. Drugstore 2000… Available balance 82634.32 RUB

http://journal.tinkoff.ru/declined/

Central bank not only in emails...

Mature player and kiddies used the same brand name



March 17, 10:35 Julia Titova

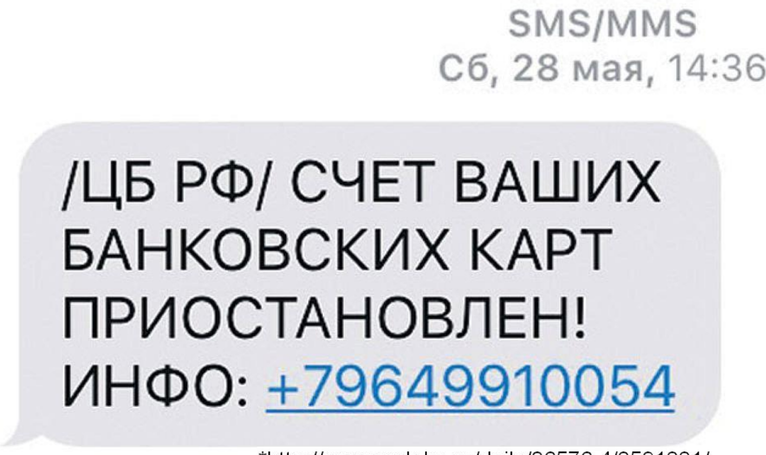
Hackers have stolen from the banks of almost 2 billion rubles. with "letters from the Central Bank"

Forensics found a new virus, with which hackers attacked banks and stole from them for half a year to 1.8 billion rubles. Attackers allegedly sent out letters to banks from the Bank of Russia

Over the past six months, from August 2015 to February 2016, with the help of virus Buhtrap hackers have made 13 successful attacks on Russian banks, as a result of which the kidnapped 1.8 billion rubles., According to a report the

Photo: Yekaterina Kuzmina / RBC

http://www.rbc.ru/finances/17/03/2016/56e97c089a794797e5b8e6b3



SMS/MMS
Сб, 28 мая, 14:36

/ЦБ РФ/ СЧЕТ ВАШИХ БАНКОВСКИХ КАРТ ПРИОСТАНОВЛЕН! ИНФО: +79649910054

*http://www.msk.kp.ru/daily/26576.4/3591331/

/Cental Bank of Russian Federation/ Your banking cards accounts was suspended!
Info: +79649910054

Social engineering telco staff

POSITIVE TECHNOLOGIES

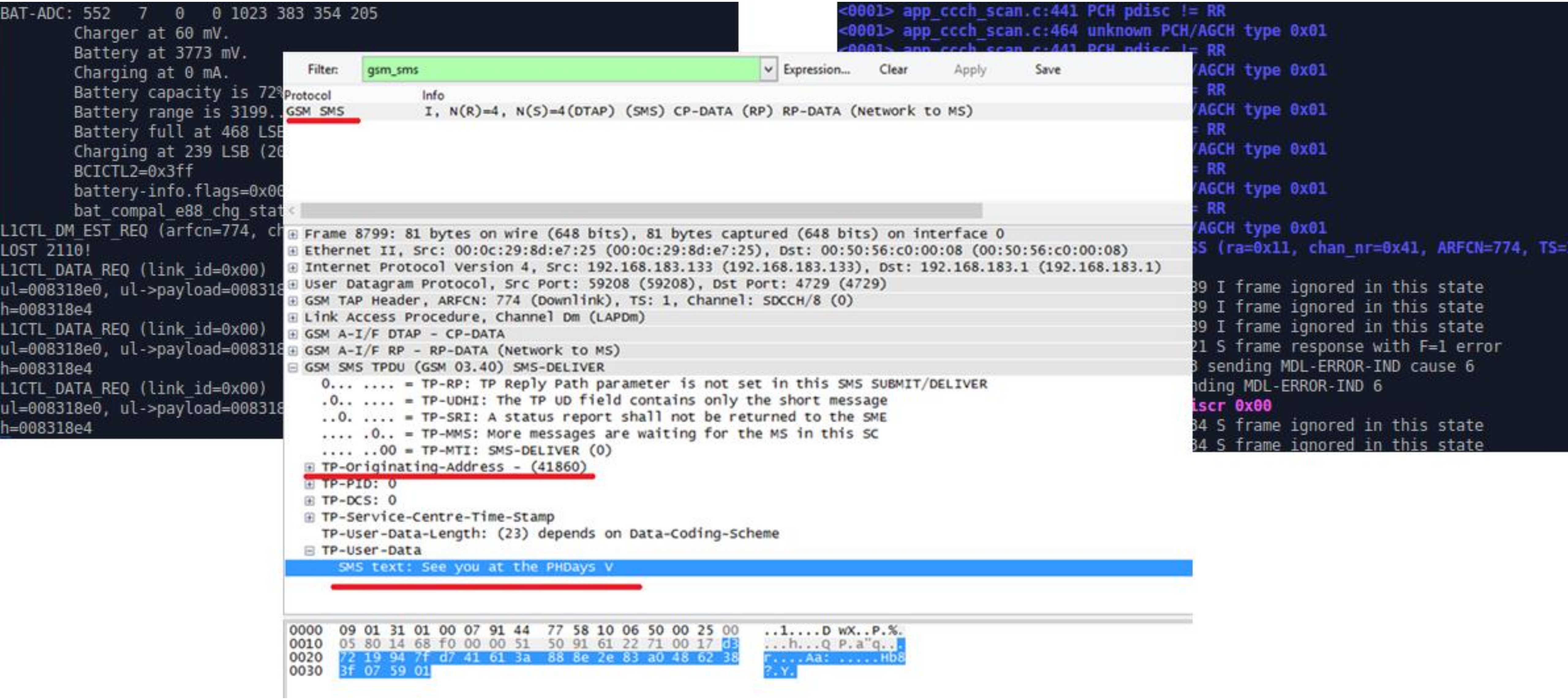
- Temporary redirect calls and SMS to another number
- Own victim email, social networks accounts, messengers and in some cases Money (Banking OTP TBD)
- Fast WIN

MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.
REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?

Cases (Level1)

SMS interception

POSITIVE TECHNOLOGIES



```
BAT-ADC: 552   7   0   0 1023 383 354 205
        Charger at 60 mV.
        Battery at 3773 mV.
        Charging at 0 mA.
        Battery capacity is 72%
        Battery range is 3199.
        Battery full at 468 LSB
        Charging at 239 LSB (20
        BCICTL2=0x3ff
        battery-info.flags=0x00
        bat_compal_e88_chg_stat
L1CTL_DM_EST_REQ (arfcn=774, ch
LOST 2110!
L1CTL_DATA_REQ (link_id=0x00)
ul=008318e0, ul->payload=008318
h=008318e4
L1CTL_DATA_REQ (link_id=0x00)
ul=008318e0, ul->payload=008318
h=008318e4
L1CTL_DATA_REQ (link_id=0x00)
ul=008318e0, ul->payload=008318
h=008318e4
```

```
<0001> app_ccch_scan.c:441 PCH pdisc != RR
<0001> app_ccch_scan.c:464 unknown PCH/AGCH type 0x01
<0001> app_ccch_scan.c:441 PCH pdisc != RR
/AGCH type 0x01
= RR
/AGCH type 0x01
= RR
/AGCH type 0x01
= RR
/AGCH type 0x01
= RR
/AGCH type 0x01
SS (ra=0x11, chan_nr=0x41, ARFCN=774, TS=

39 I frame ignored in this state
39 I frame ignored in this state
39 I frame ignored in this state
21 S frame response with F=1 error
3 sending MDL-ERROR-IND cause 6
nding MDL-ERROR-IND 6
iscr 0x00
34 S frame ignored in this state
34 S frame ignored in this state
```

Filter: gsm_sms

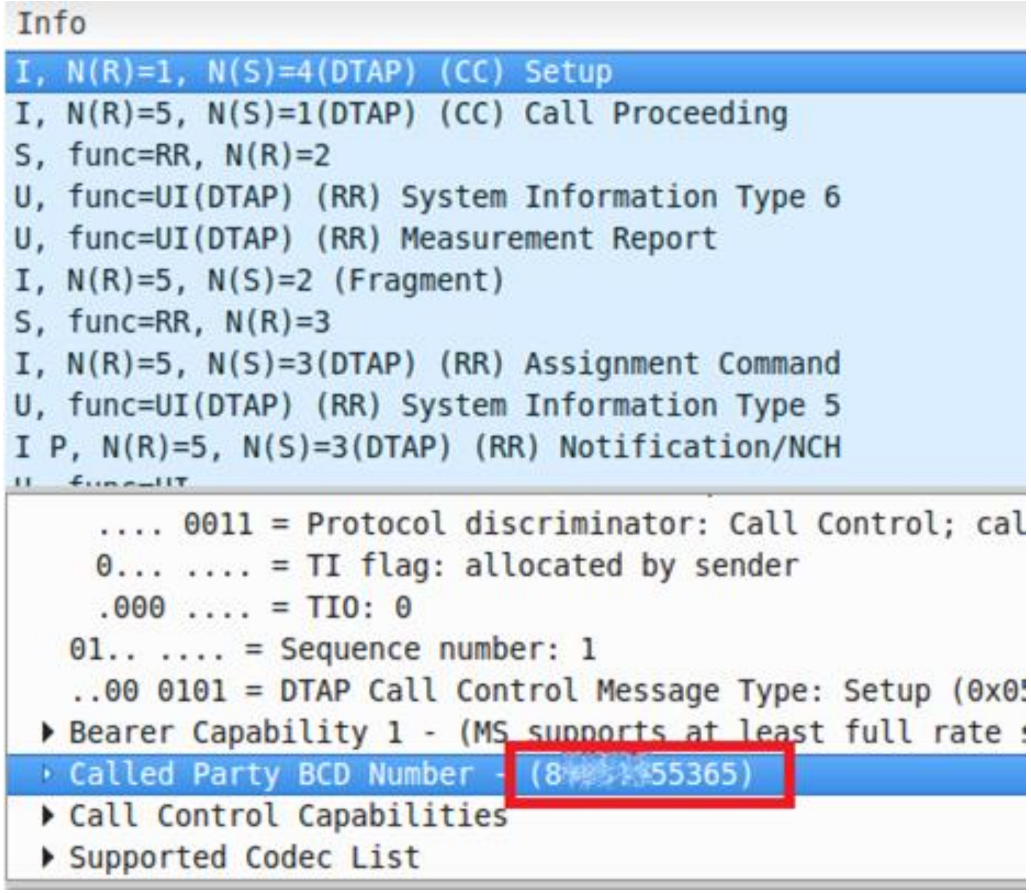
Protocol	Info
GSM SMS	I, N(R)=4, N(S)=4(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)

```
⊞ Frame 8799: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
⊞ Ethernet II, Src: 00:0c:29:8d:e7:25 (00:0c:29:8d:e7:25), Dst: 00:50:56:c0:00:08 (00:50:56:c0:00:08)
⊞ Internet Protocol Version 4, Src: 192.168.183.133 (192.168.183.133), Dst: 192.168.183.1 (192.168.183.1)
⊞ User Datagram Protocol, Src Port: 59208 (59208), Dst Port: 4729 (4729)
⊞ GSM TAP Header, ARFCN: 774 (Downlink), TS: 1, Channel: SDCCH/8 (0)
⊞ Link Access Procedure, Channel Dm (LAPDm)
⊞ GSM A-I/F DTAP - CP-DATA
⊞ GSM A-I/F RP - RP-DATA (Network to MS)
⊟ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..0. .... = TP-SRI: A status report shall not be returned to the SME
    .... .0.. = TP-MMS: More messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ⊞ TP-Originating-Address - (41860)
  ⊞ TP-PID: 0
  ⊞ TP-DCS: 0
  ⊞ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (23) depends on Data-Coding-Scheme
  ⊟ TP-User-Data
      SMS text: See you at the PHDays V

0000  09 01 31 01 00 07 91 44  77 58 10 06 50 00 25 00   ..1....D wX..P.%.
0010  05 80 14 68 f0 00 00 51  50 91 61 22 71 00 17 d3   ...h...Q P.a"q...
0020  72 19 94 7f d7 41 61 3a  88 8e 2e 83 a0 48 62 38   r....Aa: .....Hb8
0030  3f 07 59 01                                        ?.Y.
```

Voice call interception

POSITIVE TECHNOLOGIES

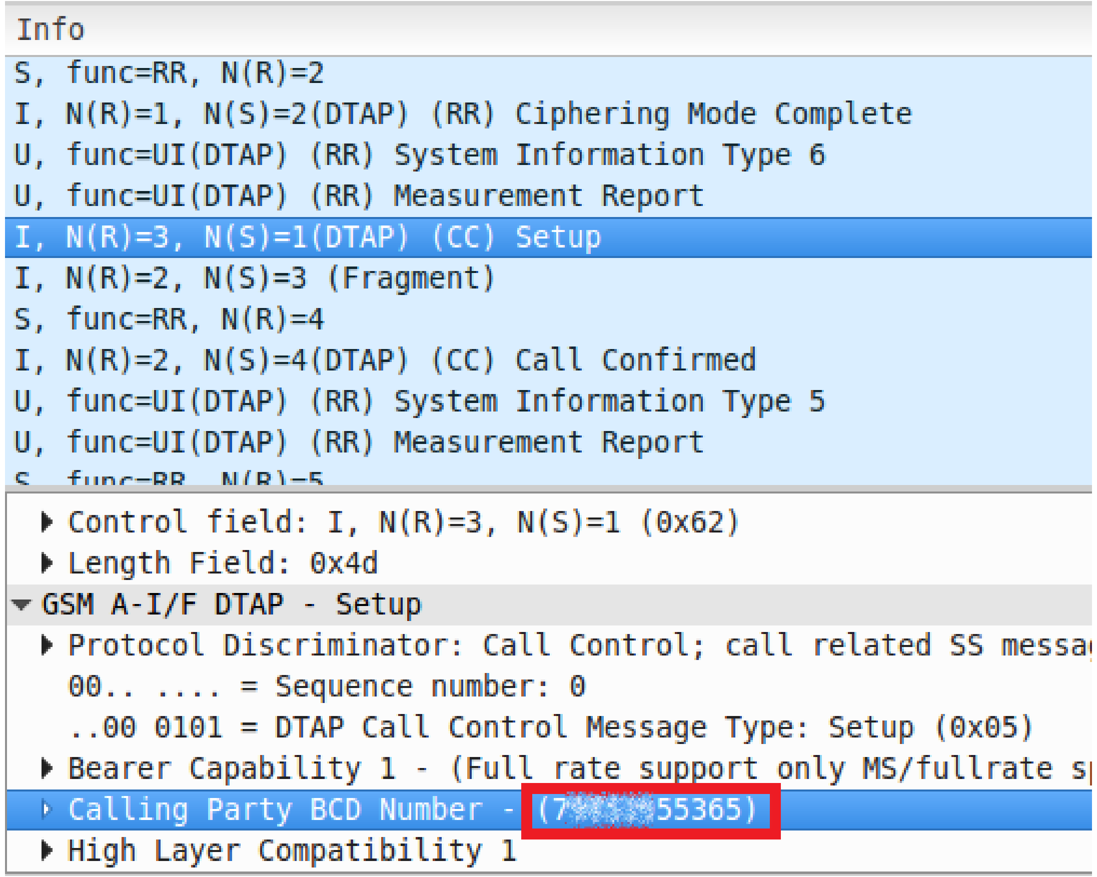
- Originating call



```
Info
I, N(R)=1, N(S)=4(DTAP) (CC) Setup
I, N(R)=5, N(S)=1(DTAP) (CC) Call Proceeding
S, func=RR, N(R)=2
U, func=UI(DTAP) (RR) System Information Type 6
U, func=UI(DTAP) (RR) Measurement Report
I, N(R)=5, N(S)=2 (Fragment)
S, func=RR, N(R)=3
I, N(R)=5, N(S)=3(DTAP) (RR) Assignment Command
U, func=UI(DTAP) (RR) System Information Type 5
I P, N(R)=5, N(S)=3(DTAP) (RR) Notification/NCH
U, func=UI
```

```
    .... 0011 = Protocol discriminator: Call Control; cal
    0... .... = TI flag: allocated by sender
    .000 .... = TIO: 0
  01.. .... = Sequence number: 1
  ..00 0101 = DTAP Call Control Message Type: Setup (0x0
▸ Bearer Capability 1 - (MS supports at least full rate s
▸ Called Party BCD Number - (8[redacted]55365)
▸ Call Control Capabilities
▸ Supported Codec List
```

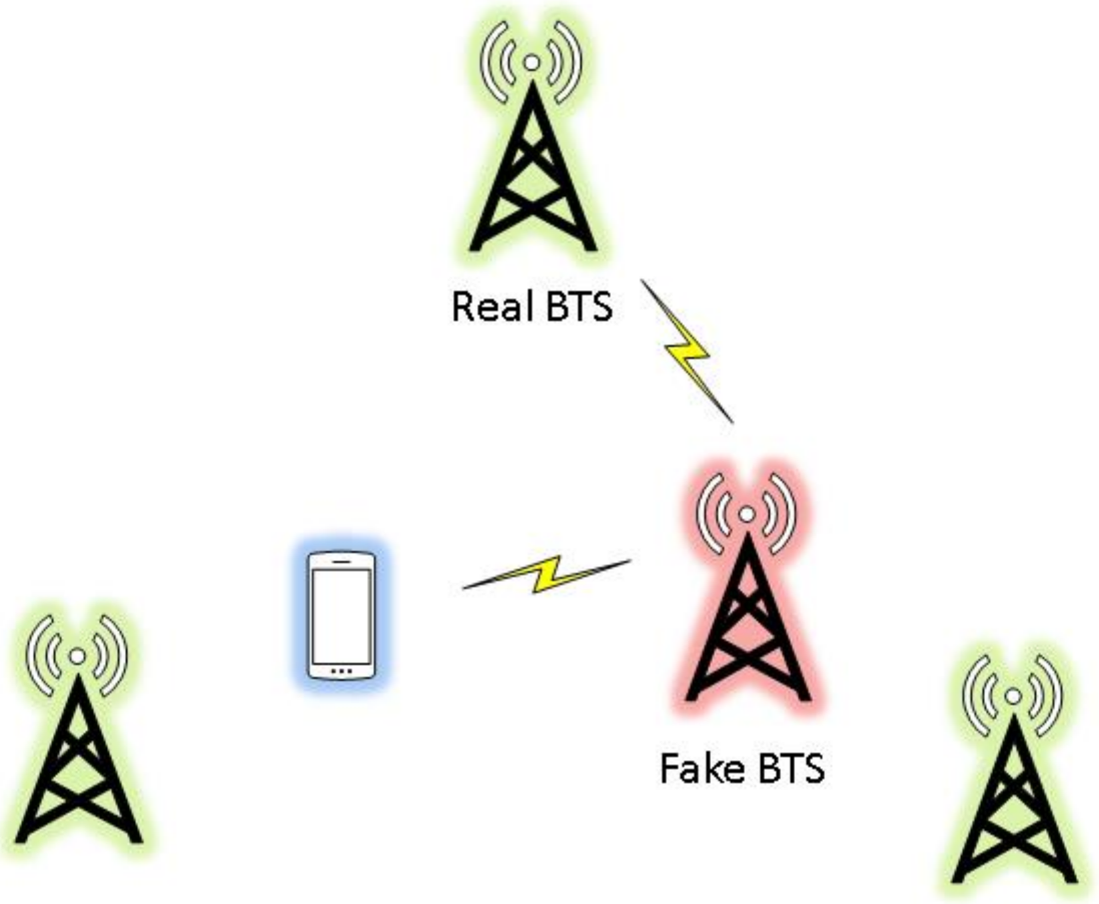
- Terminating call



```
Info
S, func=RR, N(R)=2
I, N(R)=1, N(S)=2(DTAP) (RR) Ciphering Mode Complete
U, func=UI(DTAP) (RR) System Information Type 6
U, func=UI(DTAP) (RR) Measurement Report
I, N(R)=3, N(S)=1(DTAP) (CC) Setup
I, N(R)=2, N(S)=3 (Fragment)
S, func=RR, N(R)=4
I, N(R)=2, N(S)=4(DTAP) (CC) Call Confirmed
U, func=UI(DTAP) (RR) System Information Type 5
U, func=UI(DTAP) (RR) Measurement Report
S, func=RR, N(R)=5
```

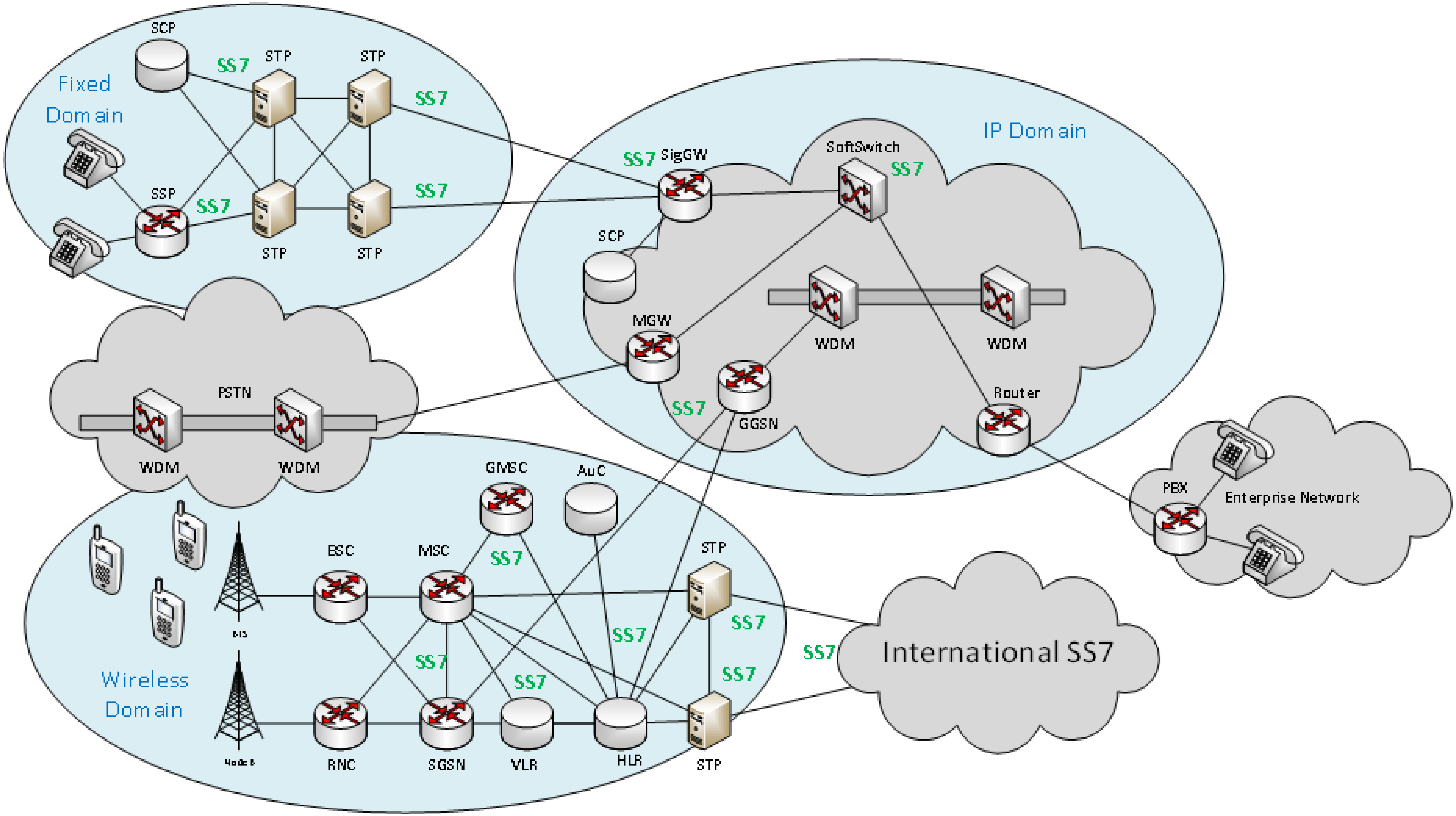
```
 ▸ Control field: I, N(R)=3, N(S)=1 (0x62)
 ▸ Length Field: 0x4d
▾ GSM A-I/F DTAP - Setup
 ▸ Protocol Discriminator: Call Control; call related SS messa
   00.. .... = Sequence number: 0
   ..00 0101 = DTAP Call Control Message Type: Setup (0x05)
 ▸ Bearer Capability 1 - (Full rate support only MS/fullrate s
 ▸ Calling Party BCD Number - (7[redacted]55365)
 ▸ High Layer Compatibility 1
```

Voice call interception. MitM

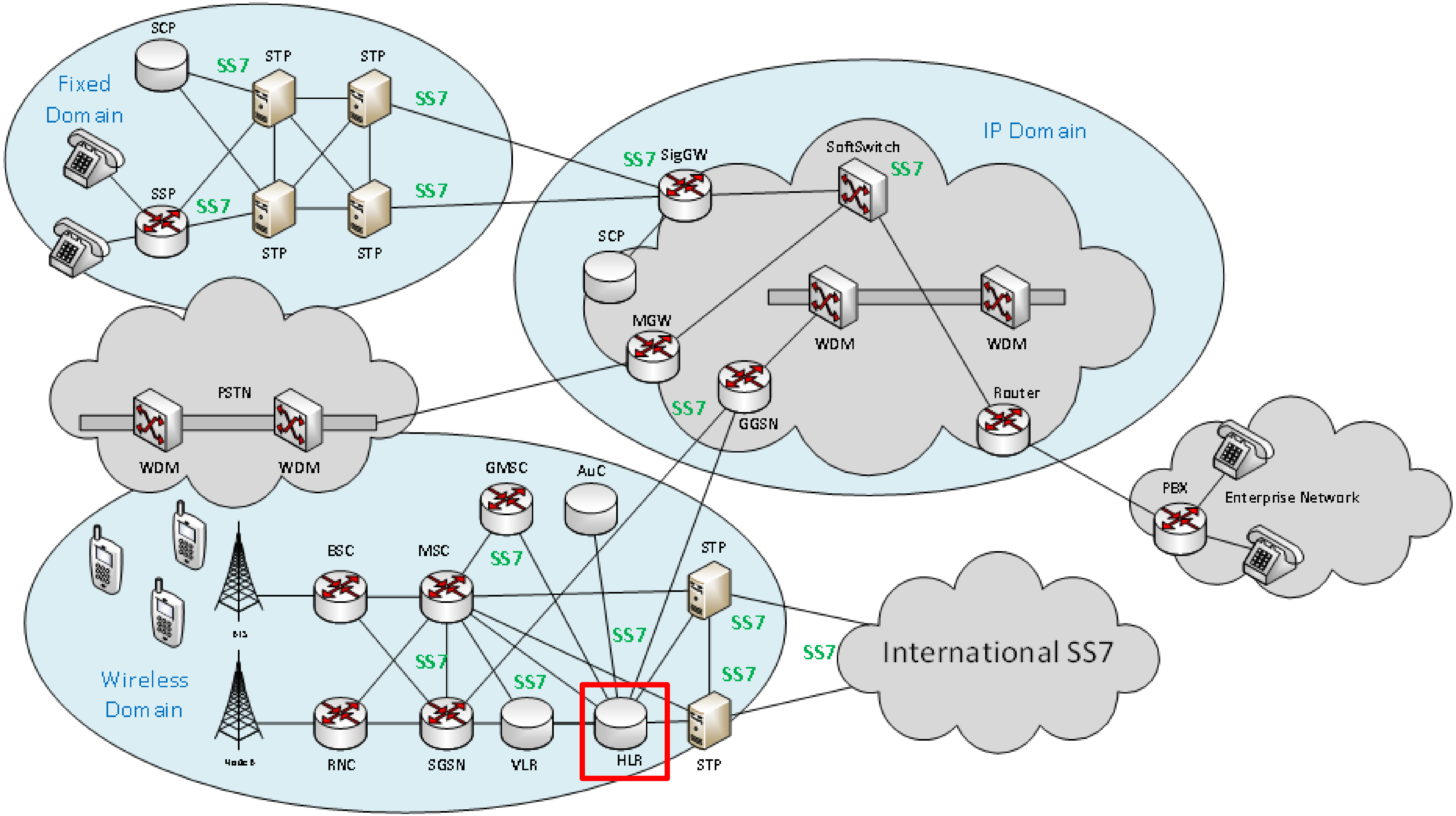


Level2 Cases (global impact)

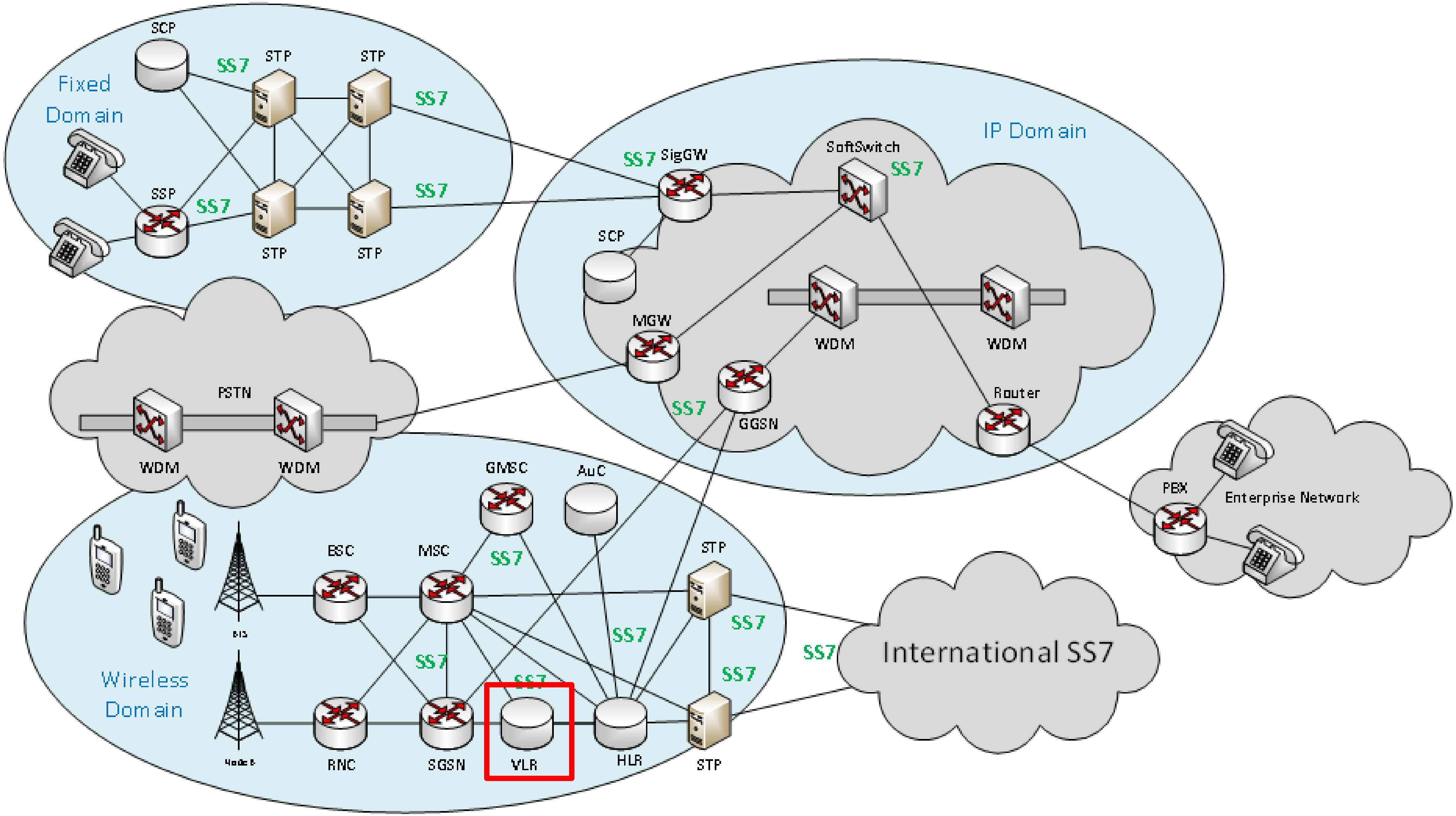
Telco infrastructure, technical view



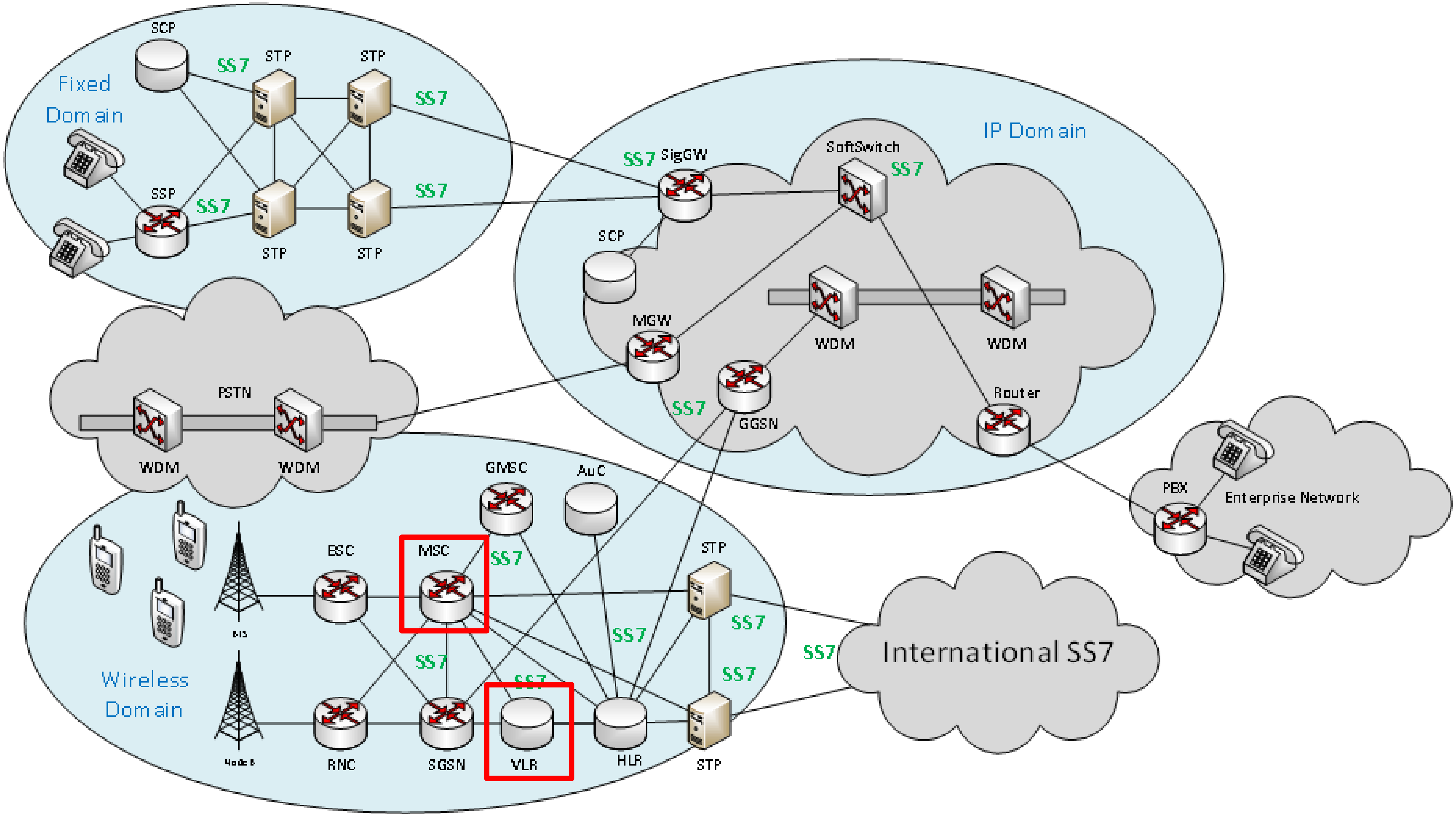
Telco infrastructure, technical view



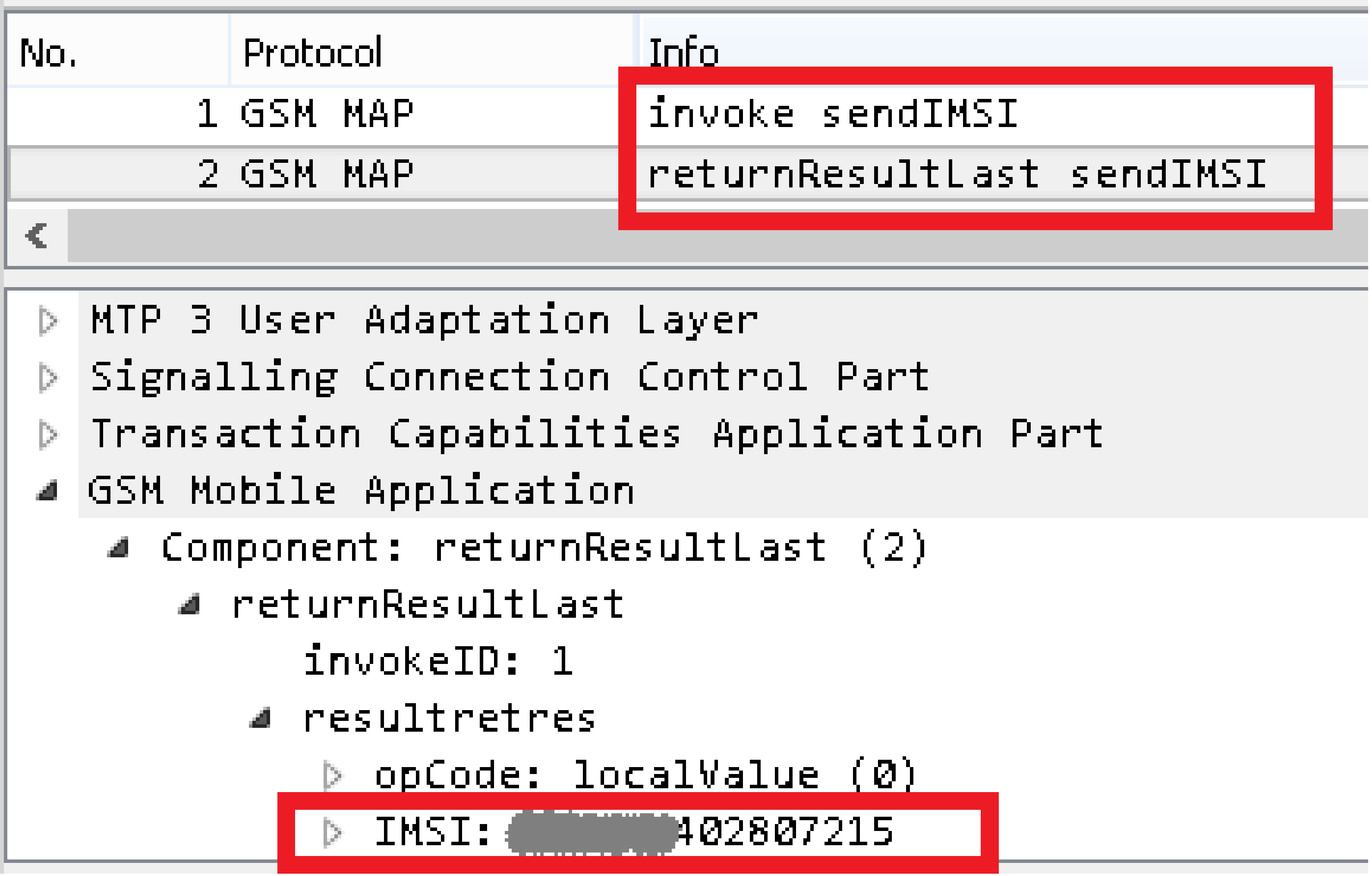
Telco infrastructure, technical view



Telco infrastructure, technical view



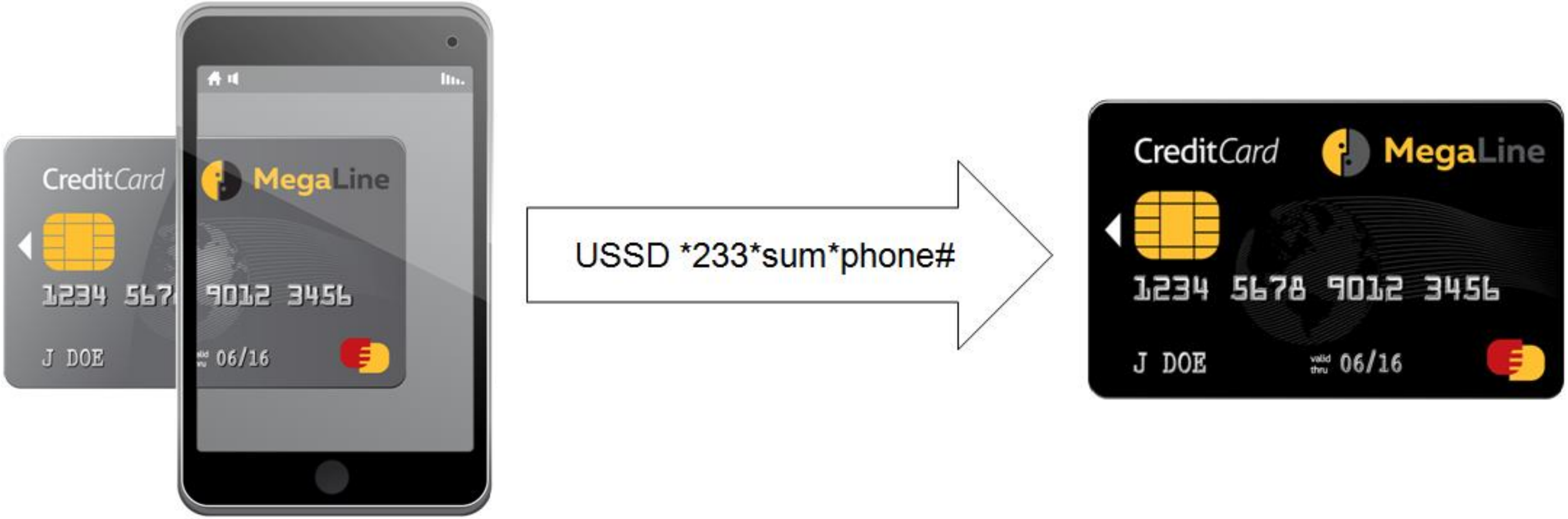
IMSI Disclosure



No.	Protocol	Info
1	GSM MAP	invoke sendIMSI
2	GSM MAP	returnResultLast sendIMSI

```
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
    ◢ Component: returnResultLast (2)
        ◢ returnResultLast
              invokeID: 1
            ◢ resultretres
                ▷ opCode: localValue (0)
                ▷ IMSI: [redacted]402807215
```

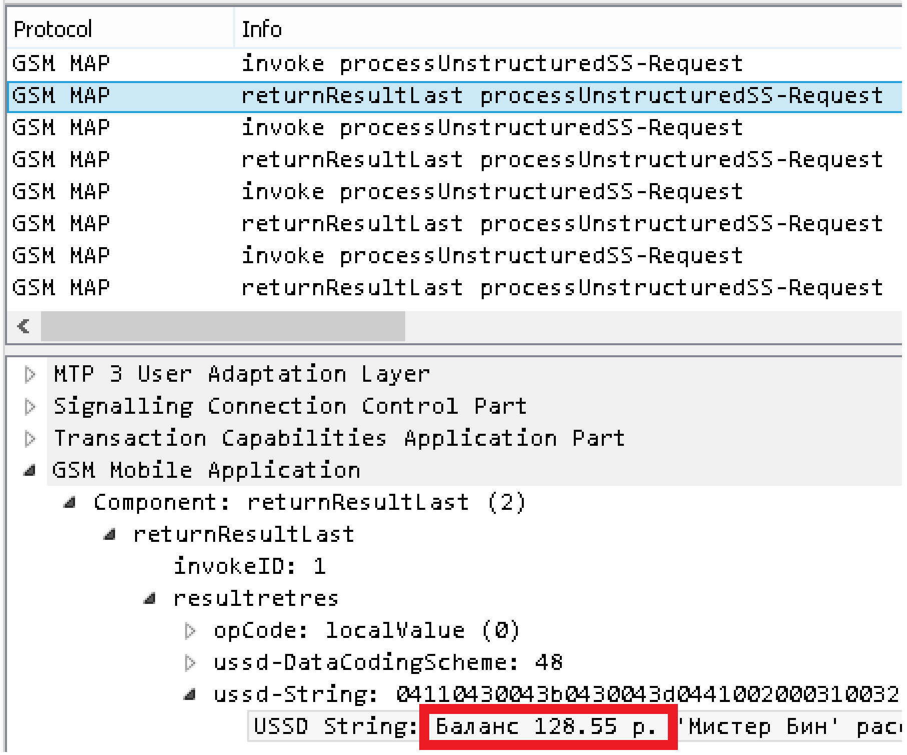
Money fraud cases



- Infect smartphone with malware.
- Use fake base station (IMSI catcher) and to make software clone of SIM card.
- Conduct an attack via SS7 network forging USSD request.

USSD manipulation

Request the balance *100#. Balance is 128.55 Roubles



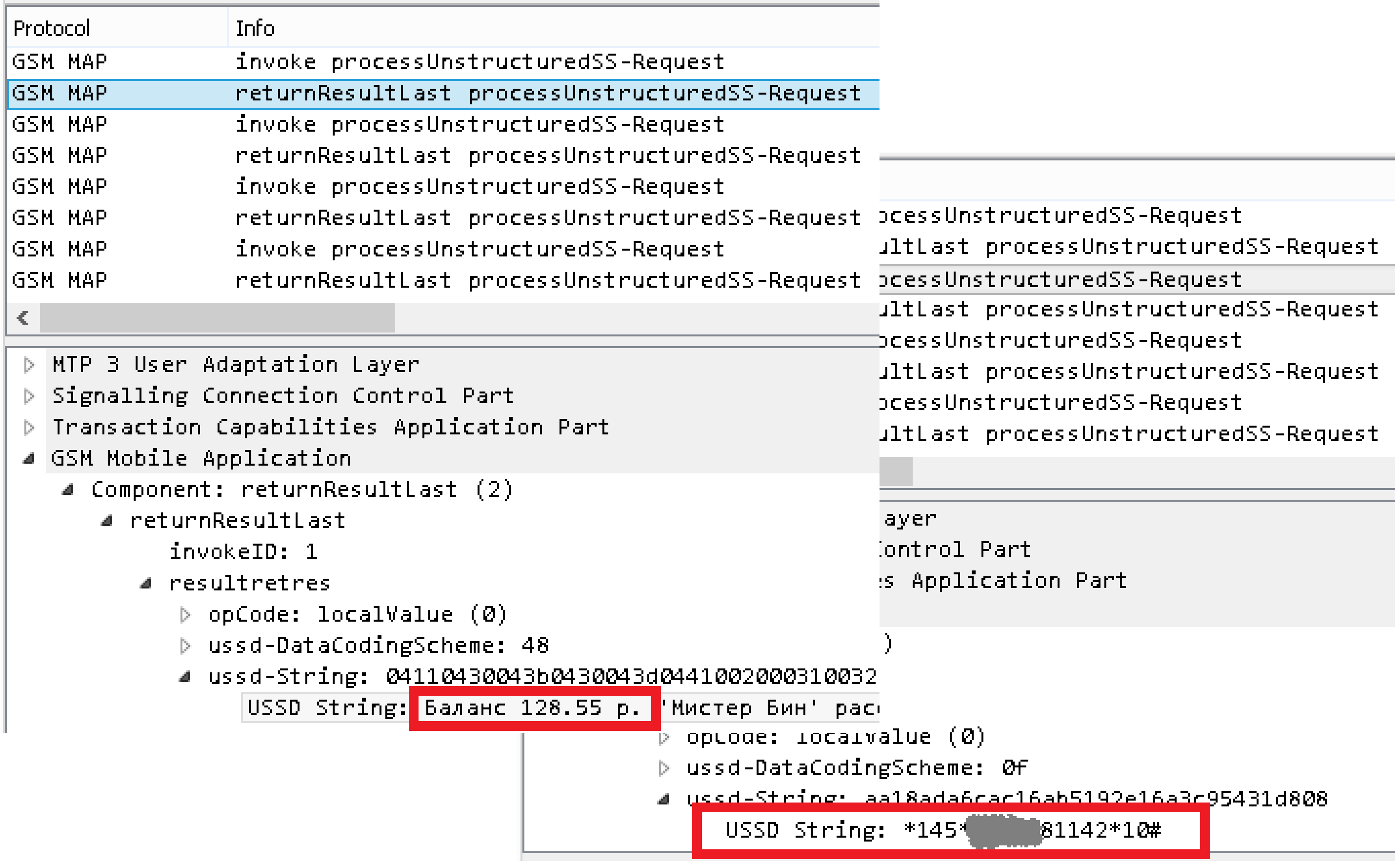
```
Protocol     Info
GSM MAP      invoke processUnstructuredSS-Request
GSM MAP      returnResultLast processUnstructuredSS-Request
GSM MAP      invoke processUnstructuredSS-Request
GSM MAP      returnResultLast processUnstructuredSS-Request
GSM MAP      invoke processUnstructuredSS-Request
GSM MAP      returnResultLast processUnstructuredSS-Request
GSM MAP      invoke processUnstructuredSS-Request
GSM MAP      returnResultLast processUnstructuredSS-Request
```

```
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
   ◢ Component: returnResultLast (2)
      ◢ returnResultLast
           invokeID: 1
         ◢ resultretres
            ▷ opCode: localValue (0)
            ▷ ussd-DataCodingScheme: 48
            ◢ ussd-String: 04110430043b0430043d0441002000310032
                 USSD String: Баланс 128.55 р. 'Мистер Бин' рас
```

USSD manipulation

POSITIVE TECHNOLOGIES

*145*xxxxxx81142*10# - Transfer 10 Roubles to the number xxxxxx81142



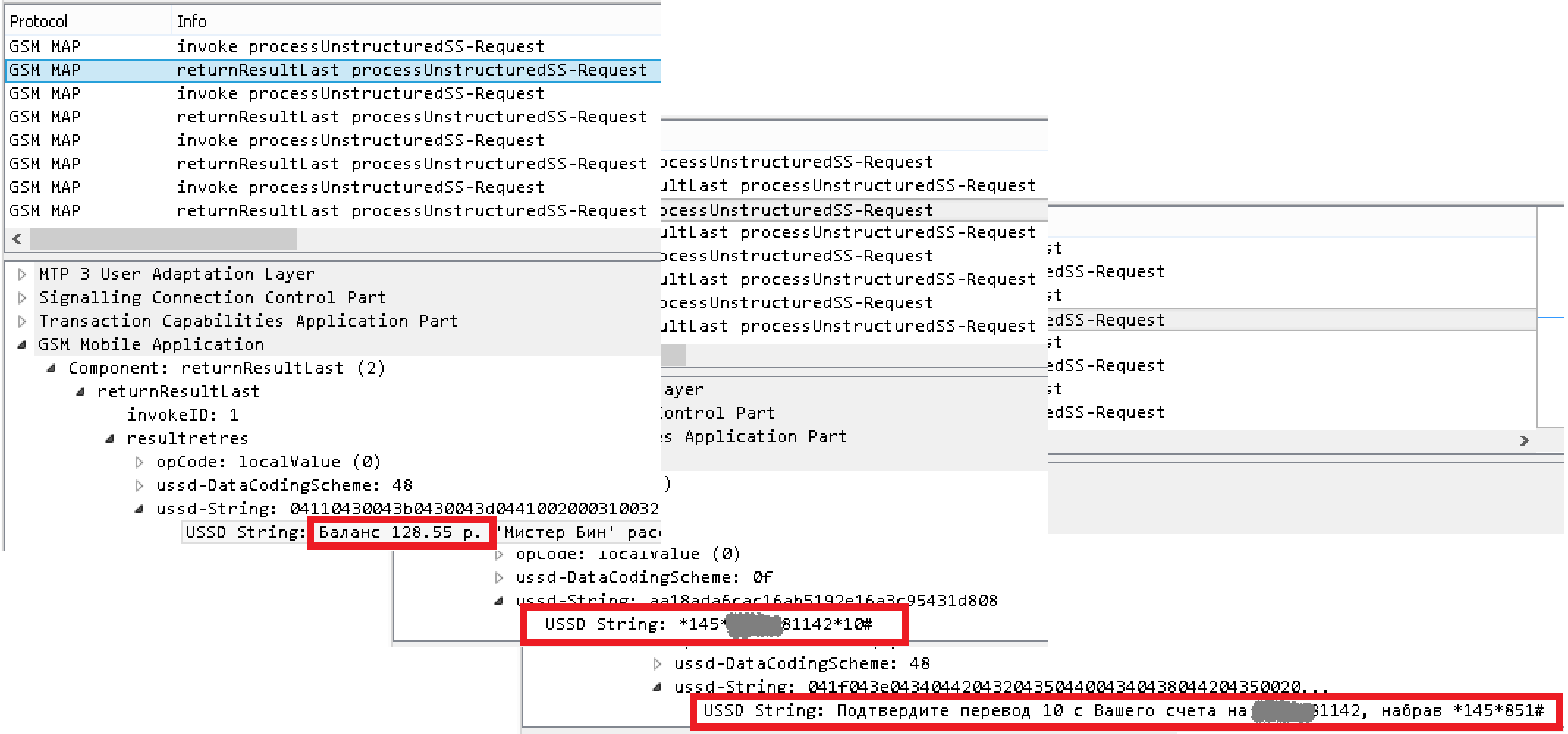
```
Protocol          Info
GSM MAP           invoke processUnstructuredSS-Request
GSM MAP           returnResultLast processUnstructuredSS-Request
GSM MAP           invoke processUnstructuredSS-Request
GSM MAP           returnResultLast processUnstructuredSS-Request
GSM MAP           invoke processUnstructuredSS-Request
GSM MAP           returnResultLast processUnstructuredSS-Request
GSM MAP           invoke processUnstructuredSS-Request
GSM MAP           returnResultLast processUnstructuredSS-Request

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
   ◢ Component: returnResultLast (2)
      ◢ returnResultLast
           invokeID: 1
         ◢ resultretres
            ▷ opCode: localValue (0)
            ▷ ussd-DataCodingScheme: 48
            ◢ ussd-String: 04110430043b0430043d0441002000310032
                 USSD String: Баланс 128.55 р. 'Мистер Бин' рас
```

```
ocessUnstructuredSS-Request
ultLast processUnstructuredSS-Request
ocessUnstructuredSS-Request
ultLast processUnstructuredSS-Request
ocessUnstructuredSS-Request
ultLast processUnstructuredSS-Request
ocessUnstructuredSS-Request
ultLast processUnstructuredSS-Request

ayer
Control Part
s Application Part

)
            ▷ opCode: localValue (0)
            ▷ ussd-DataCodingScheme: 0f
            ◢ ussd-String: aa18ada6cac16ab5192e16a3c95431d808
                 USSD String: *145*[redacted]81142*10#
```

USSD manipulation

POSITIVE TECHNOLOGIES

Cool security mechanism. Just send *145*851# to confirm the transaction



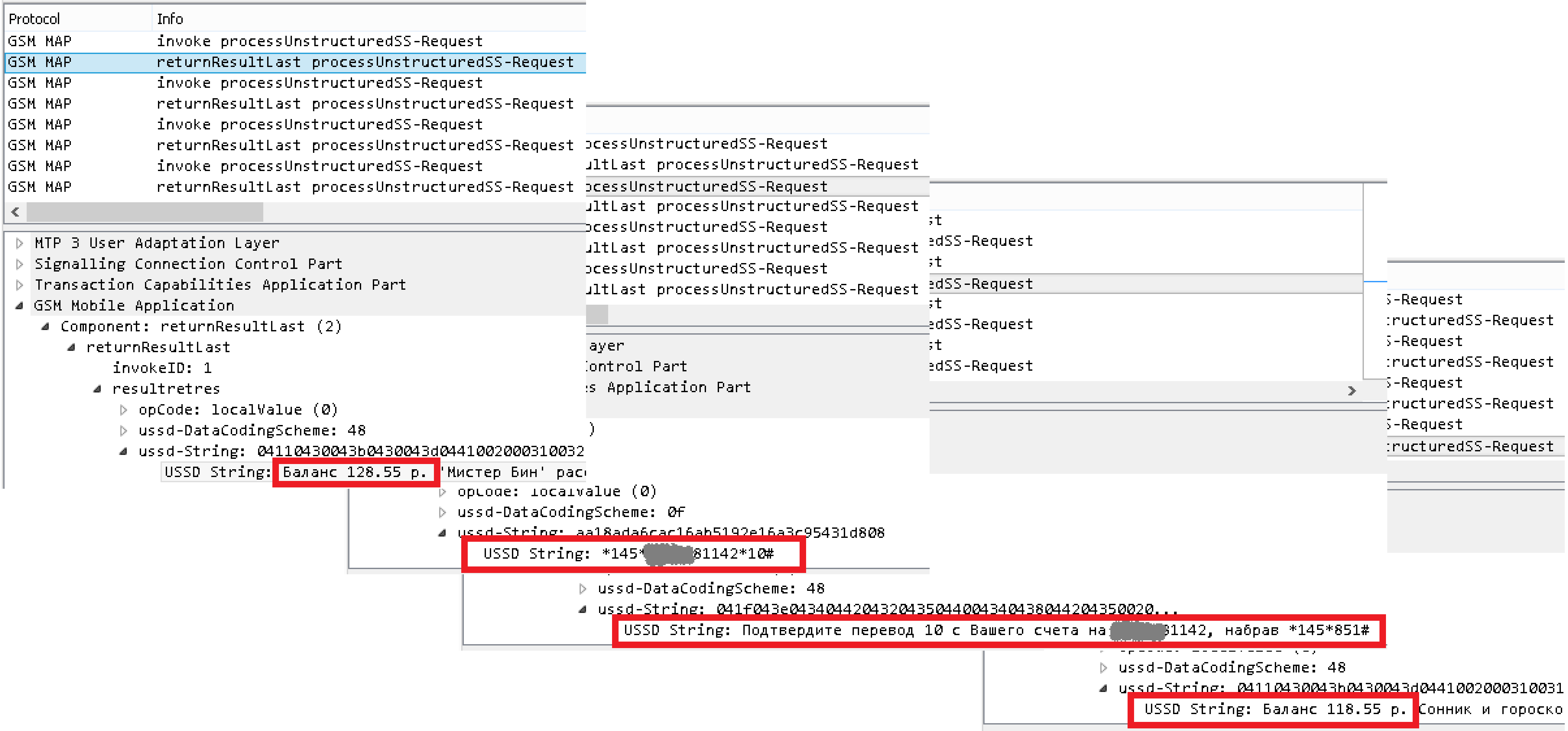
```
Protocol    Info
GSM MAP     invoke processUnstructuredSS-Request
GSM MAP     returnResultLast processUnstructuredSS-Request
GSM MAP     invoke processUnstructuredSS-Request
GSM MAP     returnResultLast processUnstructuredSS-Request
GSM MAP     invoke processUnstructuredSS-Request
GSM MAP     returnResultLast processUnstructuredSS-Request
GSM MAP     invoke processUnstructuredSS-Request
GSM MAP     returnResultLast processUnstructuredSS-Request

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
   ◢ Component: returnResultLast (2)
      ◢ returnResultLast
           invokeID: 1
         ◢ resultretres
            ▷ opCode: localValue (0)
            ▷ ussd-DataCodingScheme: 48
            ◢ ussd-String: 04110430043b0430043d0441002000310032
                 USSD String: Баланс 128.55 р. 'Мистер Бин' рас
```

```
            ▷ opCode: localValue (0)
            ▷ ussd-DataCodingScheme: 0f
            ◢ ussd-String: aa18ada6cac16ab5192e16a3c95431d808
                 USSD String: *145*[redacted]81142*10#
```

```
            ▷ ussd-DataCodingScheme: 48
            ◢ ussd-String: 041f043e04340442043204350440043404380442043500 20...
                 USSD String: Подтвердите перевод 10 с Вашего счета на [redacted]1142, набрав *145*851#
```

USSD manipulation

New balance is 118.55 Roubles. (10 Roubles ~ 0.15 €)



```
Protocol     Info
GSM MAP      invoke processUnstructuredSS-Request
GSM MAP      returnResultLast processUnstructuredSS-Request
GSM MAP      invoke processUnstructuredSS-Request
GSM MAP      returnResultLast processUnstructuredSS-Request
GSM MAP      invoke processUnstructuredSS-Request
GSM MAP      returnResultLast processUnstructuredSS-Request
GSM MAP      invoke processUnstructuredSS-Request
GSM MAP      returnResultLast processUnstructuredSS-Request

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
   ◢ Component: returnResultLast (2)
      ◢ returnResultLast
           invokeID: 1
         ◢ resultretres
            ▷ opCode: localValue (0)
            ▷ ussd-DataCodingScheme: 48
            ◢ ussd-String: 04110430043b0430043d0441002000310032
                 USSD String: Баланс 128.55 р. 'Мистер Бин' рас
```

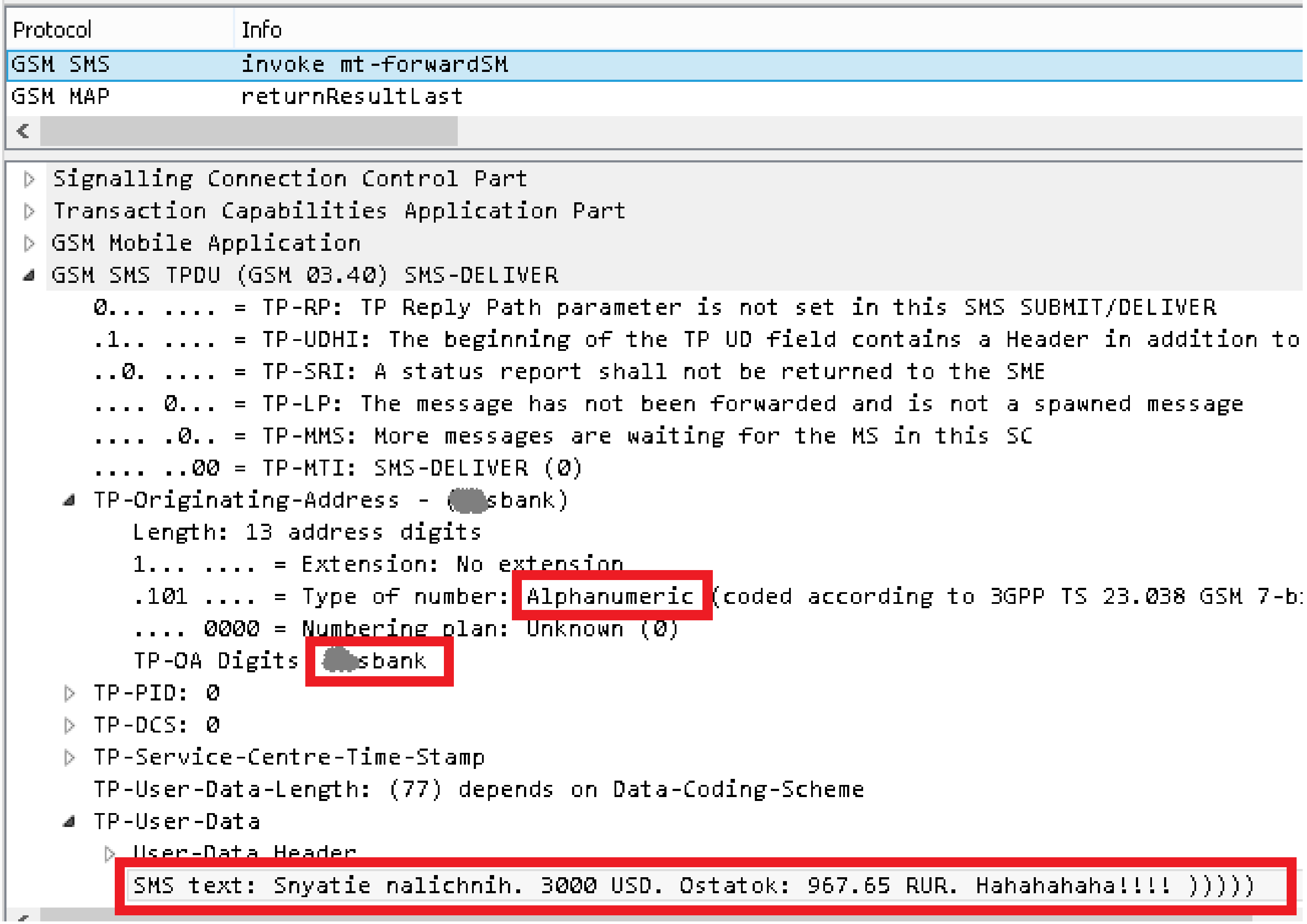
```
ocessUnstructuredSS-Request
ultLast processUnstructuredSS-Request
ocessUnstructuredSS-Request
ultLast processUnstructuredSS-Request
ocessUnstructuredSS-Request
ultLast processUnstructuredSS-Request
ocessUnstructuredSS-Request
ultLast processUnstructuredSS-Request

ayer
ontrol Part
s Application Part
)
            ▷ opCode: localValue (0)
            ▷ ussd-DataCodingScheme: 0f
            ◢ ussd-String: aa18ada6cac16ab5192e16a3c95431d808
                 USSD String: *145*[redacted]81142*10#
```

```
st
edSS-Request
st
edSS-Request
st
edSS-Request
st
edSS-Request

            ▷ ussd-DataCodingScheme: 48
            ◢ ussd-String: 041f043e043404420432043504400434043804420435002 0...
                 USSD String: Подтвердите перевод 10 с Вашего счета на [redacted]1142, набрав *145*851#
```

```
S-Request
ructuredSS-Request
S-Request
ructuredSS-Request
S-Request
ructuredSS-Request
S-Request
ructuredSS-Request

            ▷ ussd-DataCodingScheme: 48
            ◢ ussd-String: 04110430043b0430043d0441002000310031
                 USSD String: Баланс 118.55 р. Сонник и гороско
```

Calls or SMS on behalf particular person located anywhere

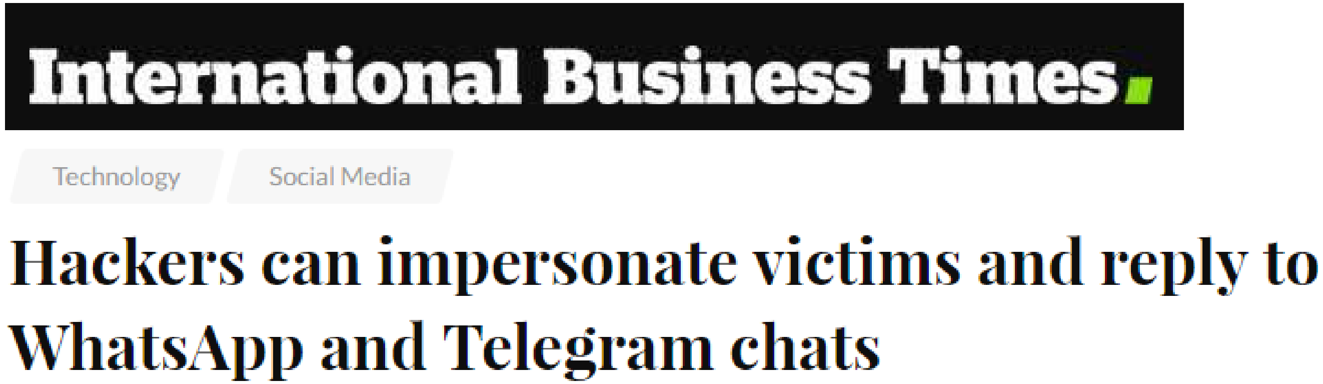
- SMS spoofing



Protocol	Info
GSM SMS	invoke mt-forwardSM
GSM MAP	returnResultLast

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
▷ GSM Mobile Application
◢ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
      0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
      .1.. .... = TP-UDHI: The beginning of the TP UD field contains a Header in addition to
      ..0. .... = TP-SRI: A status report shall not be returned to the SME
      .... 0... = TP-LP: The message has not been forwarded and is not a spawned message
      .... .0.. = TP-MMS: More messages are waiting for the MS in this SC
      .... ..00 = TP-MTI: SMS-DELIVER (0)
    ◢ TP-Originating-Address - ([redacted]sbank)
         Length: 13 address digits
         1... .... = Extension: No extension
         .101 .... = Type of number: Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-b:
         .... 0000 = Numbering plan: Unknown (0)
         TP-OA Digits [redacted]sbank
    ▷ TP-PID: 0
    ▷ TP-DCS: 0
    ▷ TP-Service-Centre-Time-Stamp
      TP-User-Data-Length: (77) depends on Data-Coding-Scheme
    ◢ TP-User-Data
       ▷ User-Data Header
         SMS text: Snyatie nalichnih. 3000 USD. Ostatok: 967.65 RUR. Hahahahaha!!!! )))))
```

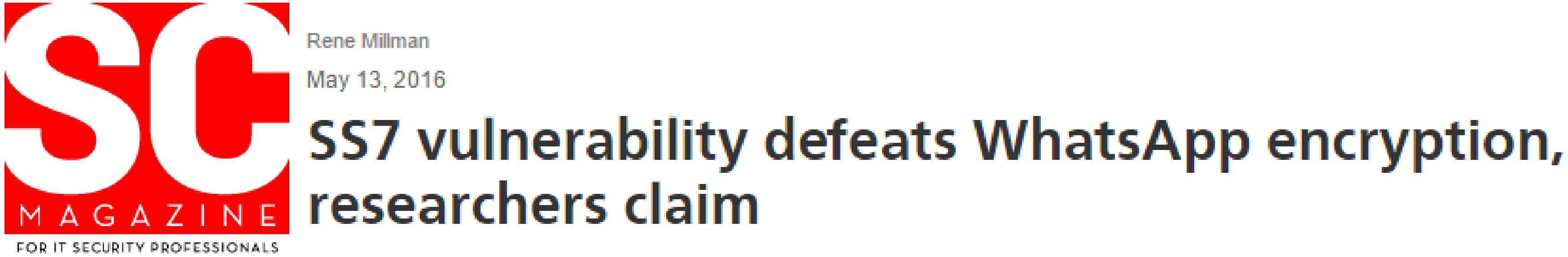
More sophisticated attacks



International Business Times

Technology Social Media

Hackers can impersonate victims and reply to WhatsApp and Telegram chats

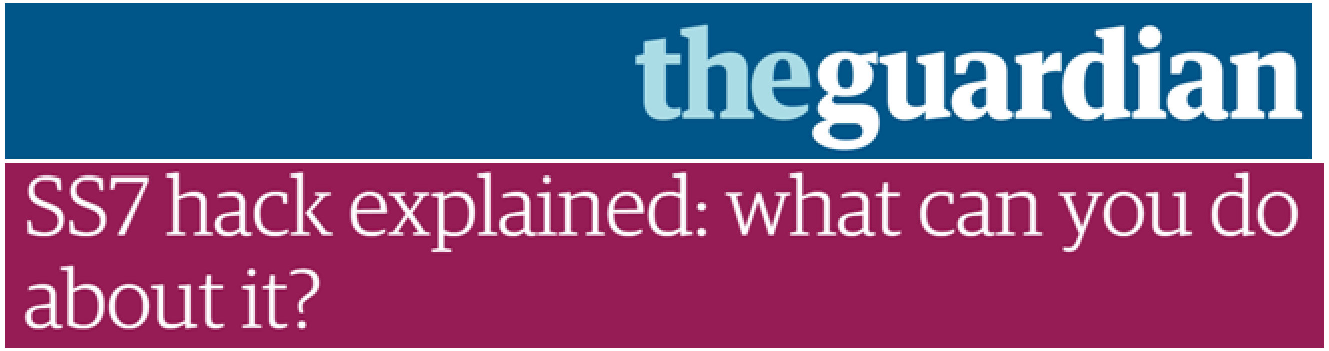


SC MAGAZINE FOR IT SECURITY PROFESSIONALS

Rene Millman

May 13, 2016

SS7 vulnerability defeats WhatsApp encryption, researchers claim



theguardian

SS7 hack explained: what can you do about it?

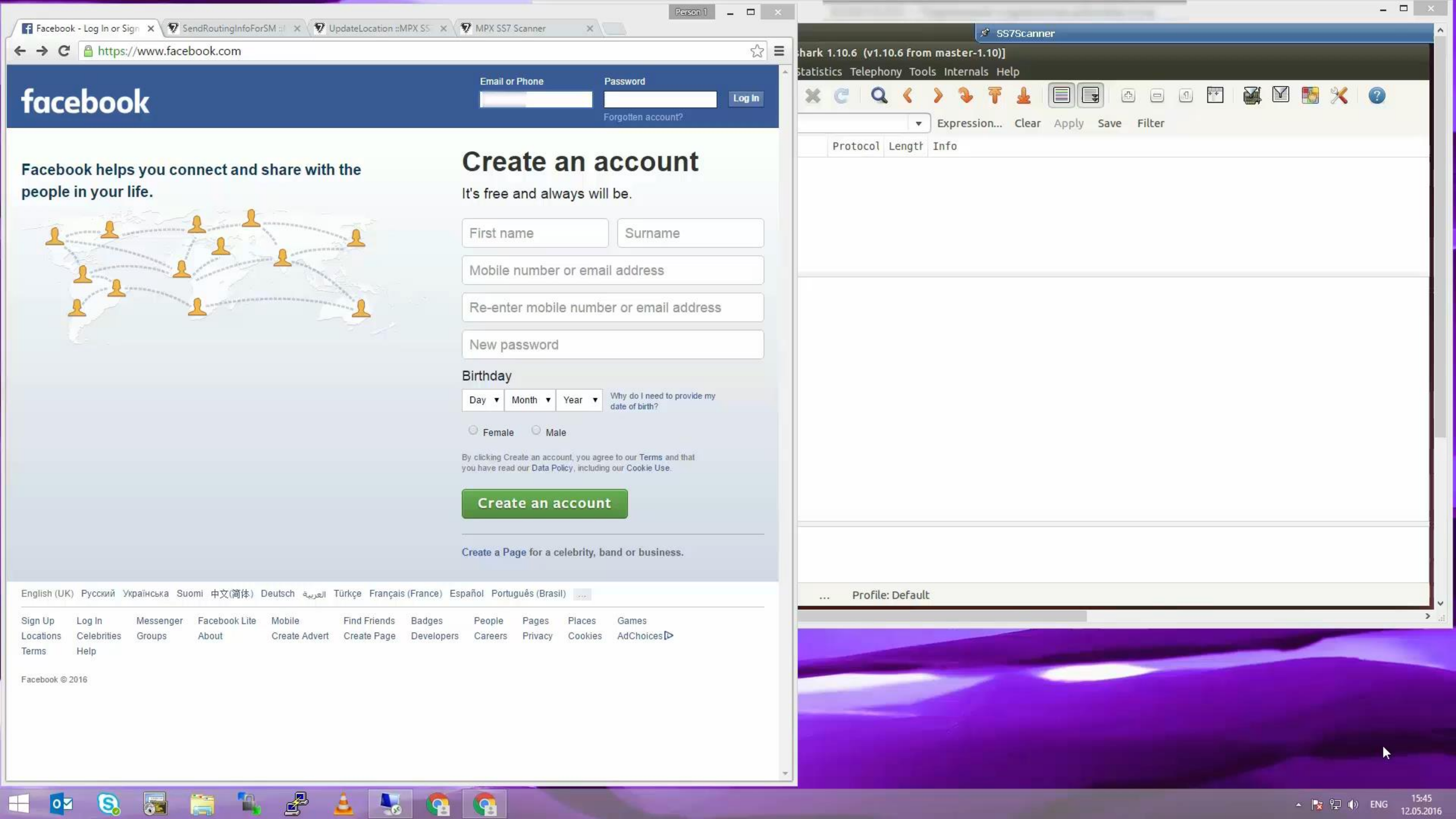
Example

Forbes / Security / #CyberSecurity

Hackers Can Steal Your Facebook Account With Just A Phone Number

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. FULL BIO



Facebook - Log In or Sign | SendRoutingInfoForSM | UpdateLocation ::MPX SS | MPX SS7 Scanner

https://www.facebook.com

facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name | Surname

Mobile number or email address

Re-enter mobile number or email address

New password

Birthday

Day ▾ Month ▾ Year ▾ Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

Create an account

Create a Page for a celebrity, band or business.

English (UK) Русский Українська Suomi 中文(简体) Deutsch العربية Türkçe Français (France) Español Português (Brasil) ...

Sign Up Log In Messenger Facebook Lite Mobile Find Friends Badges People Pages Places Games
Locations Celebrities Groups About Create Advert Create Page Developers Careers Privacy Cookies AdChoices
Terms Help

Facebook © 2016

SS7Scanner

hark 1.10.6 (v1.10.6 from master-1.10)]

Statistics Telephony Tools Internals Help

Expression... Clear Apply Save Filter

Protocol Length Info

... Profile: Default

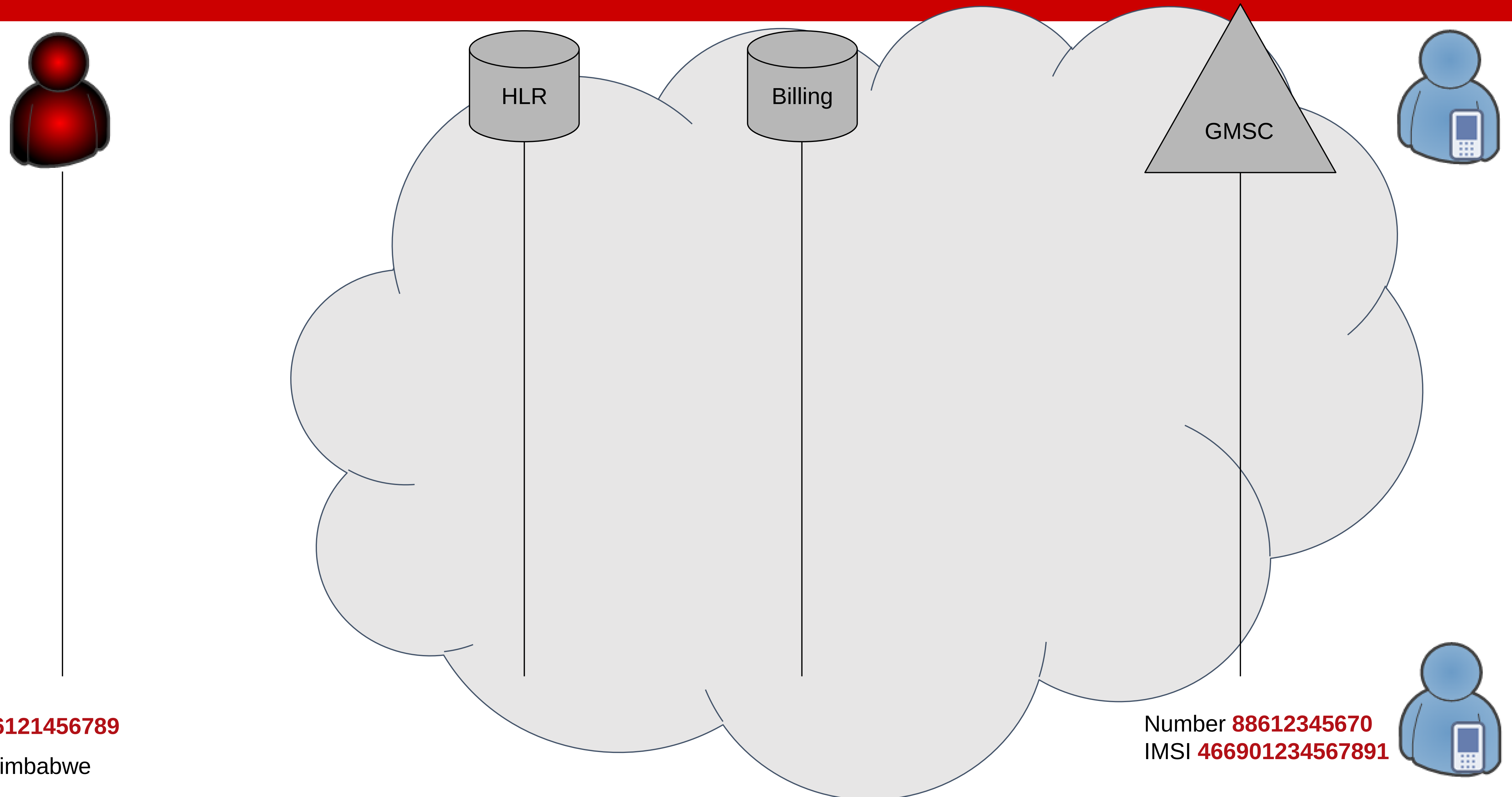
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES

Fraud case 1

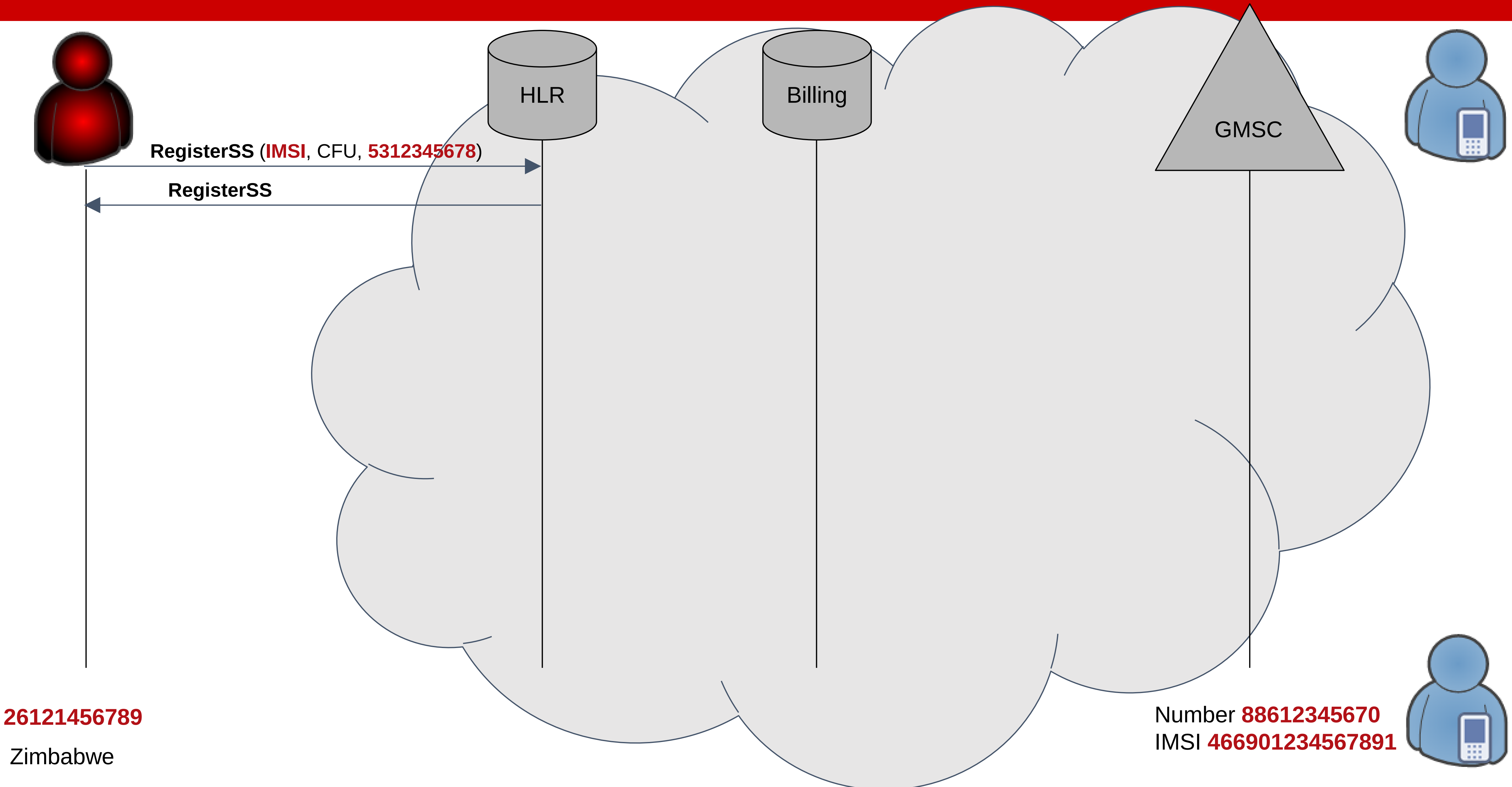
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES

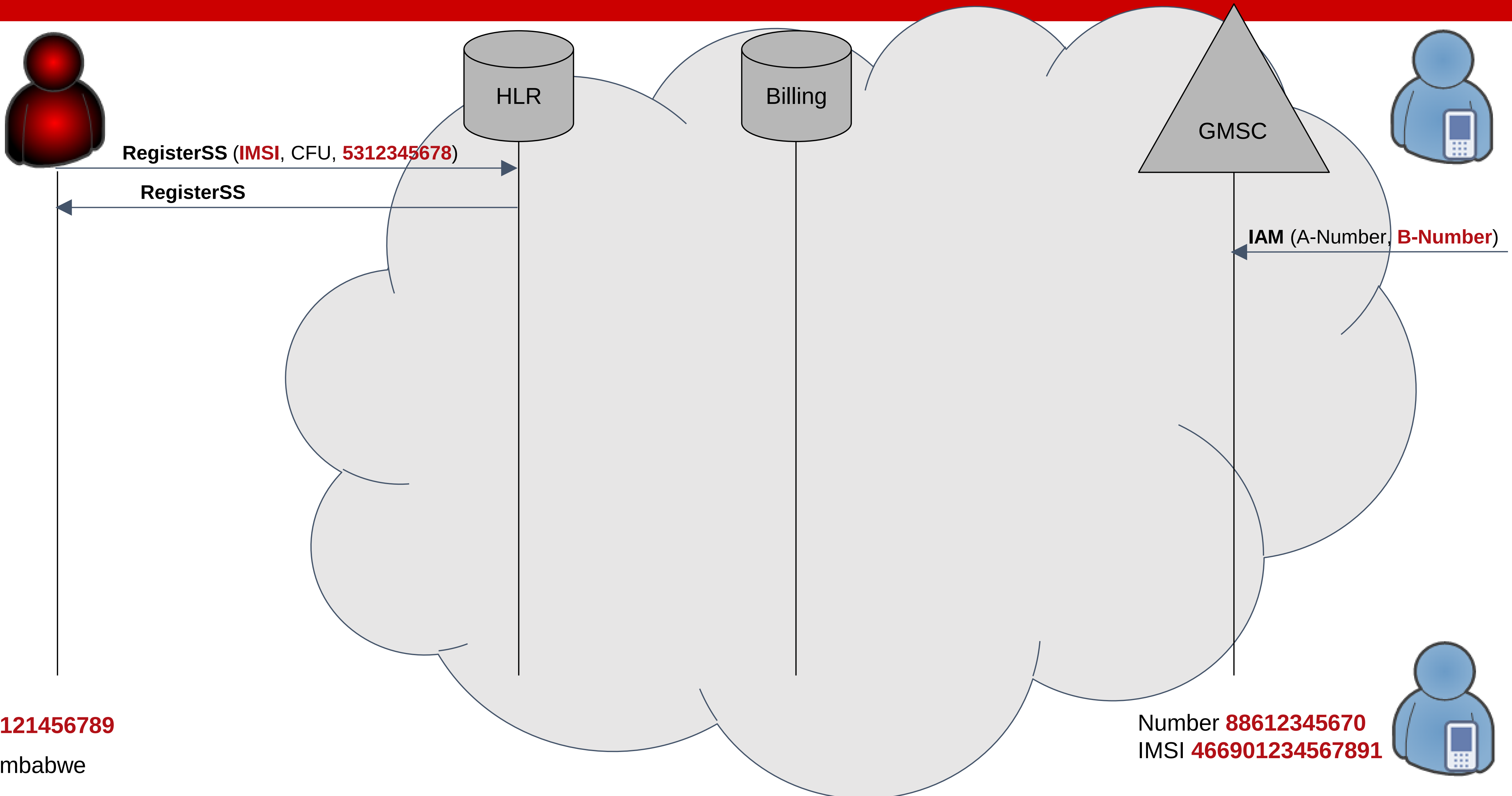


Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES

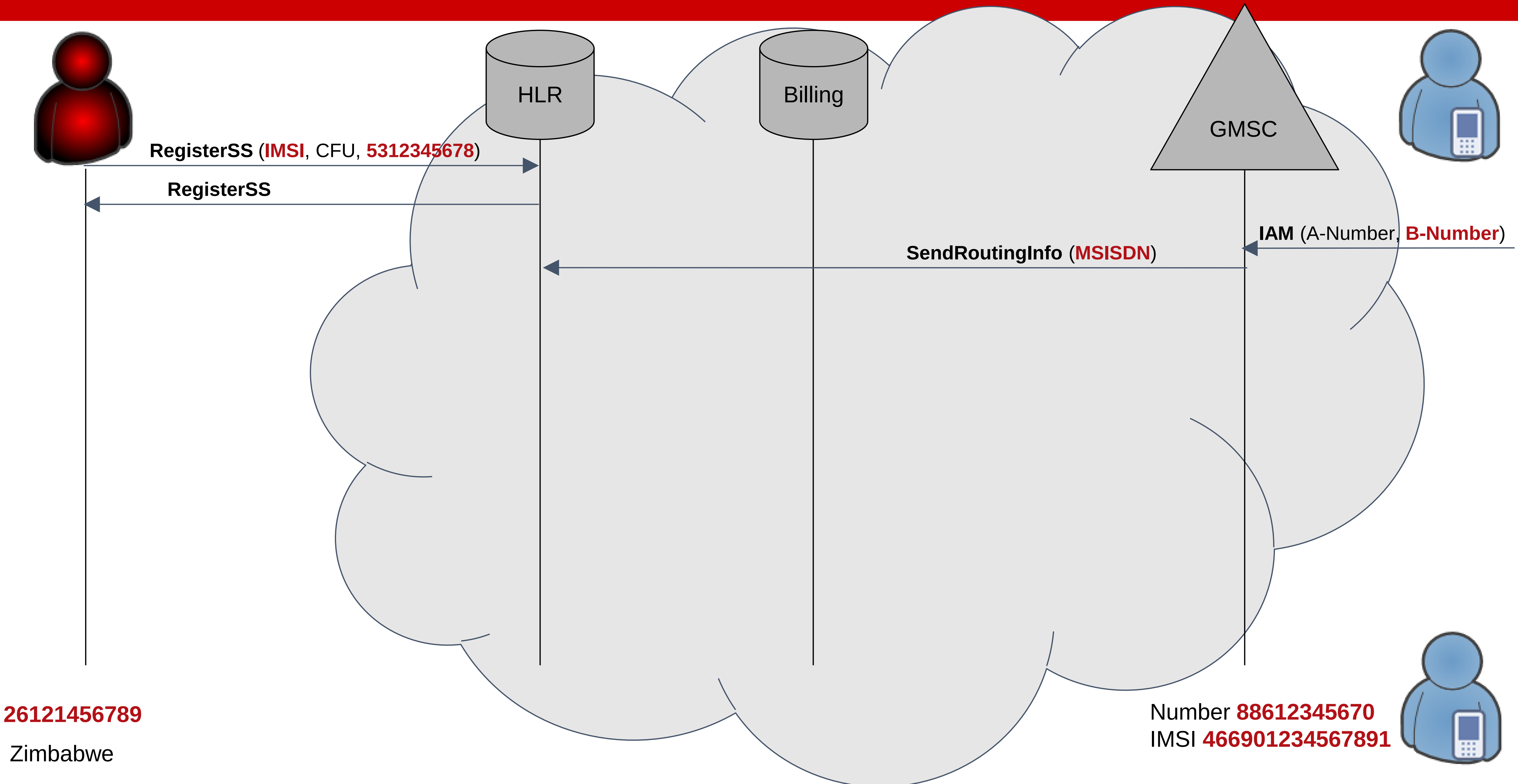


Voice call redirection with a fraudulent activity



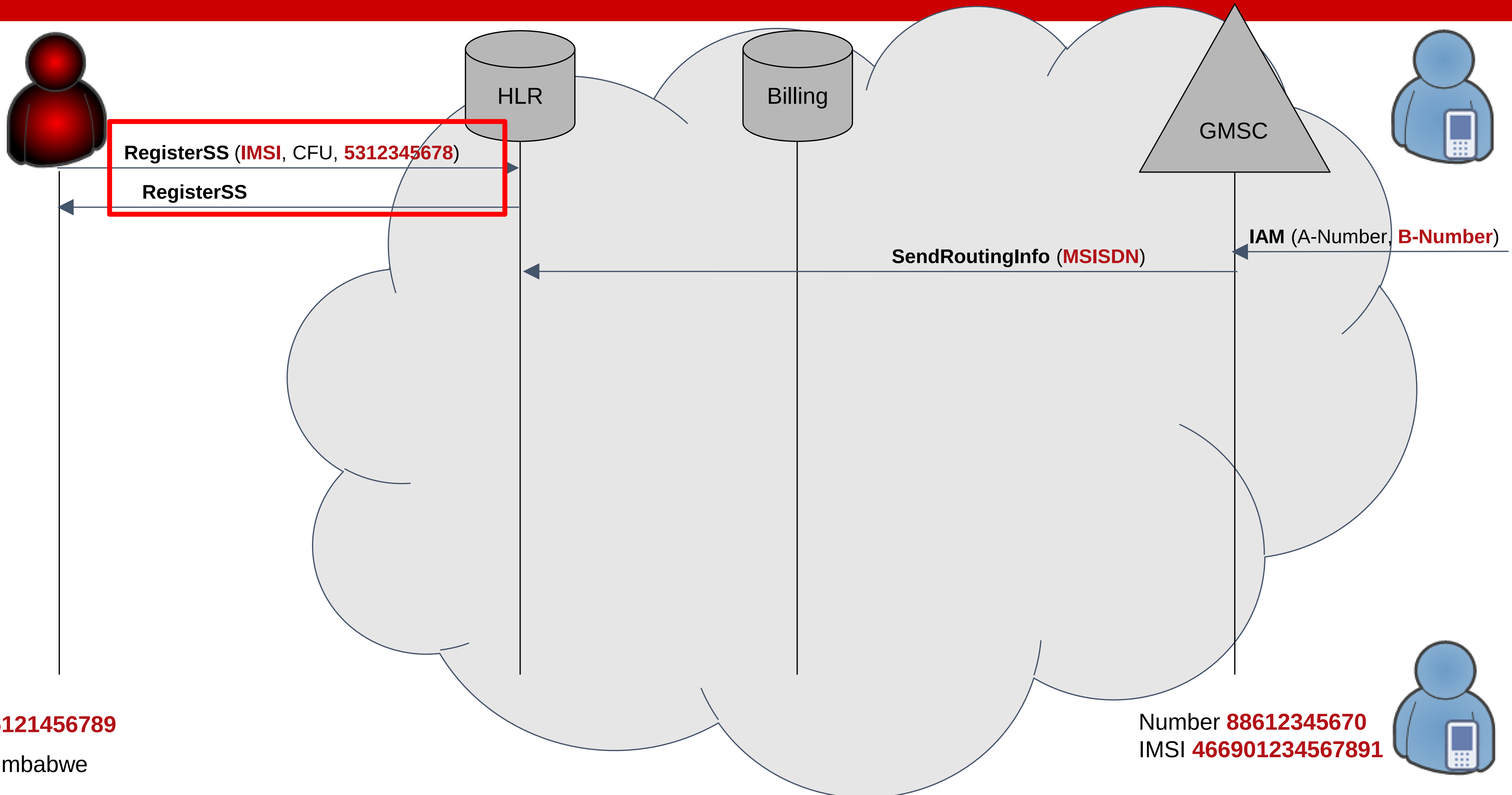
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



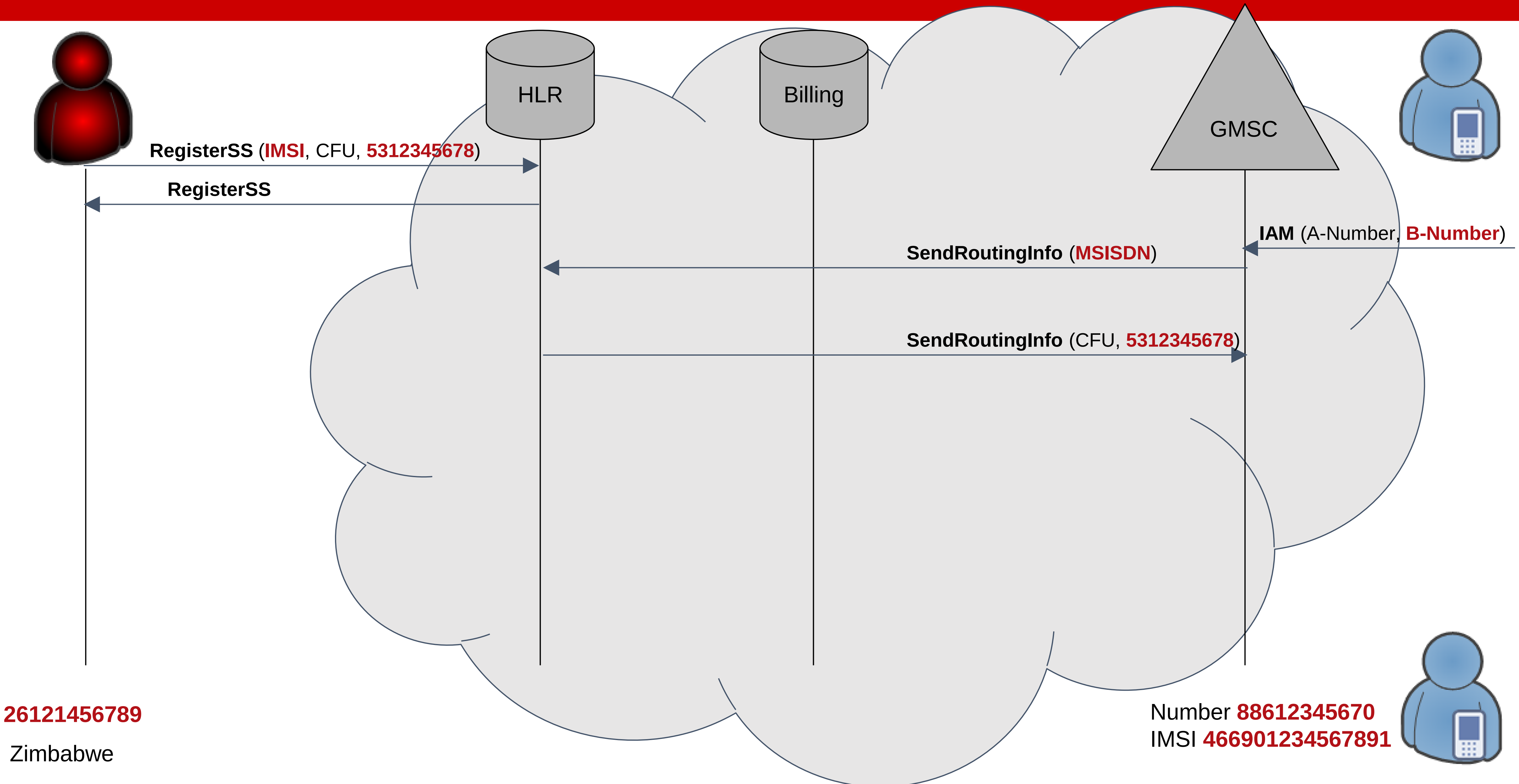
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



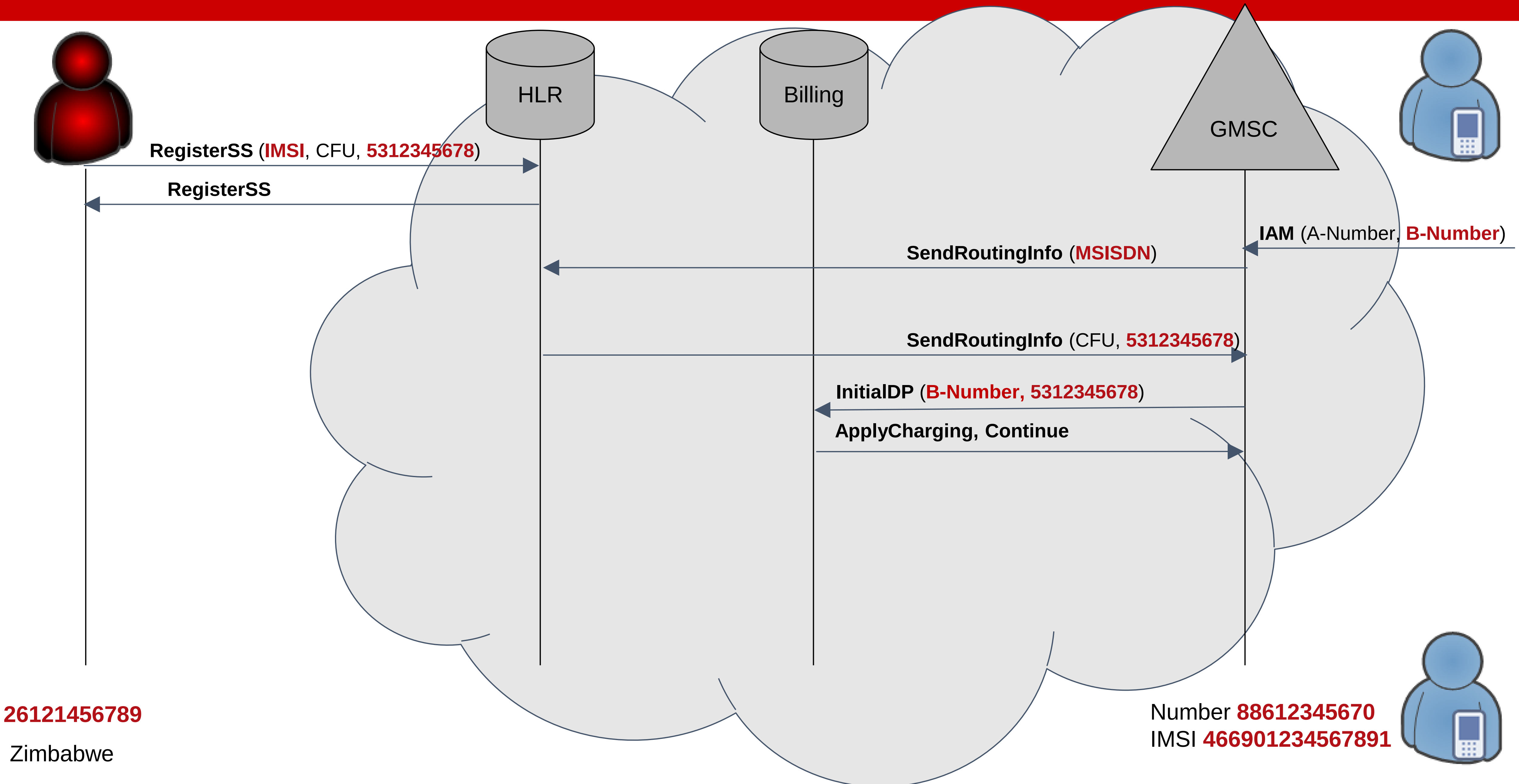
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



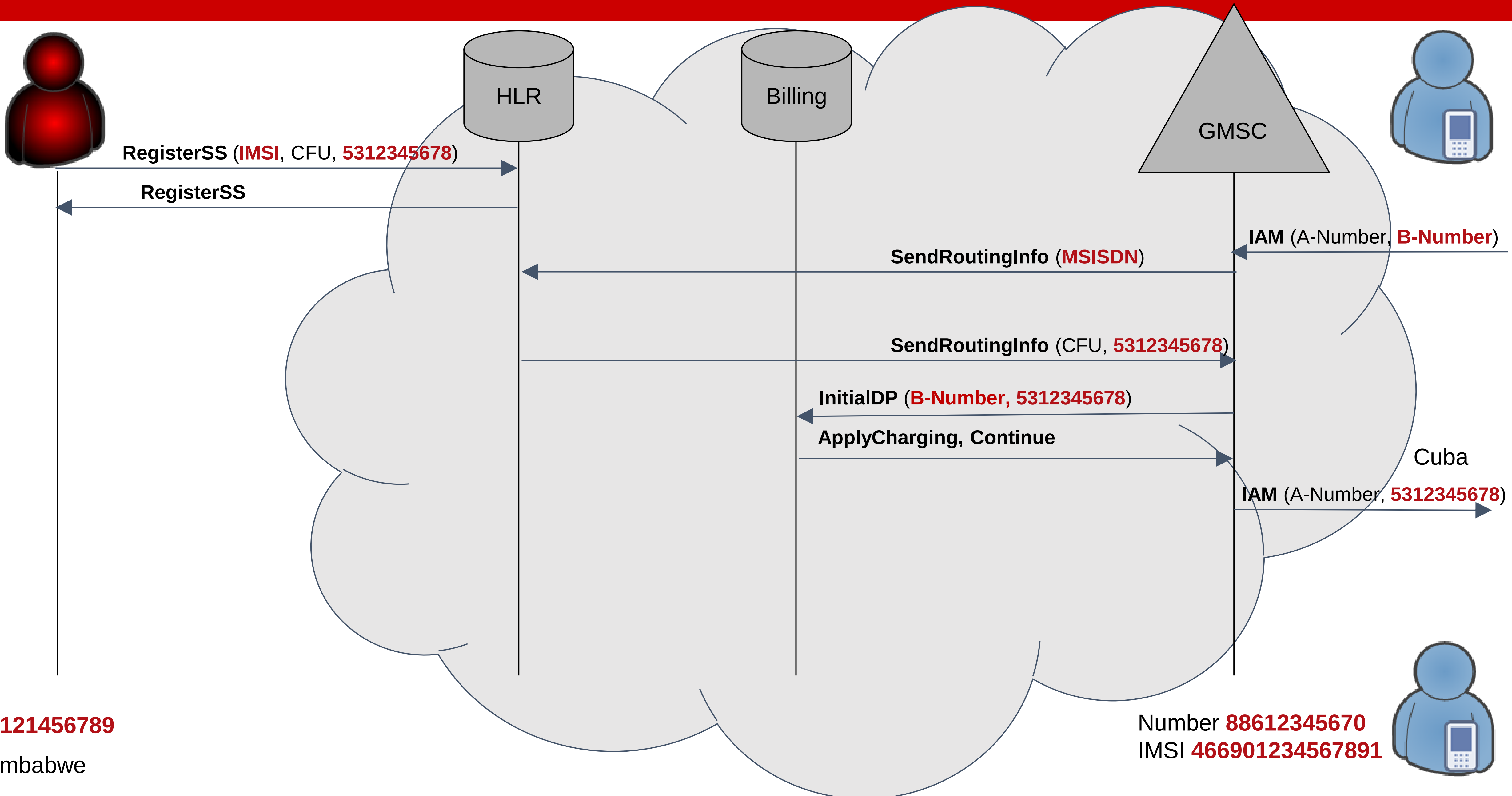
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



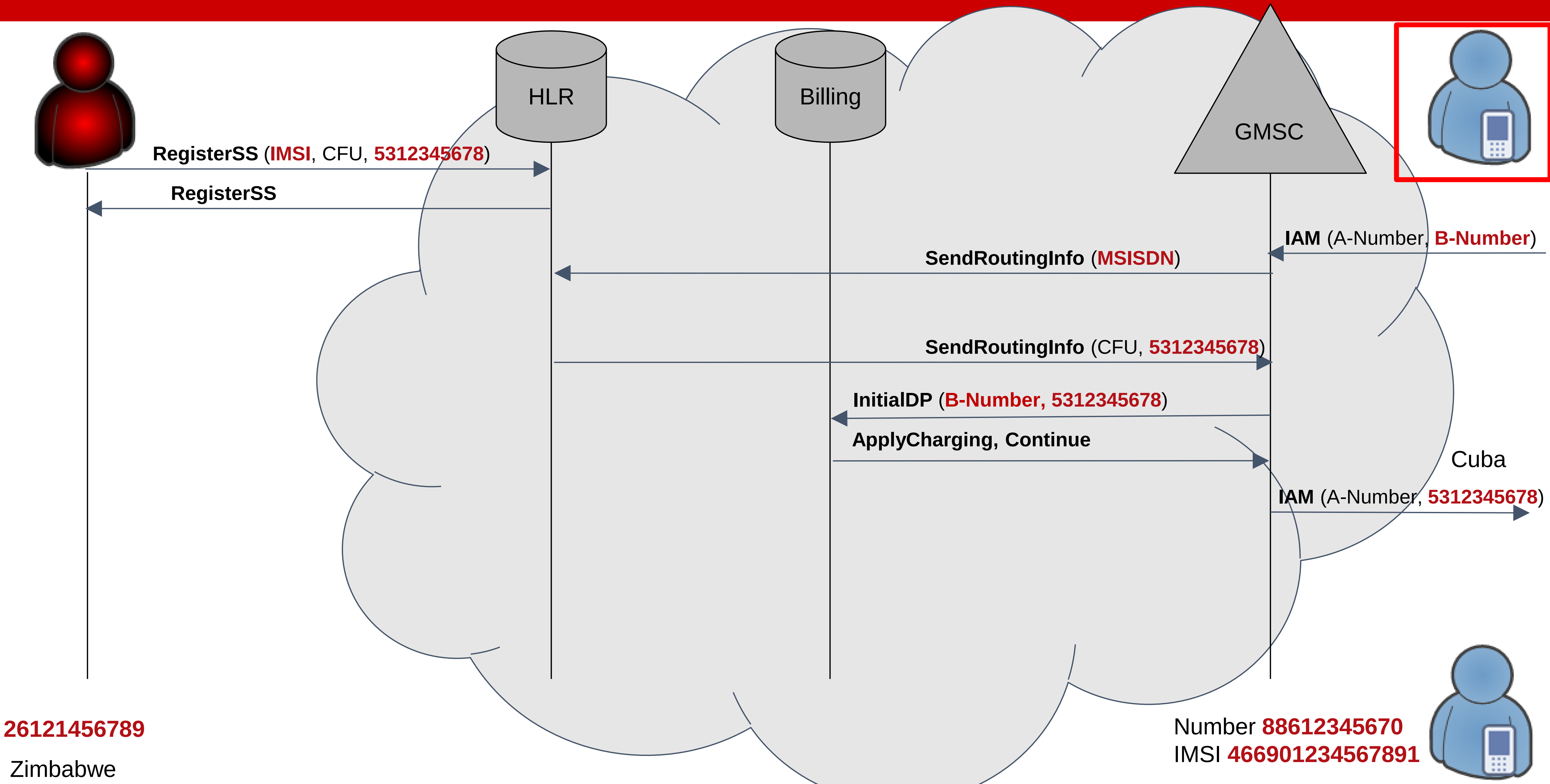
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



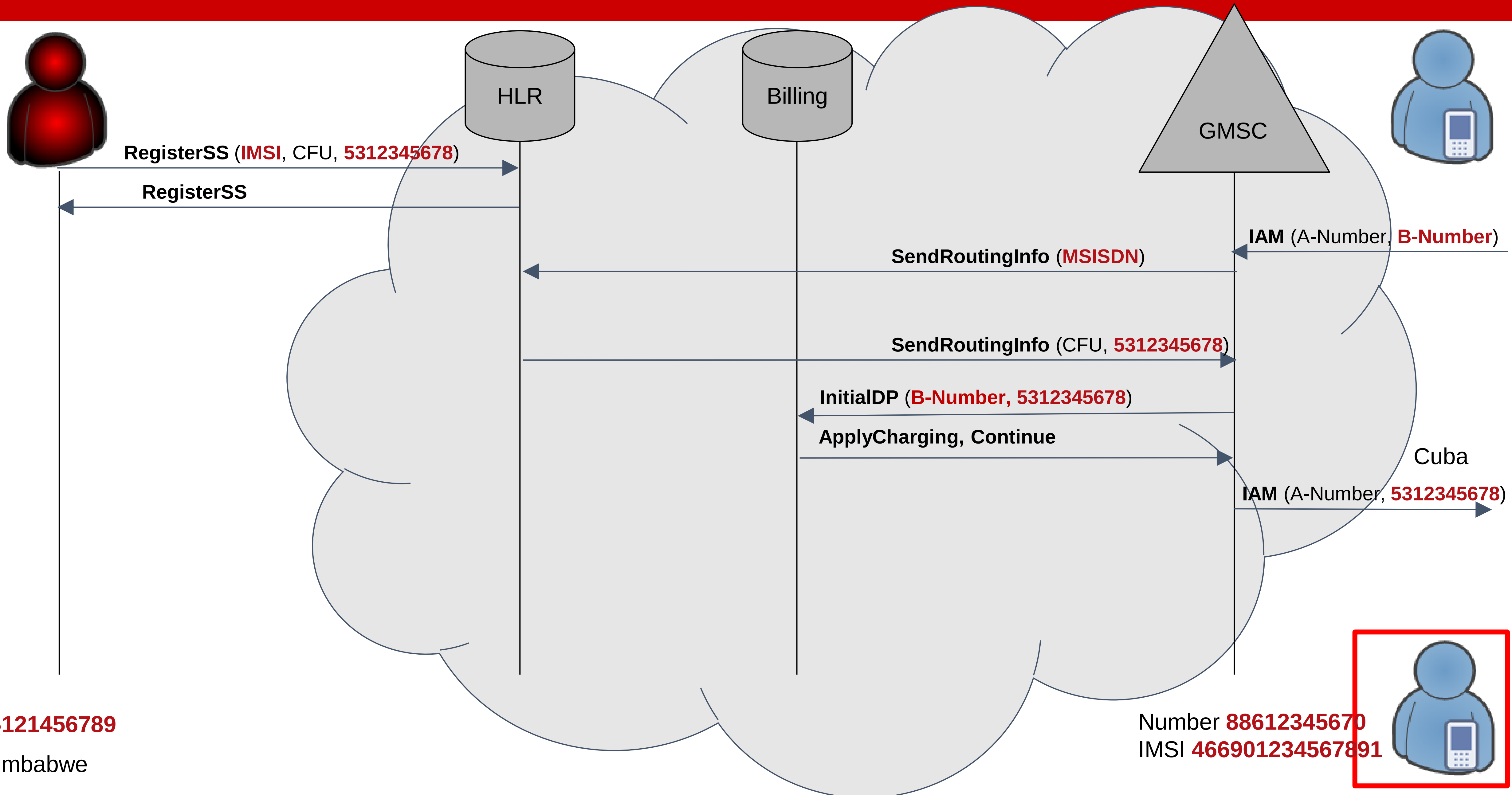
Who pays?

POSITIVE TECHNOLOGIES



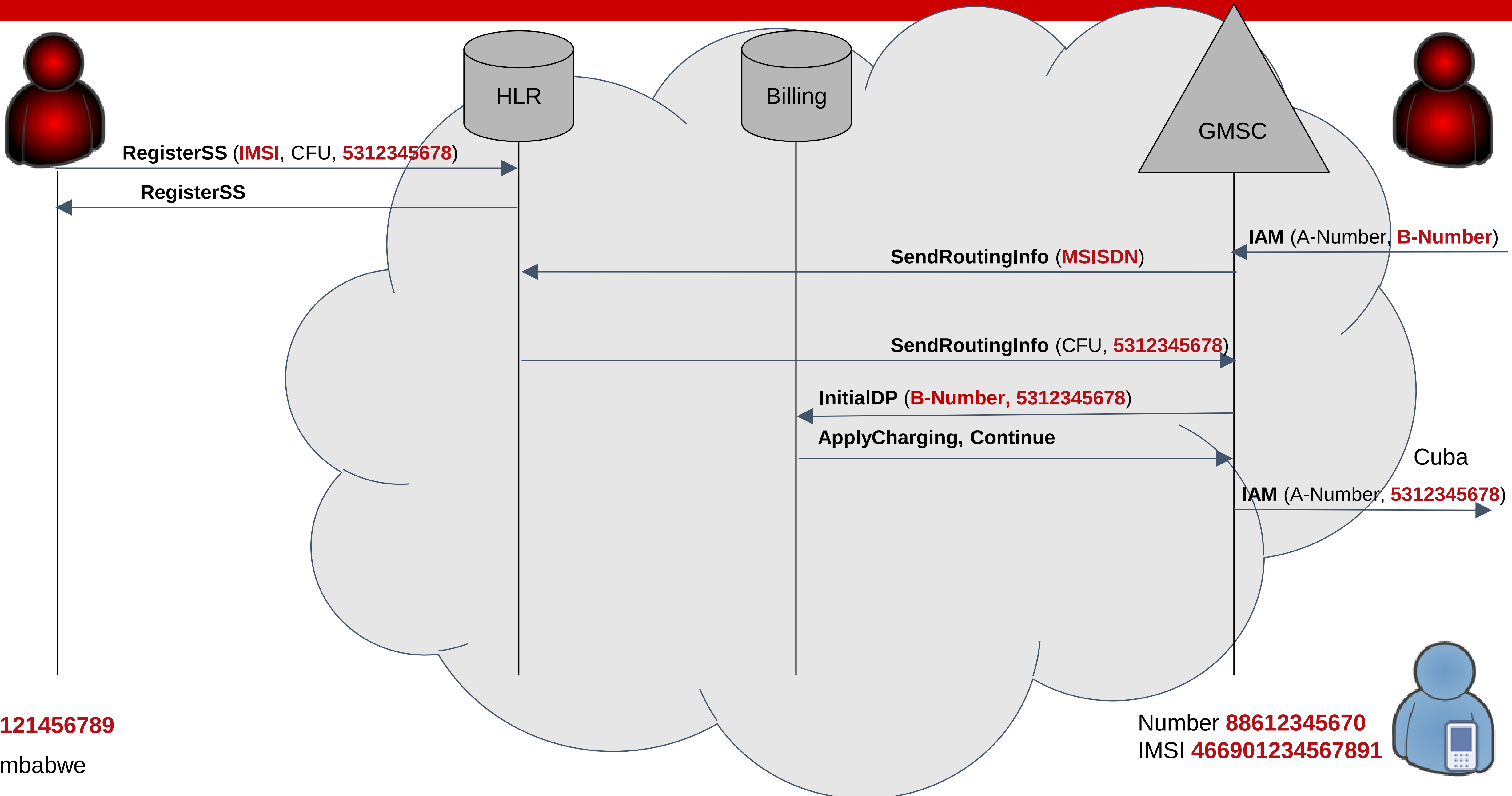
Who pays?

POSITIVE TECHNOLOGIES



Who pays?

POSITIVE TECHNOLOGIES



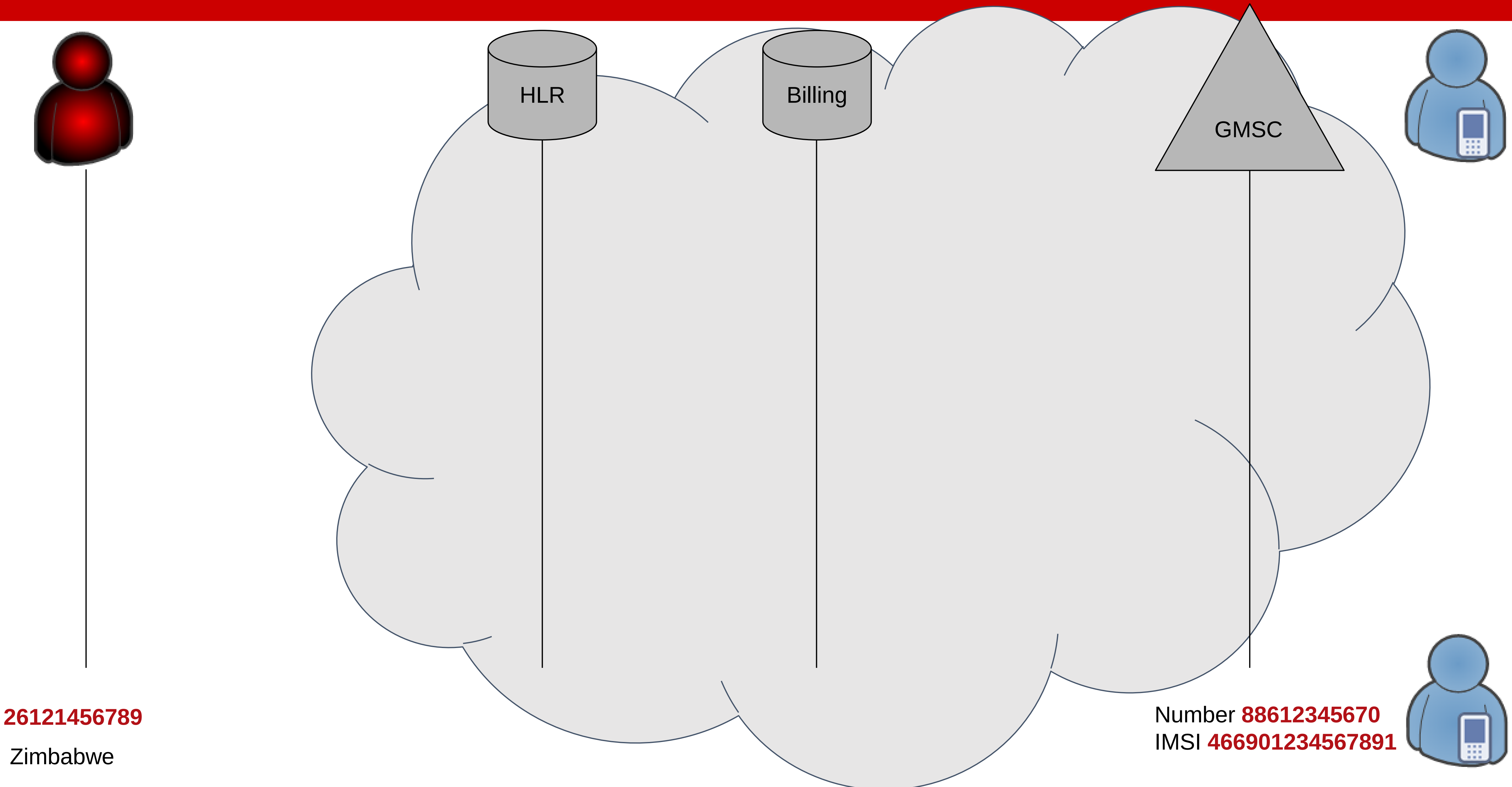
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES

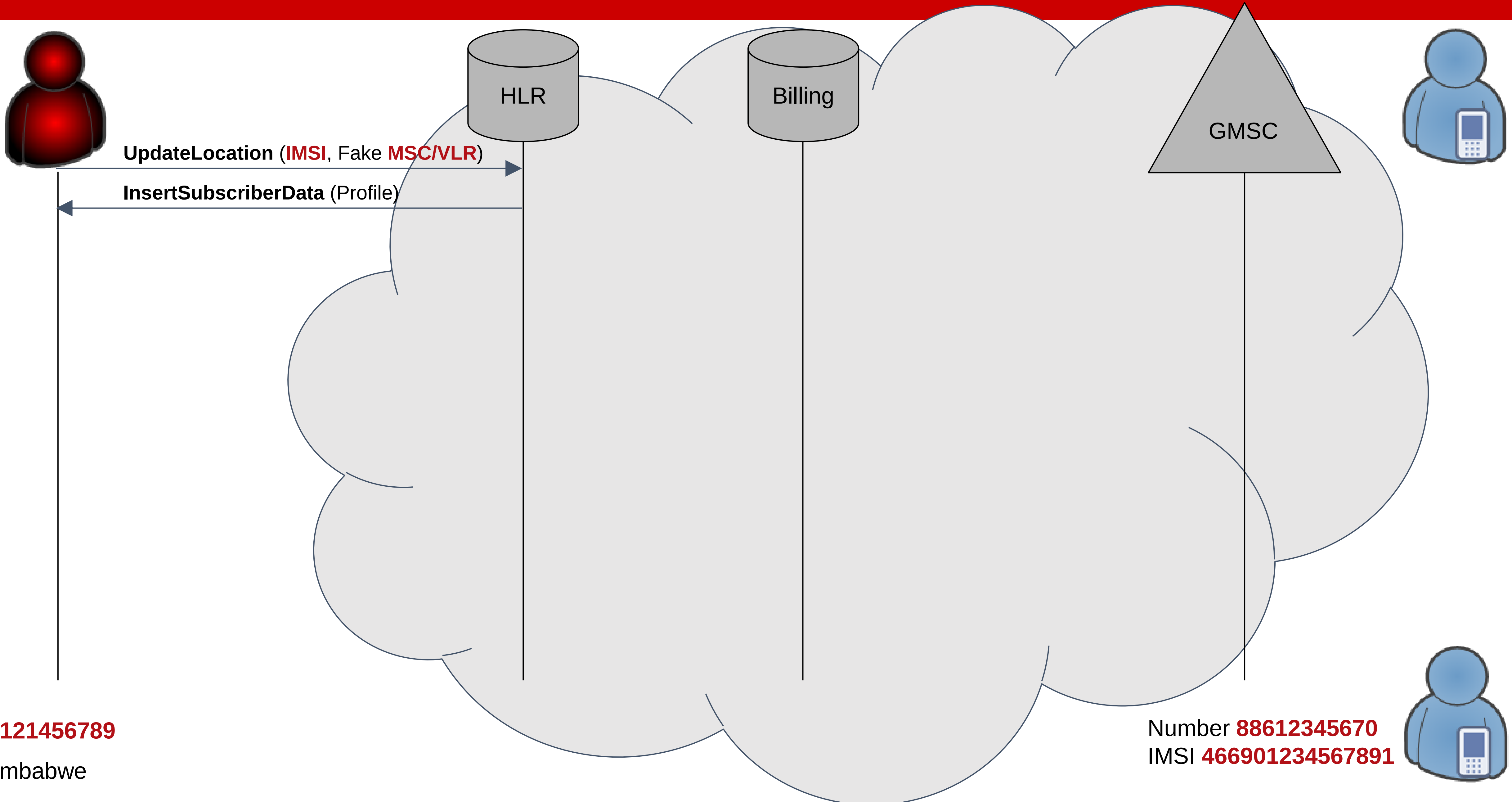
Fraud case 2

Voice call redirection with a fraudulent activity

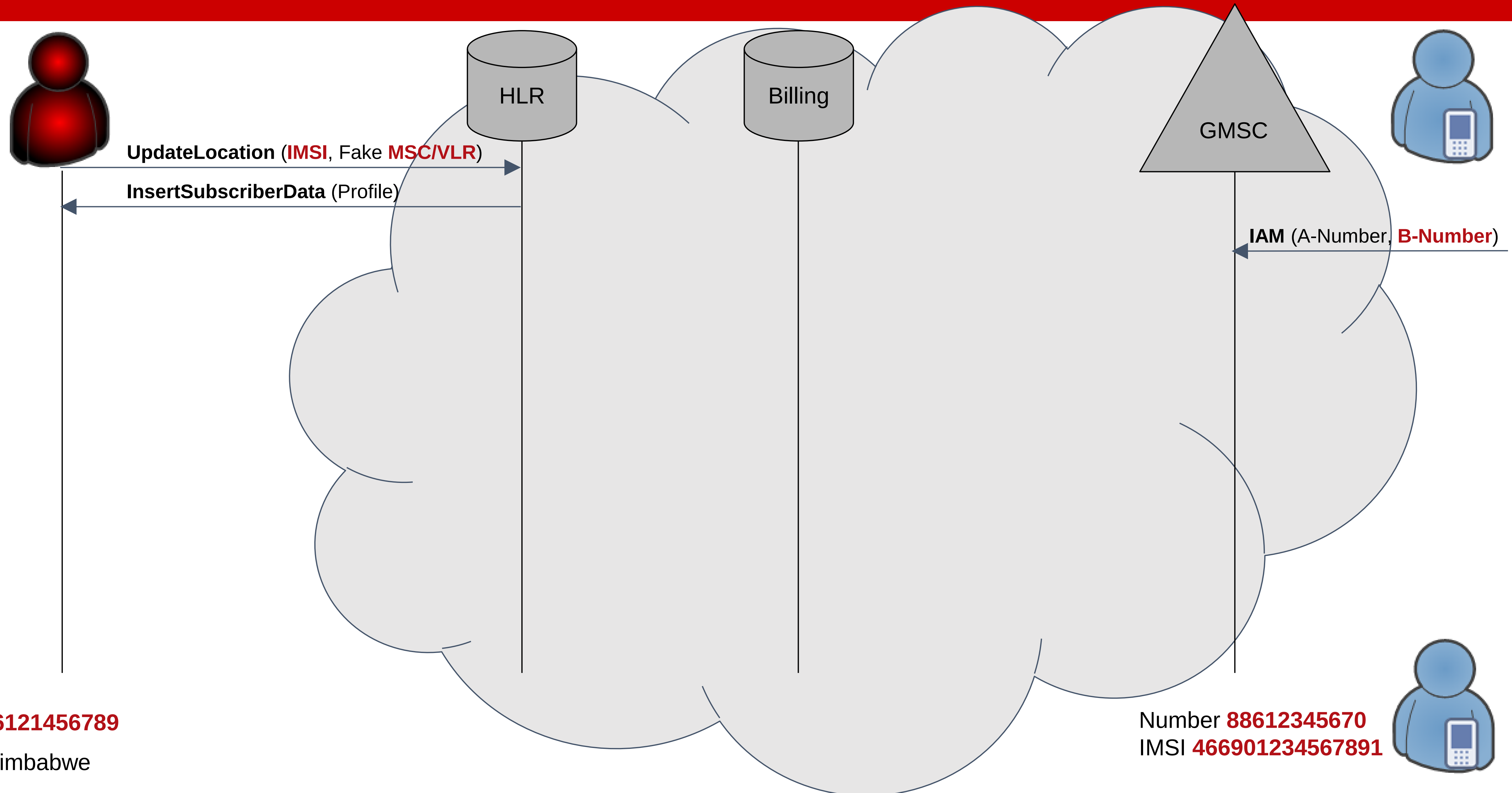
POSITIVE TECHNOLOGIES



Voice call redirection with a fraudulent activity

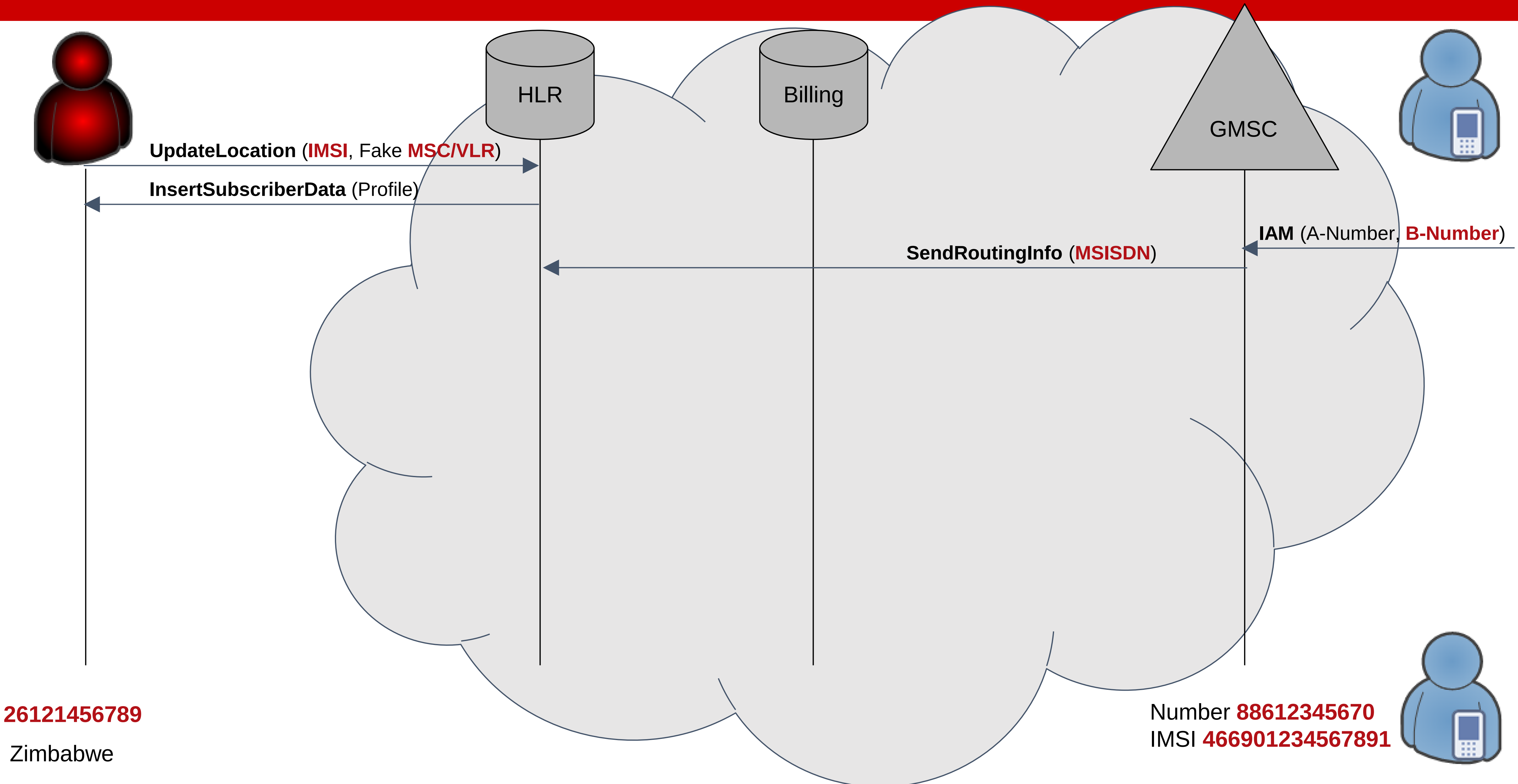


Voice call redirection with a fraudulent activity


HLR
Billing
GMSC
UpdateLocation (**IMSI**, Fake **MSC/VLR**)
InsertSubscriberData (Profile)
IAM (A-Number, **B-Number**)
26121456789
Zimbabwe
Number **88612345670**
IMSI **466901234567891**

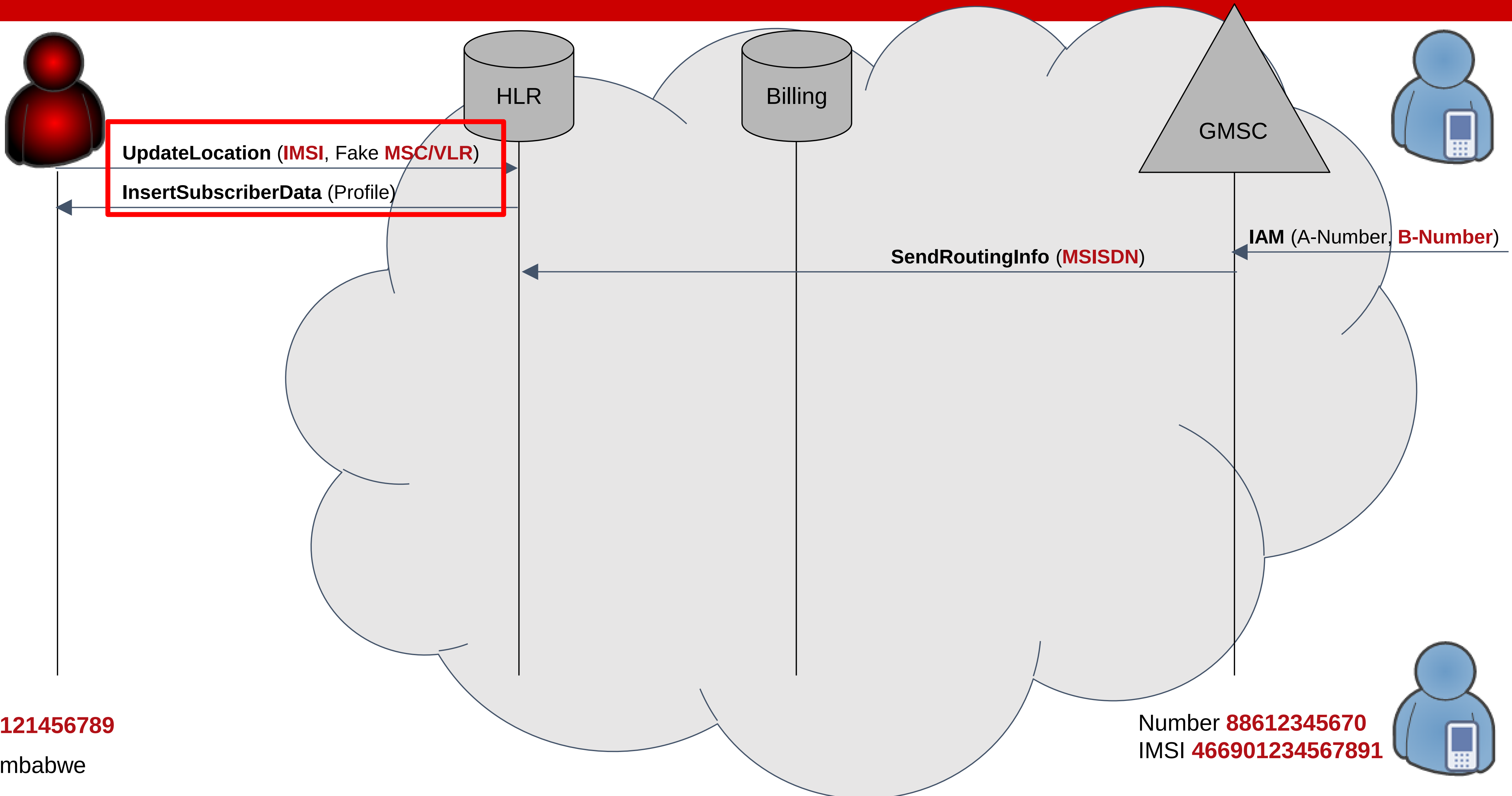
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES


HLR
Billing
GMSC
UpdateLocation (**IMSI**, Fake **MSC/VLR**)
InsertSubscriberData (Profile)
IAM (A-Number, **B-Number**)
SendRoutingInfo (**MSISDN**)
26121456789
Zimbabwe
Number **88612345670**
IMSI **466901234567891**

Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)

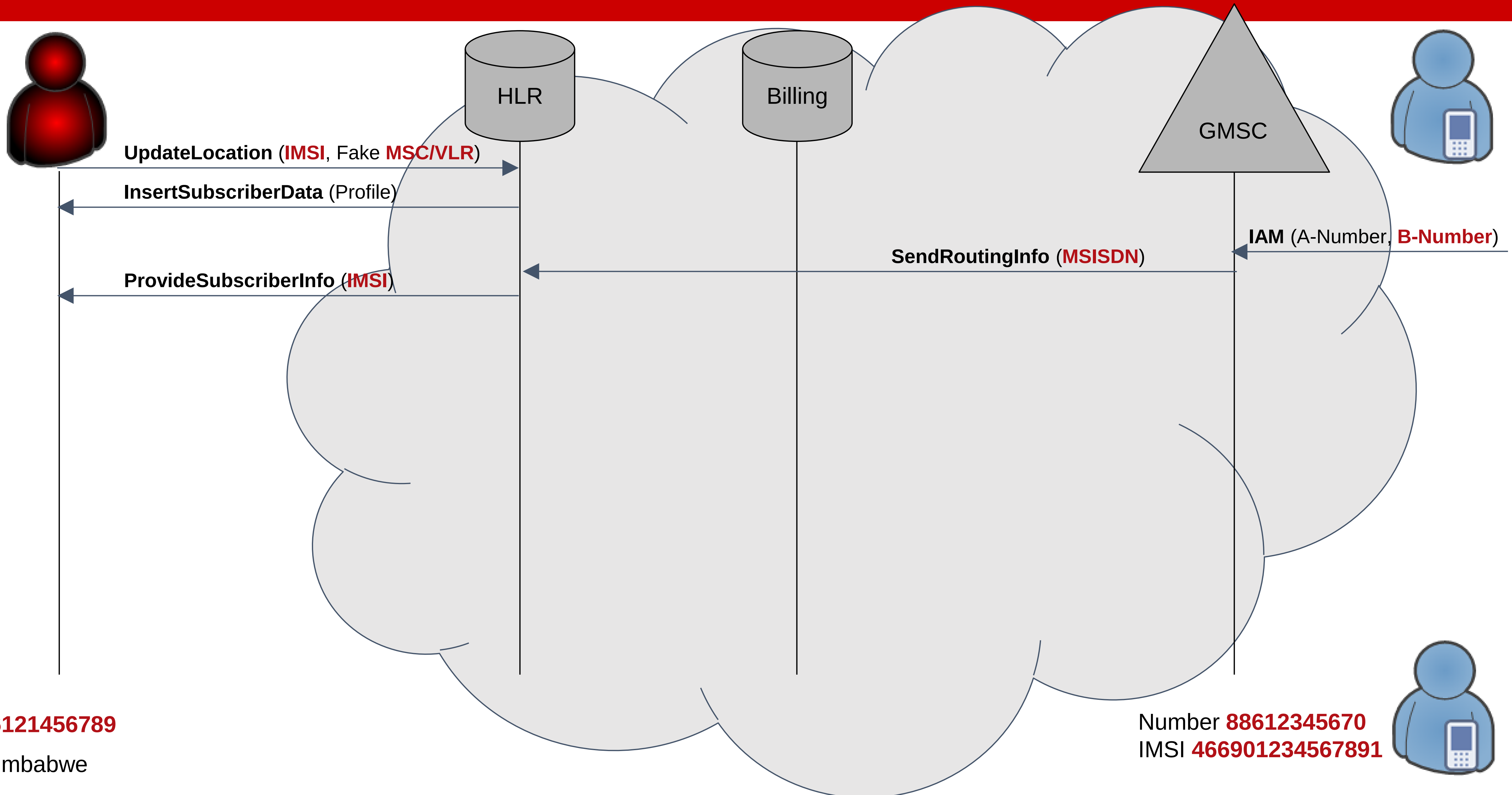
26121456789

Zimbabwe

Number 88612345670
IMSI 466901234567891

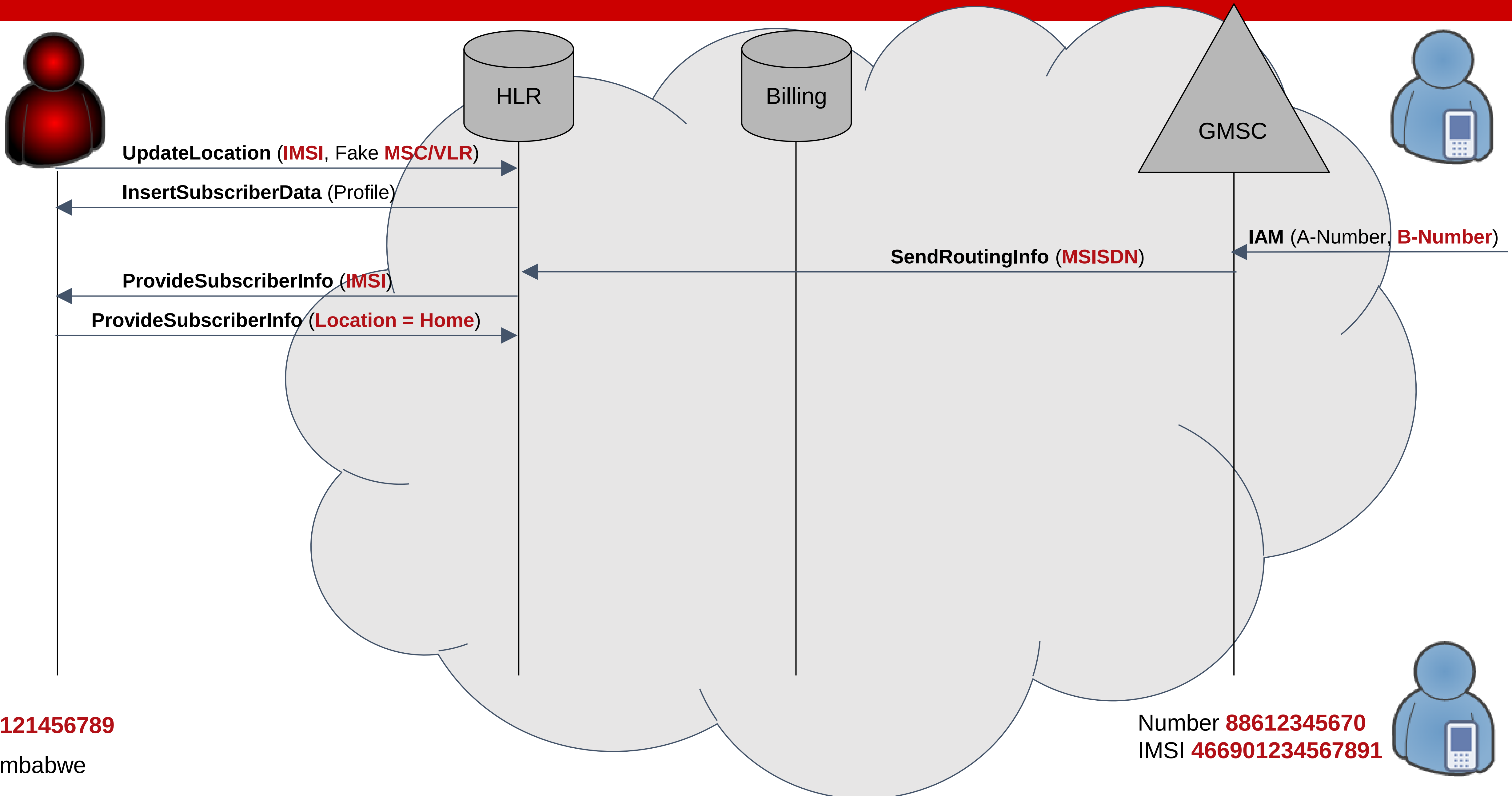
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES


HLR
Billing
GMSC
UpdateLocation (**IMSI**, Fake **MSC/VLR**)
InsertSubscriberData (Profile)
IAM (A-Number, **B-Number**)
SendRoutingInfo (**MSISDN**)
ProvideSubscriberInfo (**IMSI**)
26121456789
Zimbabwe
Number 88612345670
IMSI 466901234567891

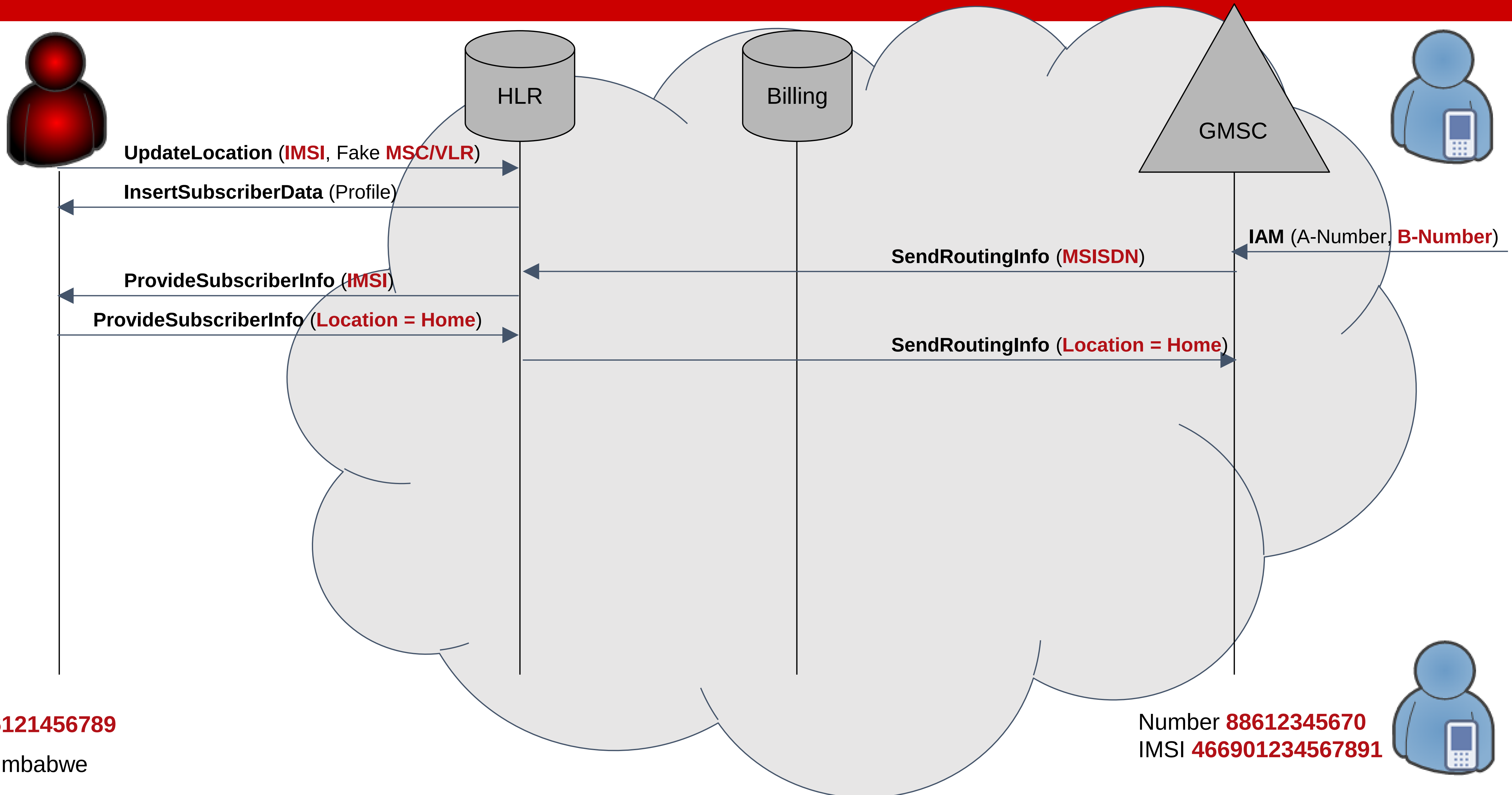
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



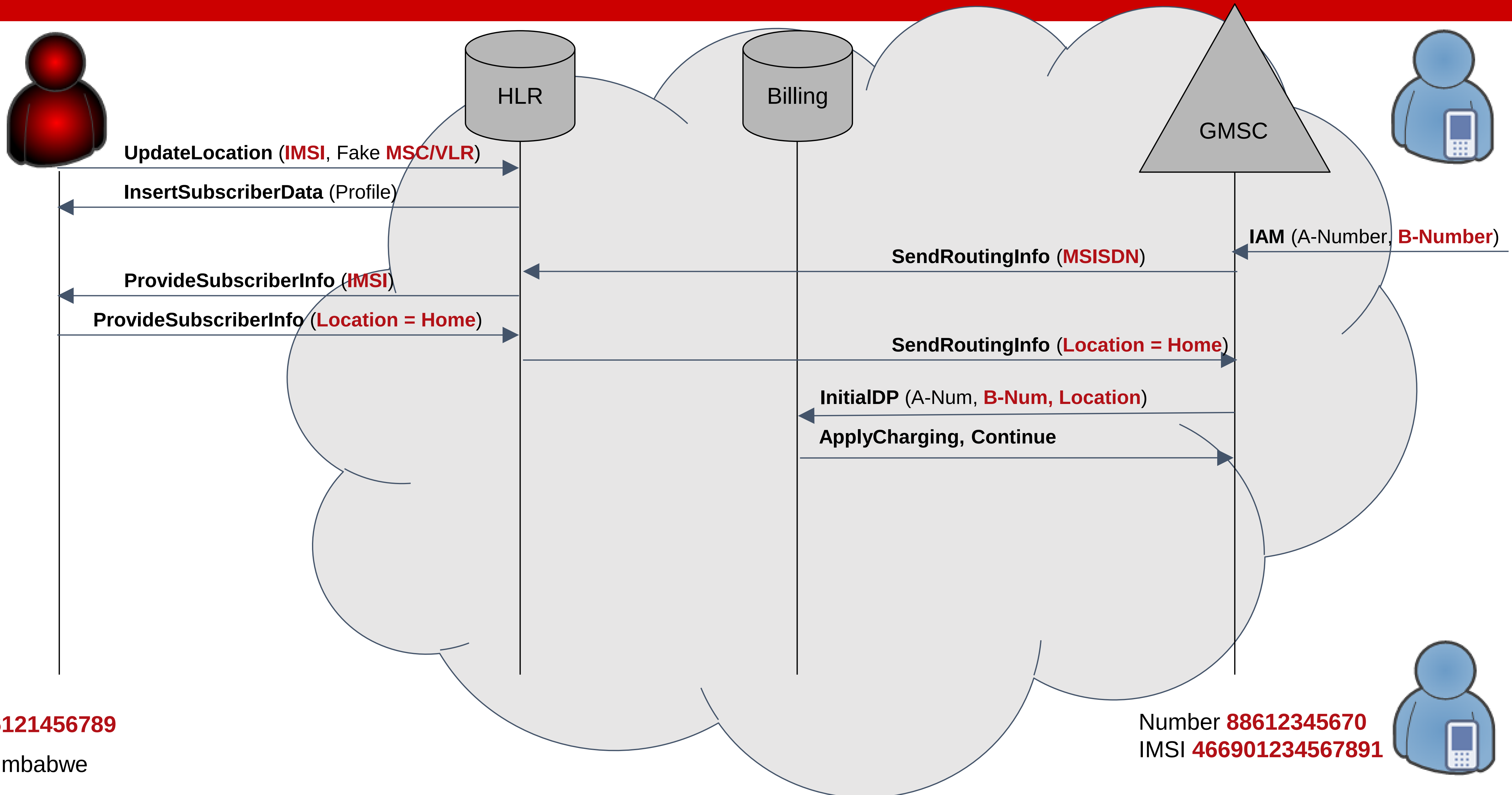
HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
26121456789
Zimbabwe
Number 88612345670
IMSI 466901234567891

Voice call redirection with a fraudulent activity


HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
SendRoutingInfo (Location = Home)
26121456789
Zimbabwe
Number 88612345670
IMSI 466901234567891

Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
SendRoutingInfo (Location = Home)
InitialDP (A-Num, B-Num, Location)
ApplyCharging, Continue

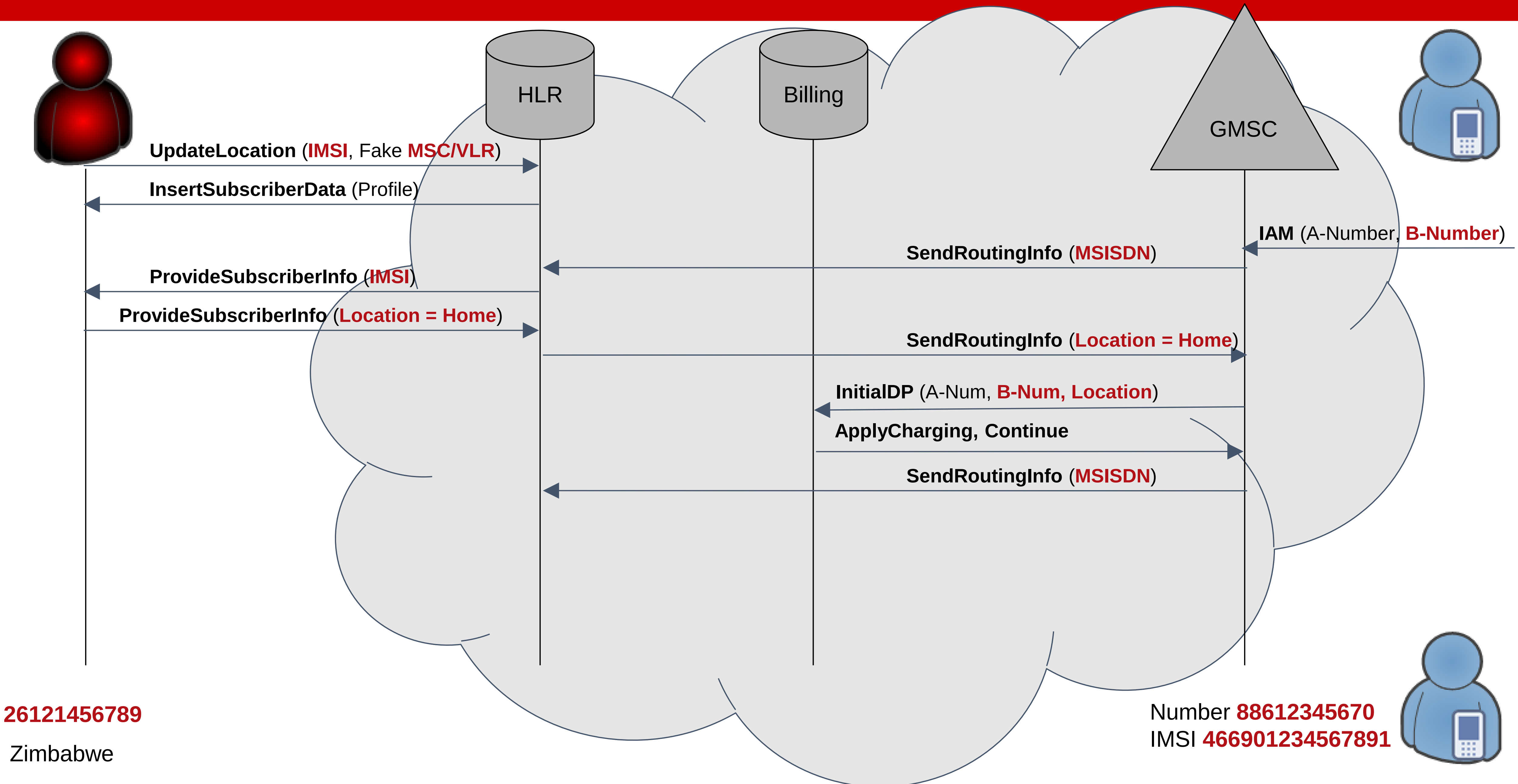
26121456789

Zimbabwe

Number 88612345670
IMSI 466901234567891

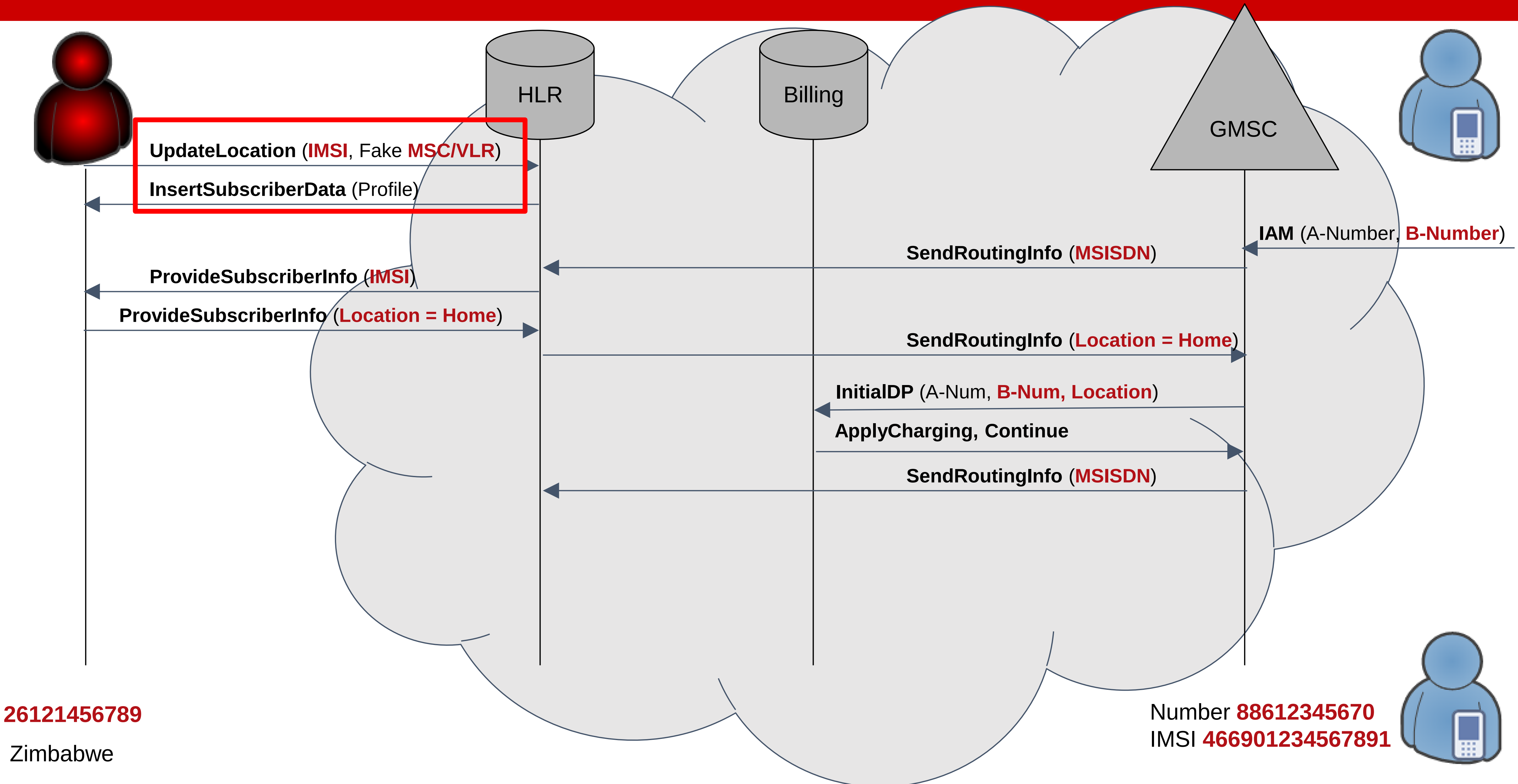
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES



HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
SendRoutingInfo (Location = Home)
InitialDP (A-Num, B-Num, Location)
ApplyCharging, Continue
SendRoutingInfo (MSISDN)
26121456789
Zimbabwe
Number 88612345670
IMSI 466901234567891

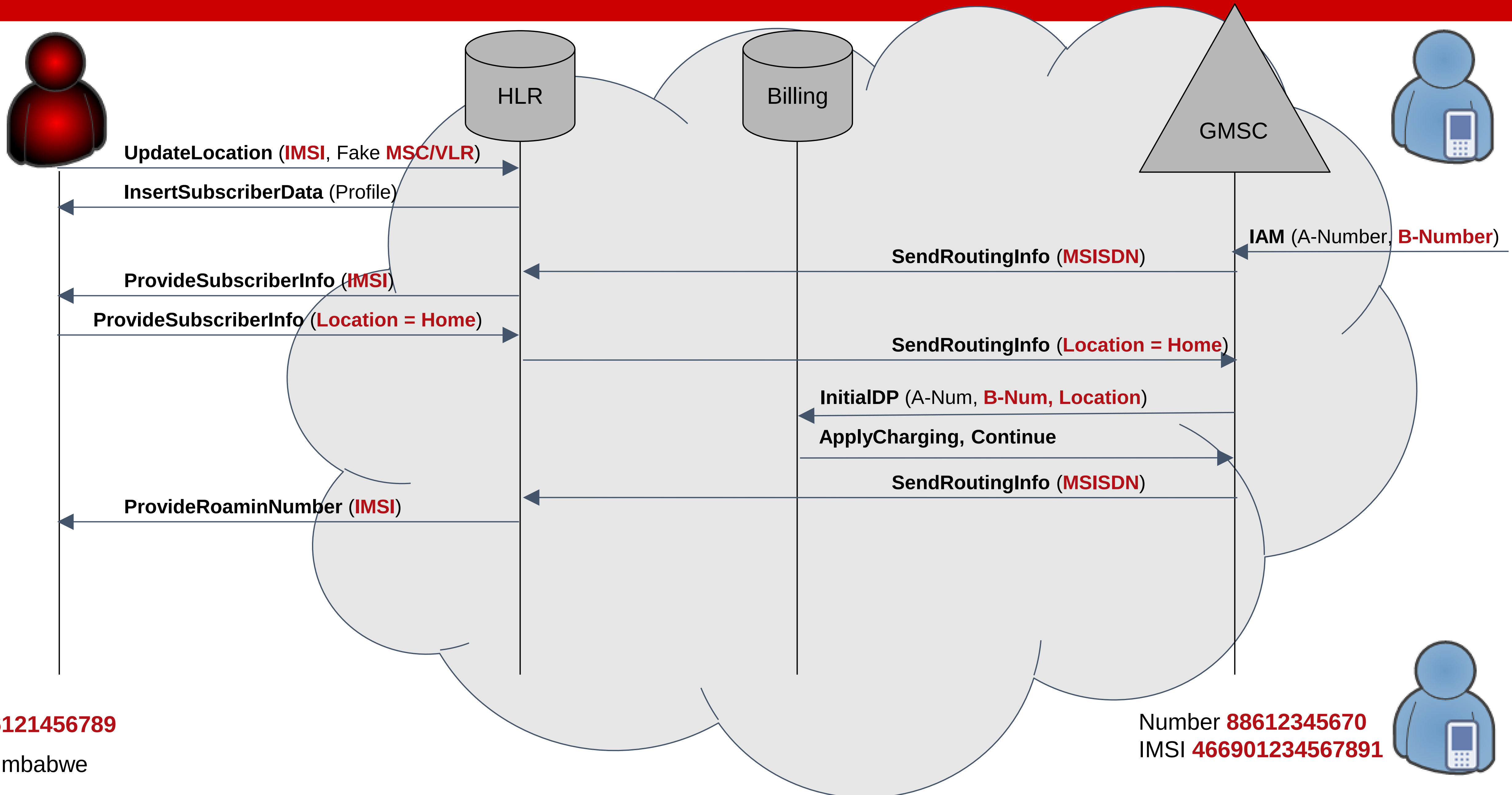
Voice call redirection with a fraudulent activity



HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
SendRoutingInfo (Location = Home)
InitialDP (A-Num, B-Num, Location)
ApplyCharging, Continue
SendRoutingInfo (MSISDN)
26121456789
Zimbabwe
Number 88612345670
IMSI 466901234567891

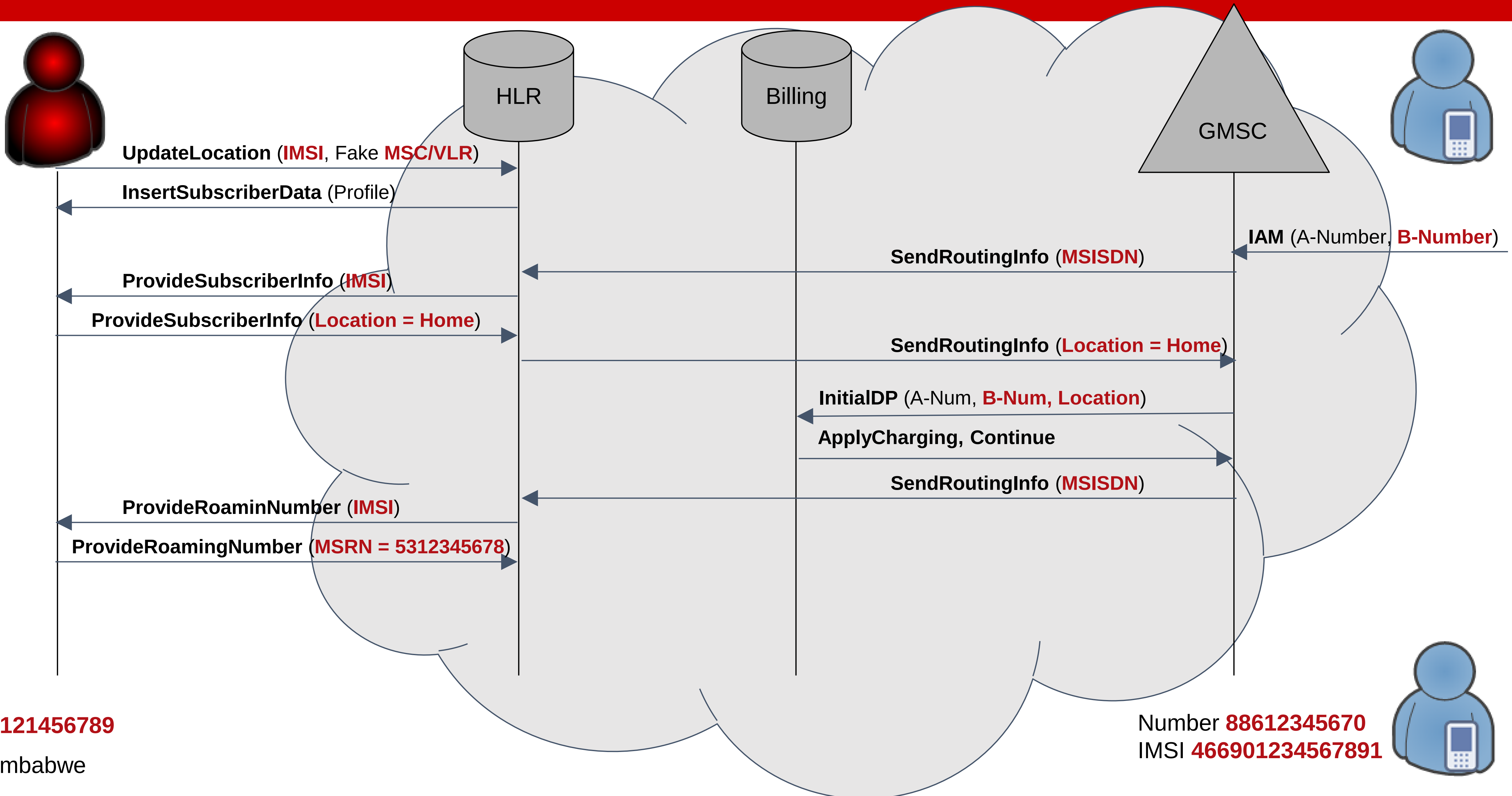
Voice call redirection with a fraudulent activity

POSITIVE TECHNOLOGIES


HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
SendRoutingInfo (Location = Home)
InitialDP (A-Num, B-Num, Location)
ApplyCharging, Continue
SendRoutingInfo (MSISDN)
ProvideRoaminNumber (IMSI)
26121456789
Zimbabwe
Number 88612345670
IMSI 466901234567891

Voice call redirection with a fraudulent activity

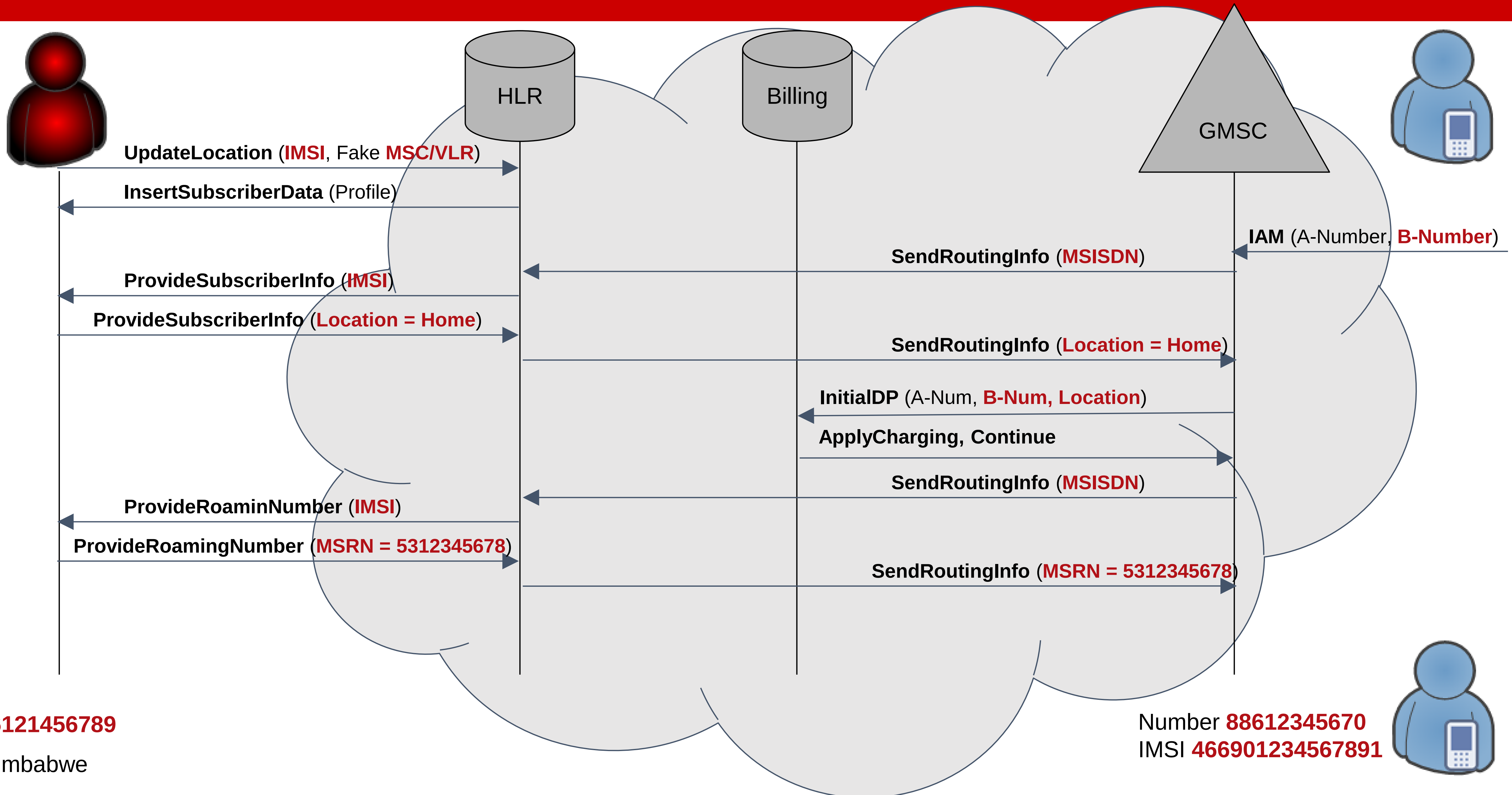
POSITIVE TECHNOLOGIES


HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
SendRoutingInfo (Location = Home)
InitialDP (A-Num, B-Num, Location)
ApplyCharging, Continue
SendRoutingInfo (MSISDN)
ProvideRoaminNumber (IMSI)
ProvideRoamingNumber (MSRN = 5312345678)
Number 88612345670
IMSI 466901234567891

26121456789

Zimbabwe

Voice call redirection with a fraudulent activity



HLR

Billing

GMSC

UpdateLocation (**IMSI**, Fake **MSC/VLR**)

InsertSubscriberData (Profile)

IAM (A-Number, **B-Number**)

SendRoutingInfo (**MSISDN**)

ProvideSubscriberInfo (**IMSI**)

ProvideSubscriberInfo (**Location = Home**)

SendRoutingInfo (**Location = Home**)

InitialDP (A-Num, **B-Num, Location**)

ApplyCharging, Continue

SendRoutingInfo (**MSISDN**)

ProvideRoaminNumber (**IMSI**)

ProvideRoamingNumber (**MSRN = 5312345678**)

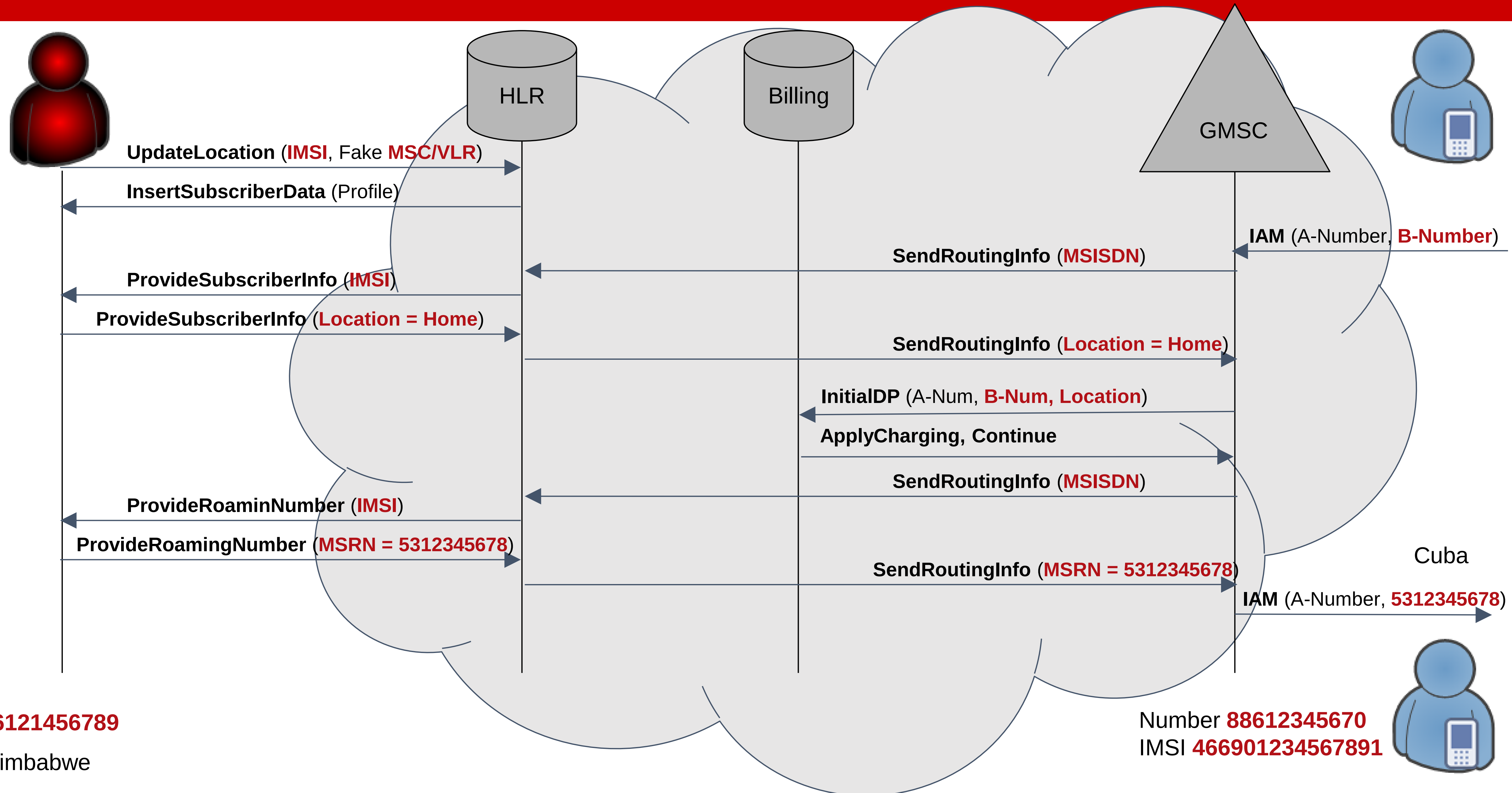
SendRoutingInfo (**MSRN = 5312345678**)

26121456789

Zimbabwe

Number **88612345670**
IMSI **466901234567891**

Voice call redirection with a fraudulent activity



HLR

Billing

GMSC

UpdateLocation (IMSI, Fake MSC/VLR)

InsertSubscriberData (Profile)

IAM (A-Number, B-Number)

SendRoutingInfo (MSISDN)

ProvideSubscriberInfo (IMSI)

ProvideSubscriberInfo (Location = Home)

SendRoutingInfo (Location = Home)

InitialDP (A-Num, B-Num, Location)

ApplyCharging, Continue

SendRoutingInfo (MSISDN)

ProvideRoaminNumber (IMSI)

ProvideRoamingNumber (MSRN = 5312345678)

SendRoutingInfo (MSRN = 5312345678)

IAM (A-Number, 5312345678)

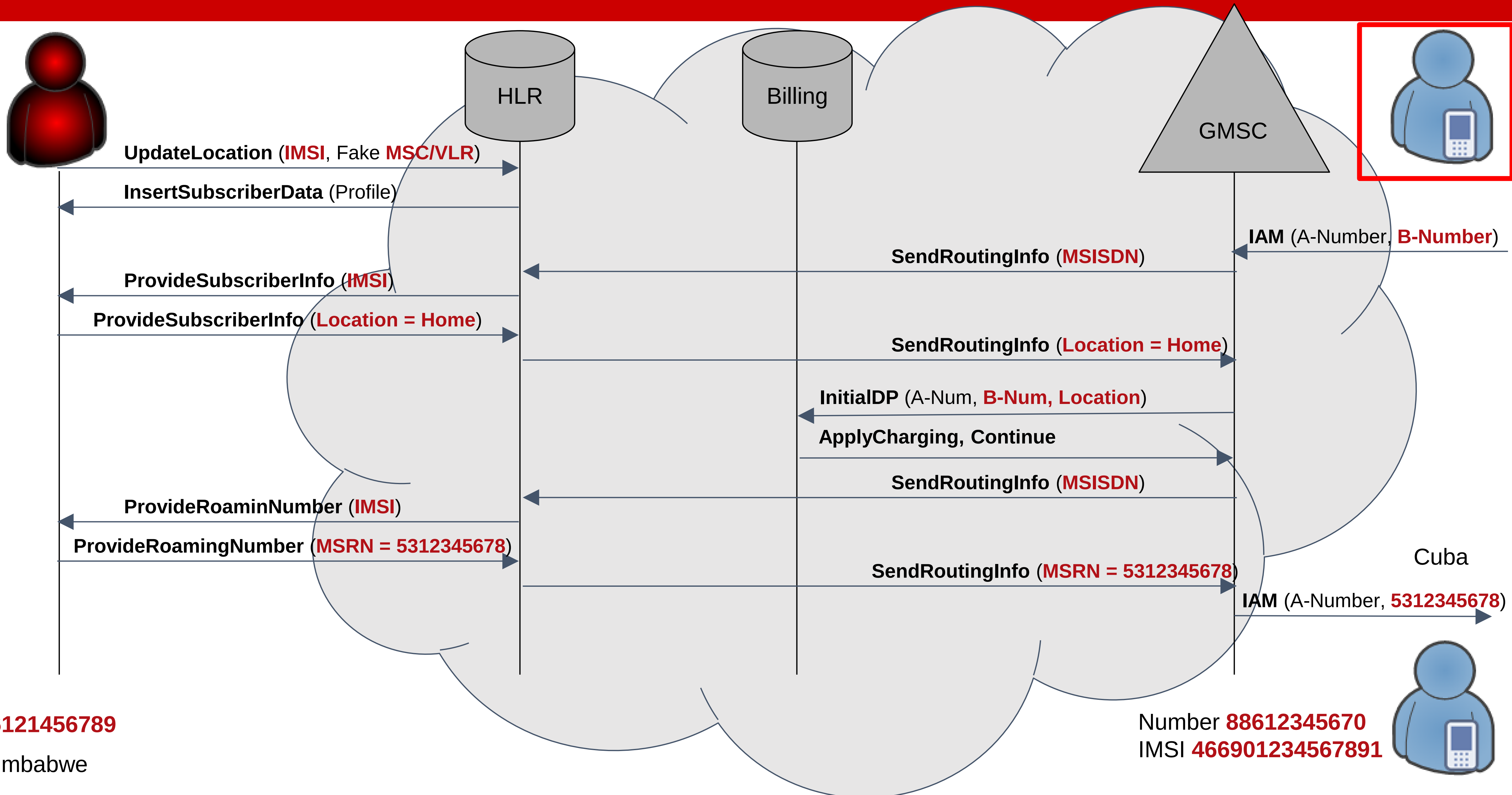
Cuba

26121456789

Zimbabwe

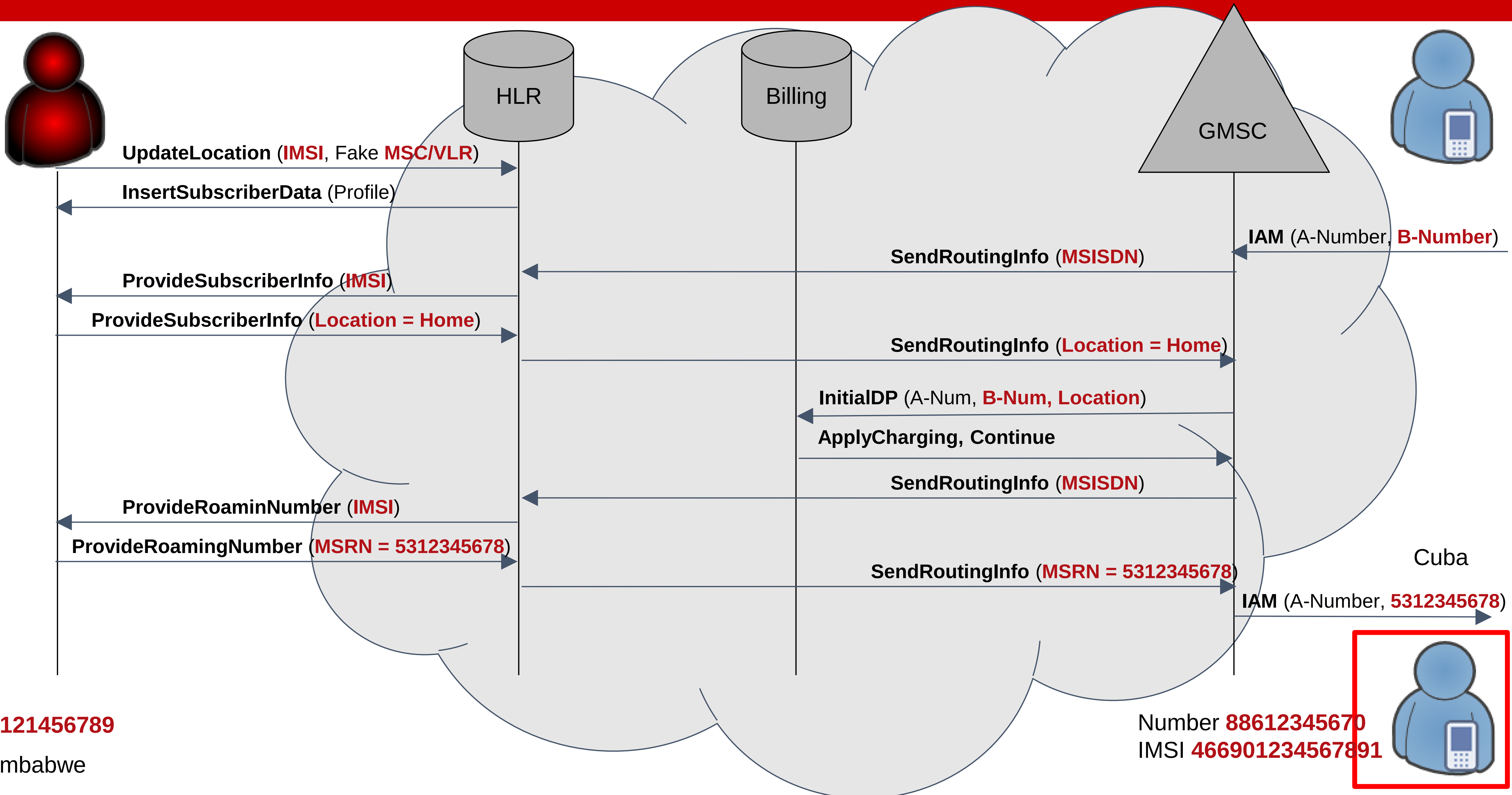
Number 88612345670
IMSI 466901234567891

Who pays?


HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
SendRoutingInfo (Location = Home)
InitialDP (A-Num, B-Num, Location)
ApplyCharging, Continue
SendRoutingInfo (MSISDN)
ProvideRoaminNumber (IMSI)
ProvideRoamingNumber (MSRN = 5312345678)
SendRoutingInfo (MSRN = 5312345678)
IAM (A-Number, 5312345678)
Cuba
26121456789
Zimbabwe
Number 88612345670
IMSI 466901234567891

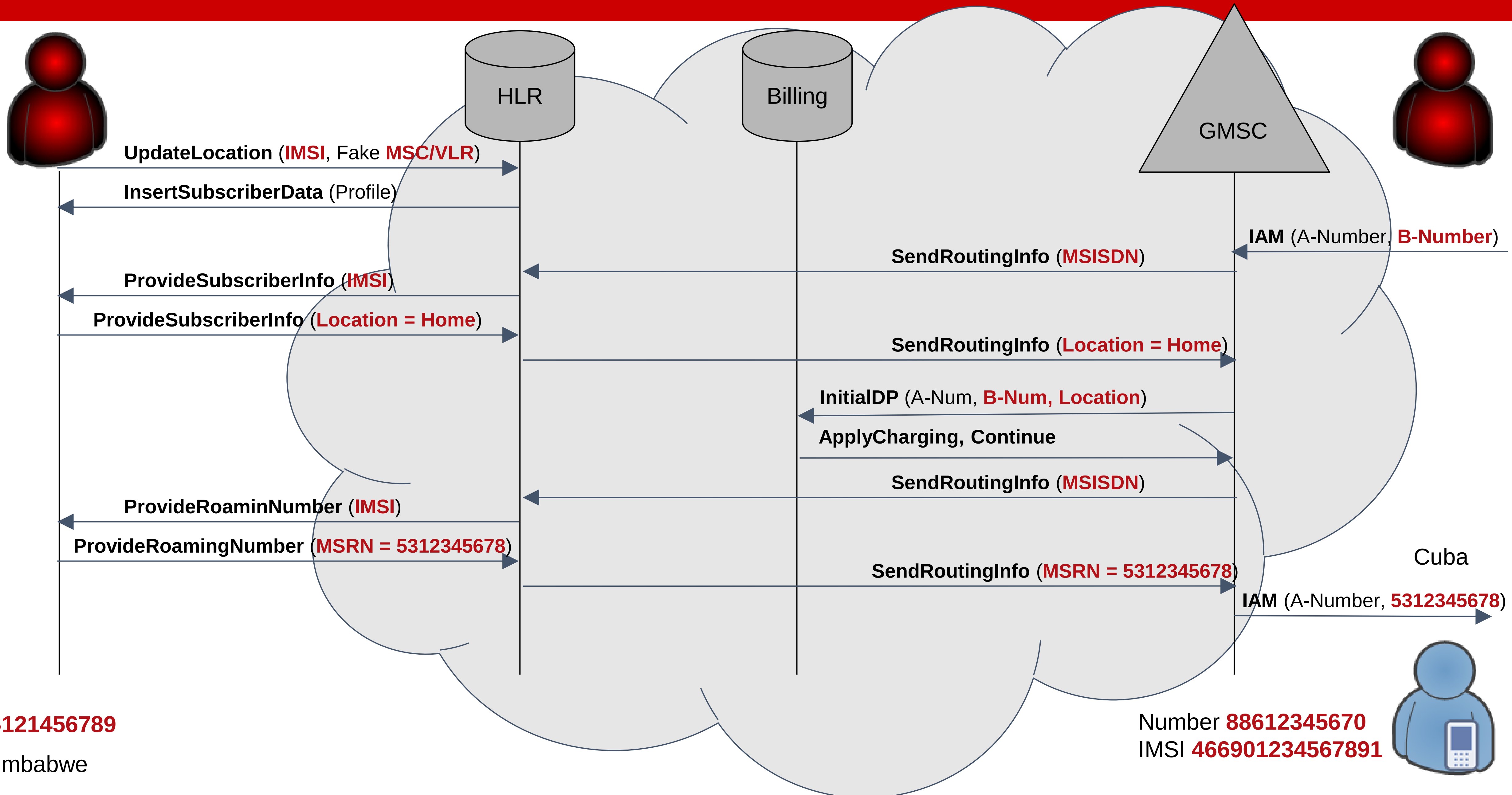
Who pays?

POSITIVE TECHNOLOGIES


HLR
Billing
GMSC
UpdateLocation (IMSI, Fake MSC/VLR)
InsertSubscriberData (Profile)
IAM (A-Number, B-Number)
SendRoutingInfo (MSISDN)
ProvideSubscriberInfo (IMSI)
ProvideSubscriberInfo (Location = Home)
SendRoutingInfo (Location = Home)
InitialDP (A-Num, B-Num, Location)
ApplyCharging, Continue
SendRoutingInfo (MSISDN)
ProvideRoaminNumber (IMSI)
ProvideRoamingNumber (MSRN = 5312345678)
SendRoutingInfo (MSRN = 5312345678)
IAM (A-Number, 5312345678)
Cuba
26121456789
Zimbabwe
Number 88612345670
IMSI 466901234567891

Who pays?

POSITIVE TECHNOLOGIES



HLR

Billing

GMSC

UpdateLocation (**IMSI**, Fake **MSC/VLR**)

InsertSubscriberData (Profile)

IAM (A-Number, **B-Number**)

SendRoutingInfo (**MSISDN**)

ProvideSubscriberInfo (**IMSI**)

ProvideSubscriberInfo (**Location = Home**)

SendRoutingInfo (**Location = Home**)

InitialDP (A-Num, **B-Num, Location**)

ApplyCharging, Continue

SendRoutingInfo (**MSISDN**)

ProvideRoaminNumber (**IMSI**)

ProvideRoamingNumber (**MSRN = 5312345678**)

SendRoutingInfo (**MSRN = 5312345678**)

Cuba

IAM (A-Number, **5312345678**)

26121456789

Zimbabwe

Number **88612345670**
IMSI **466901234567891**

Thank you!

POSITIVE TECHNOLOGIES

ptsecurity.com