Mobile Payment Application Security Tests

Arnold Kibuuka, Project Officer, ITU

07 December 2021

Outline

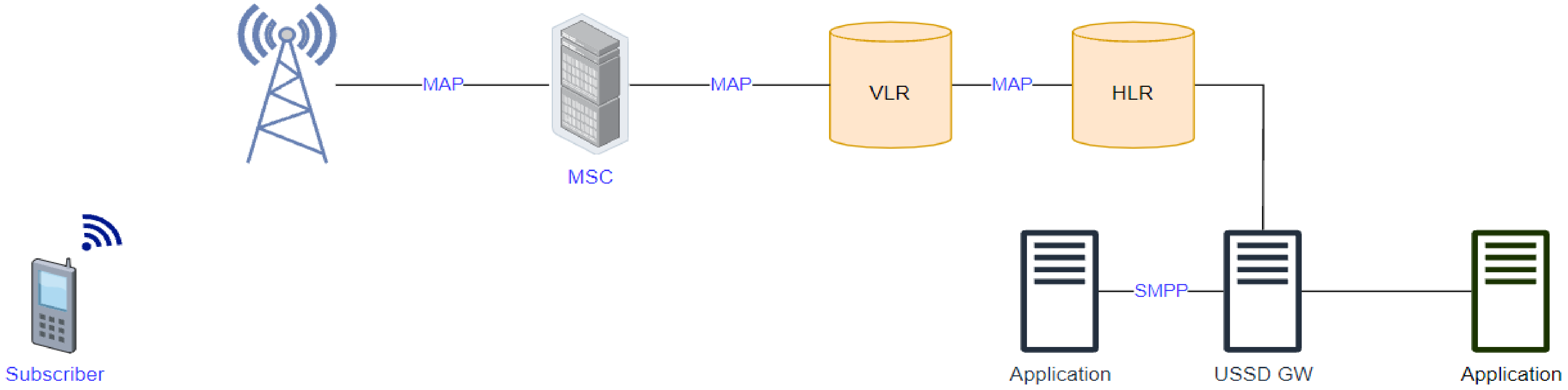
1. Introduction to USSD and STK
2. USSD & STK app tests
3. Recommendations

ITU FIGI resources

Introduction to USSD and STK

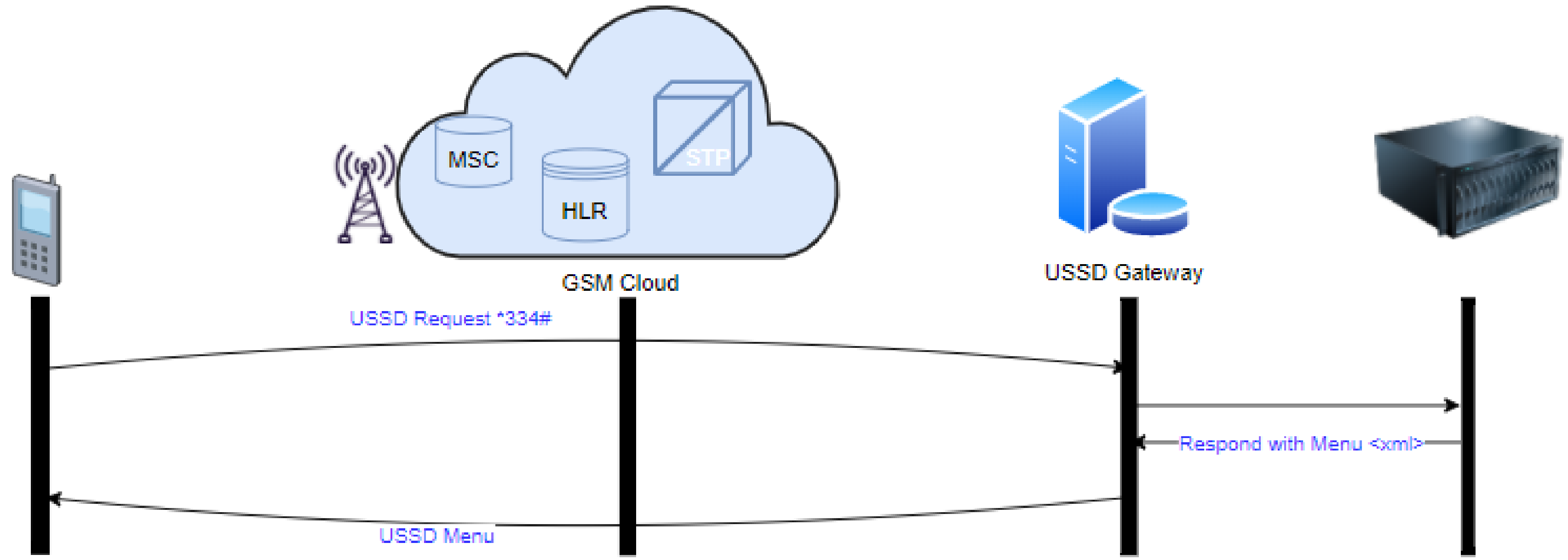
USSD

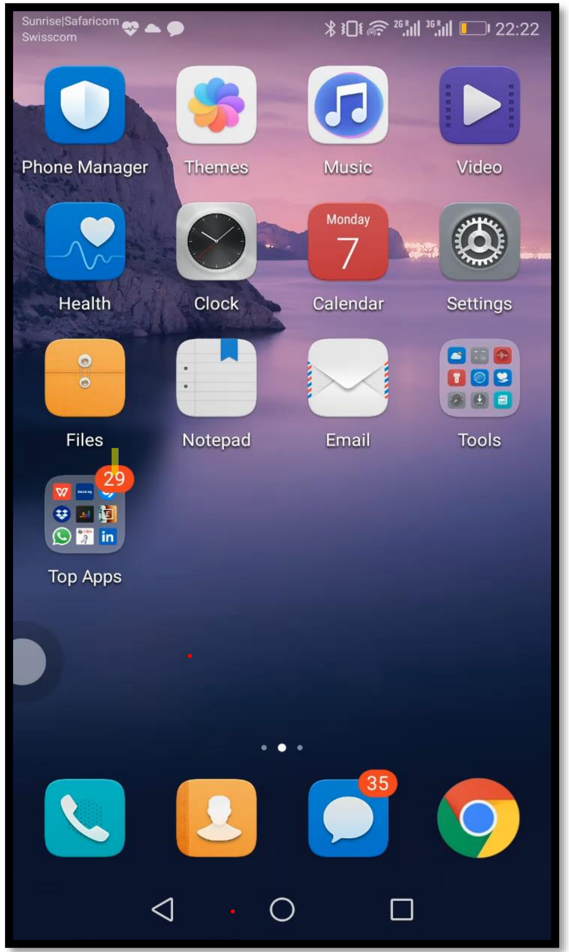
- **U**nstructured **S**upplementary **S**ervice **D**ata
- Most popular platform for mobile money services in developing countries & works on basic phones, feature phones and smartphones.
- Developed in 1994 and patented by Ericsson based on GSM specifications, further developed by Special Mobile Group (SMG) Technical Committee of ETSI and 3GPP

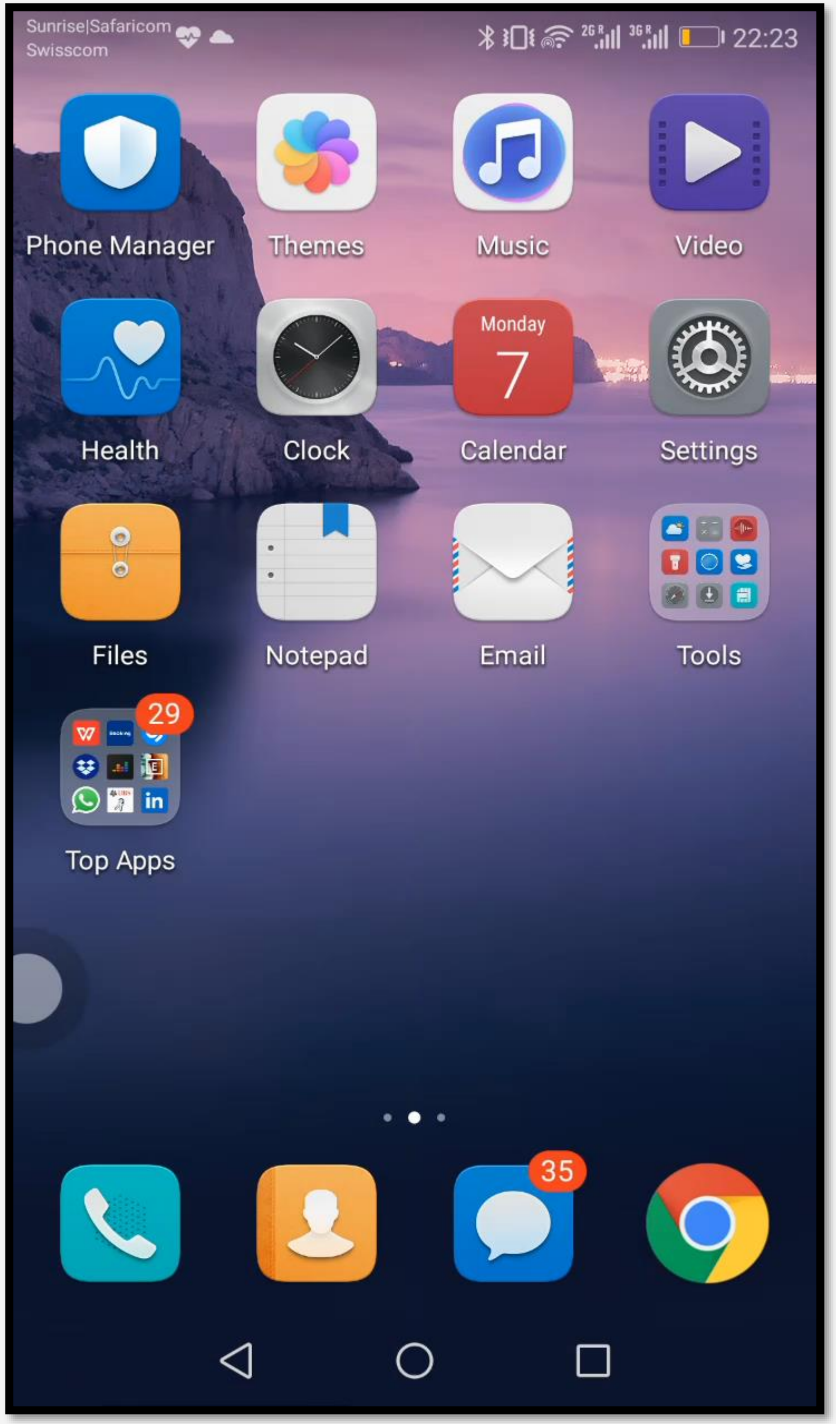


How USSD works

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cell phones to communicate with their service provider's servers. USSD can be used for prepaid call back, mobile money services, location based content services, menu based information services or even as part of phone registration and configuration on the network.







STK: SIM Application Toolkit

- SIM Application Toolkit or STK, is a set of commands which define how the SIM card should interact with the outside world and extends communication protocol to the card and the handset.
- STK has been deployed by many mobile operators for around the world for Value Added Services applications, often where a menu based approach is required, such as Mobile Banking and content browsing.
- Since 1998 almost all mobile phone produced have STK enabled.

Why USSD and STK are used for DFS.

a. Handset agnostic.

b. Session based hence interactive

  - *Offers real-time capabilities that enable speedy and responsive services.*

c. Quick deployment

  - *USSD does not require installation on device.*
  - *Uses existing network nodes & protocols.*

d. Convenience

  - *Agent distribution networks for Cash-In Cash-Out transactions are widespread.*

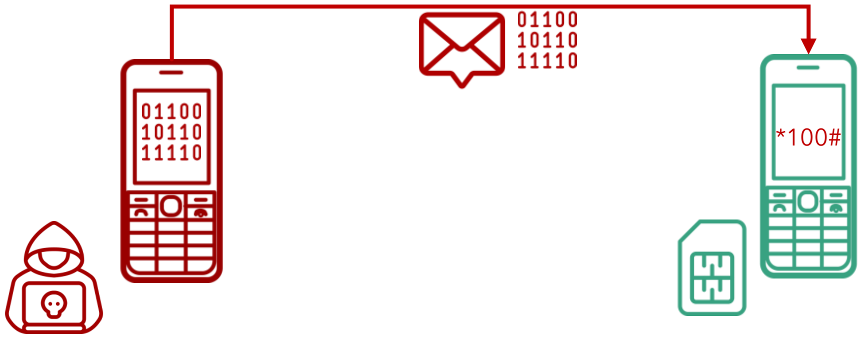
e. Cost effective

  - *No charge on USSD and STK messages (USSD mostly free when roaming).*

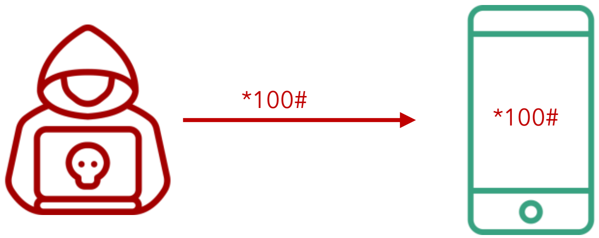
USSD and STK app Security Tests

USSD and STK App Security Tests

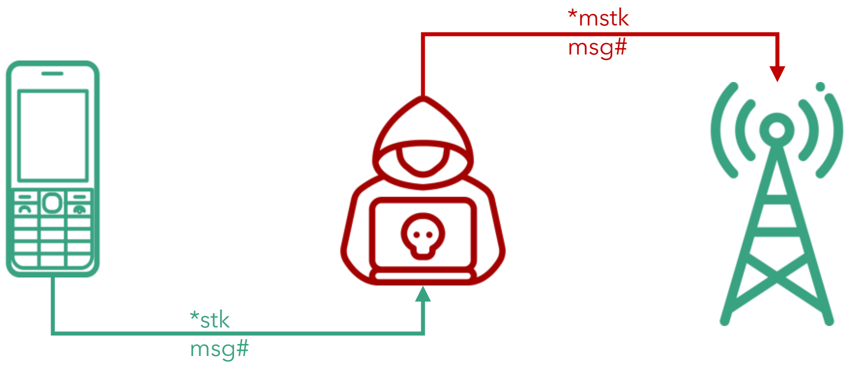
a. **SIM Swap** and **SIM cloning**



b. susceptibility to **binary OTA attacks** (SIM jacker, WIB attacks)



c. **remote USSD** execution attacks



d. **man-in-the-middle attacks** on STK based DFS applications

Hardware for security testing of USSD and STK based DFS

1. Laptop
2. Mobile Android smartphone, Samsung S4
3. Card reader
4. SIM card adapter
5. Mobile featurephone, Samsung 1200
6. Programmable/blank SIMs
7. SIMtrace microSIM & SIM (3FF) FPC Cab
8. SIMtrace2 Hardware Kit
9. Wi-Fi router - Synology RT2600AC

3

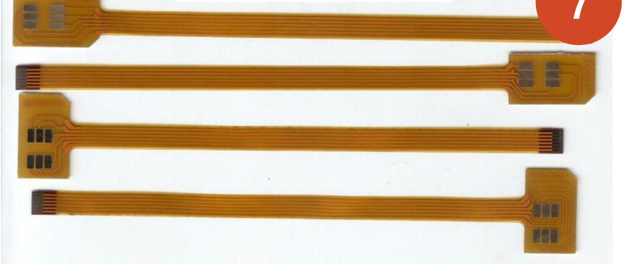
4

5

6

sysmocom
systems for mobile communications GmbH
custom-tailored GSM solutions from RAN to Core Network
Visit us at http://sysmocom.de/
• First-hand expertise in protocol R&D from A-bis to SS7/MAP
• Support, training and development for OpenBSC, OsmoSGSN
• Low-cost GSM pico-cell platform sysmoBTS
• Small, PBX-style autonomous GSM networks
sysmoSIM-SJS1-4FF

7



8

9

Software for USSD and STK based DFS security testing

i. pySIM: - SIM cloning

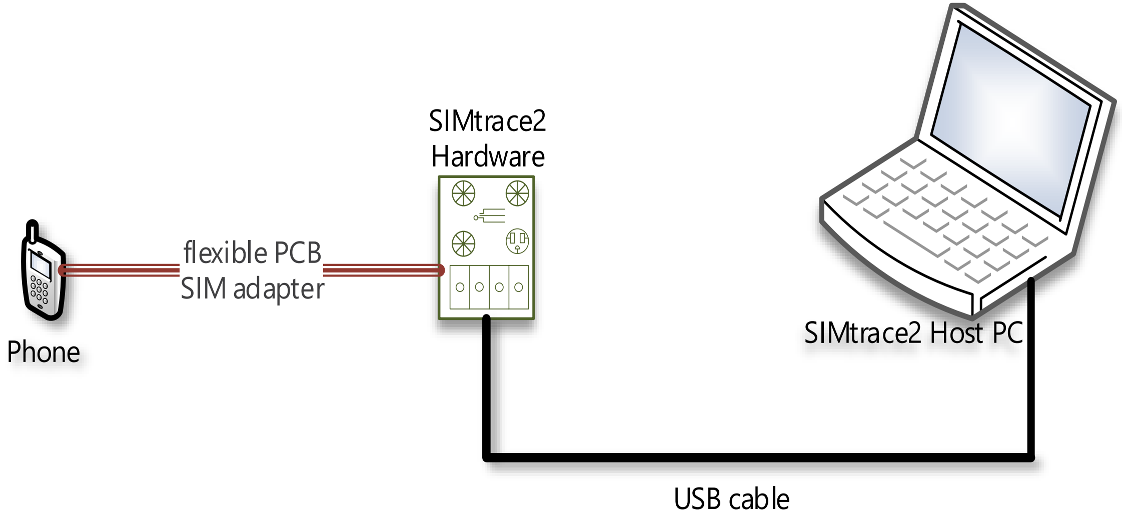
ii. SIMtrace: - Man-in-the-middle attacks

iii. SIM tester: - Binary OTA attacks

iv. ADB platform tools: - Remote USSD attack

v. Wireshark: - STK analysis

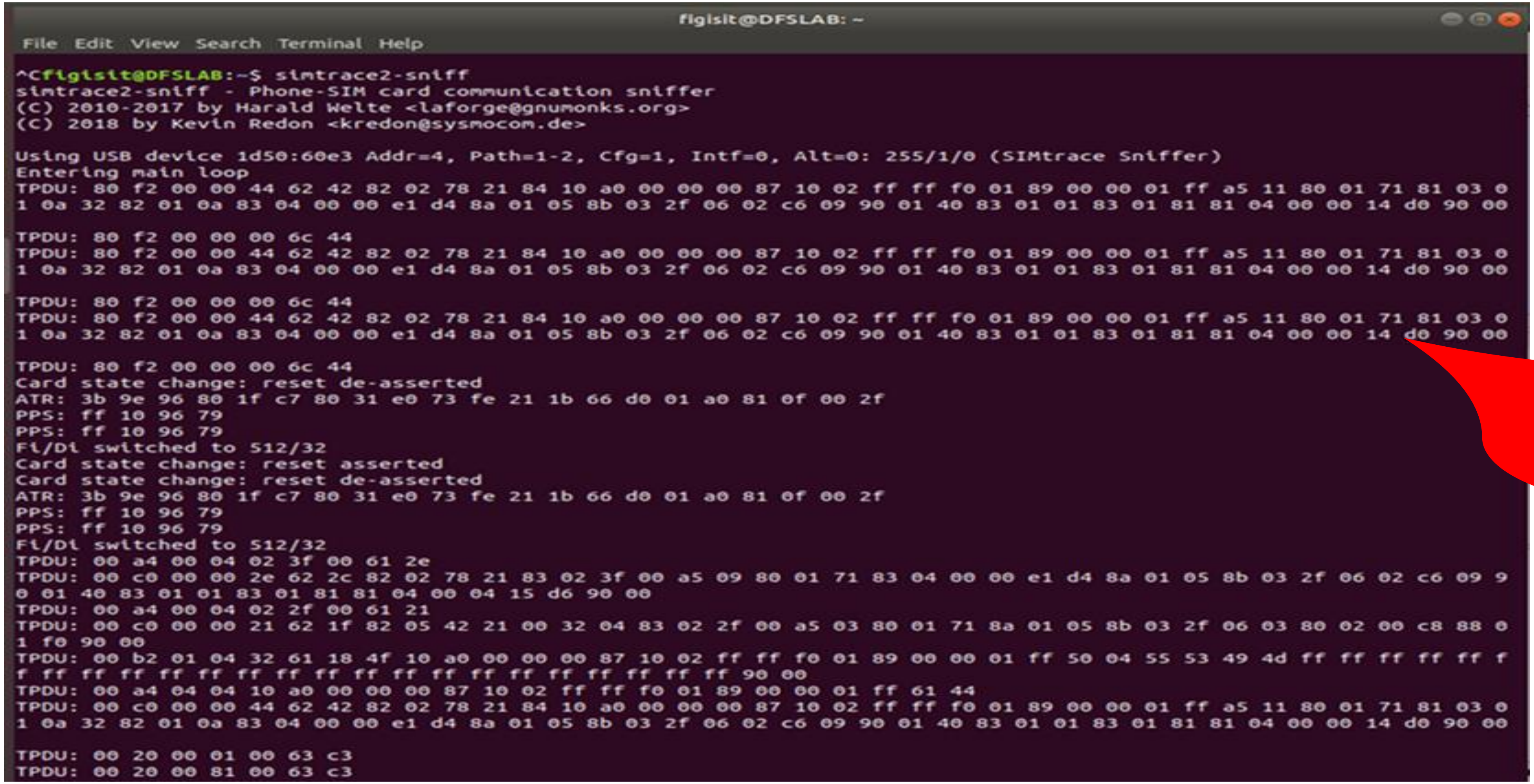
Man-in-the-Middle attacks on STK based DFS applications



MiTM attack simulation on STK using a SIMtrace

Testing Man-in-the-Middle interception using SIMtrace

Man-in-the-Middle attacks on STK based DFS applications

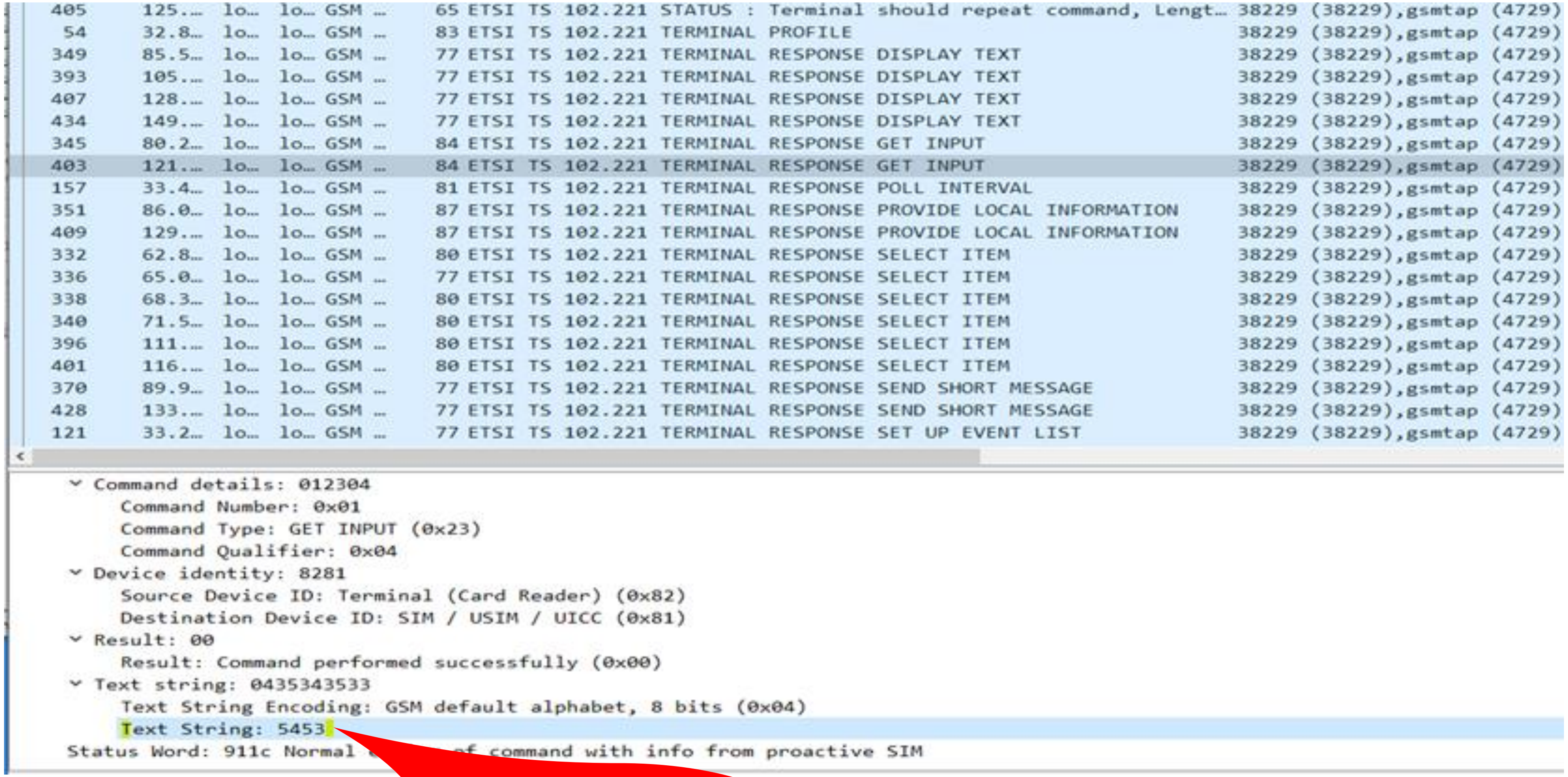


```
^Cfigisit@DFSLAB:~$ simtrace2-sniff
simtrace2-sniff - Phone-SIM card communication sniffer
(C) 2010-2017 by Harald Welte <laforge@gnumonks.org>
(C) 2018 by Kevin Redon <kredon@sysmocom.de>

Using USB device 1d50:60e3 Addr=4, Path=1-2, Cfg=1, Intf=0, Alt=0: 255/1/0 (SIMtrace Sniffer)
Entering main loop
TPDU: 80 f2 00 00 44 62 42 82 02 78 21 84 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff a5 11 80 01 71 81 03 0
1 0a 32 82 01 0a 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 90 01 40 83 01 01 83 01 81 81 04 00 00 14 d0 90 00

TPDU: 80 f2 00 00 00 6c 44
TPDU: 80 f2 00 00 44 62 42 82 02 78 21 84 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff a5 11 80 01 71 81 03 0
1 0a 32 82 01 0a 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 90 01 40 83 01 01 83 01 81 81 04 00 00 14 d0 90 00

TPDU: 80 f2 00 00 00 6c 44
TPDU: 80 f2 00 00 44 62 42 82 02 78 21 84 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff a5 11 80 01 71 81 03 0
1 0a 32 82 01 0a 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 90 01 40 83 01 01 83 01 81 81 04 00 00 14 d0 90 00

TPDU: 80 f2 00 00 00 6c 44
Card state change: reset de-asserted
ATR: 3b 9e 96 80 1f c7 80 31 e0 73 fe 21 1b 66 d0 01 a0 81 0f 00 2f
PPS: ff 10 96 79
PPS: ff 10 96 79
Fi/Di switched to 512/32
Card state change: reset asserted
Card state change: reset de-asserted
ATR: 3b 9e 96 80 1f c7 80 31 e0 73 fe 21 1b 66 d0 01 a0 81 0f 00 2f
PPS: ff 10 96 79
PPS: ff 10 96 79
Fi/Di switched to 512/32
TPDU: 00 a4 00 04 02 3f 00 61 2e
TPDU: 00 c0 00 00 2e 62 2c 82 02 78 21 83 02 3f 00 a5 09 80 01 71 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 9
0 01 40 83 01 01 83 01 81 81 04 00 04 15 d6 90 00
TPDU: 00 a4 00 04 02 2f 00 61 21
TPDU: 00 c0 00 00 21 62 1f 82 05 42 21 00 32 04 83 02 2f 00 a5 03 80 01 71 8a 01 05 8b 03 2f 06 03 80 02 00 c8 88 0
1 f0 90 00
TPDU: 00 b2 01 04 32 61 18 4f 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff 50 04 55 53 49 4d ff ff ff ff ff f
f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 90 00
TPDU: 00 a4 04 04 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff 61 44
TPDU: 00 c0 00 00 44 62 42 82 02 78 21 84 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff a5 11 80 01 71 81 03 0
1 0a 32 82 01 0a 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 90 01 40 83 01 01 83 01 81 81 04 00 00 14 d0 90 00

TPDU: 00 20 00 01 00 63 c3
TPDU: 00 20 00 81 00 63 c3
```

SIM trace sniff packet capturing

Trace packets captured by the SIMtrace device

Man-in-the-Middle attacks on STK based DFS applications



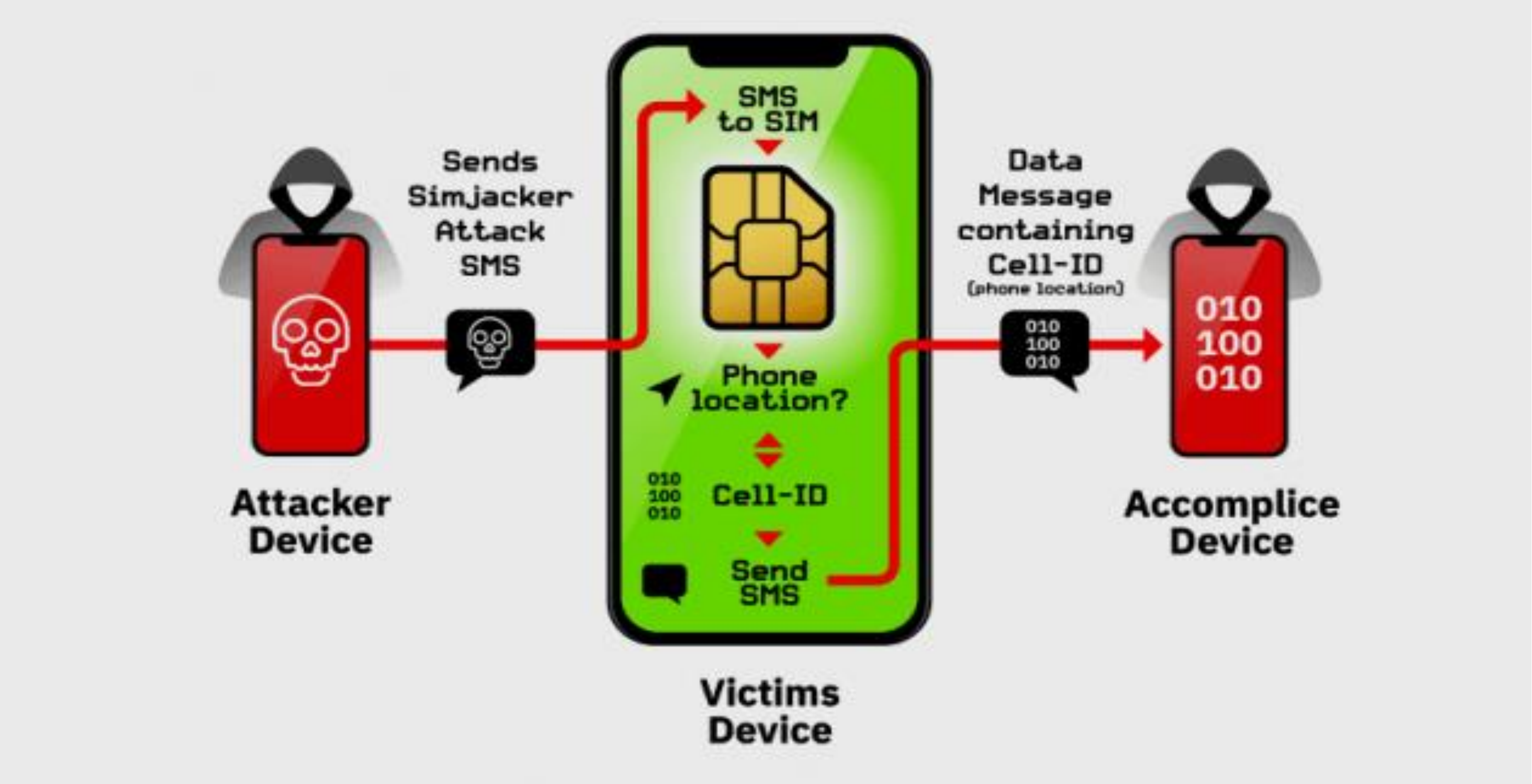
```
405   125.…  lo…  lo… GSM …   65 ETSI TS 102.221 STATUS : Terminal should repeat command, Lengt… 38229 (38229),gsmtap (4729)
 54    32.8…  lo…  lo… GSM …   83 ETSI TS 102.221 TERMINAL PROFILE                                38229 (38229),gsmtap (4729)
349    85.5…  lo…  lo… GSM …   77 ETSI TS 102.221 TERMINAL RESPONSE DISPLAY TEXT                  38229 (38229),gsmtap (4729)
393   105.…  lo…  lo… GSM …   77 ETSI TS 102.221 TERMINAL RESPONSE DISPLAY TEXT                  38229 (38229),gsmtap (4729)
407   128.…  lo…  lo… GSM …   77 ETSI TS 102.221 TERMINAL RESPONSE DISPLAY TEXT                  38229 (38229),gsmtap (4729)
434   149.…  lo…  lo… GSM …   77 ETSI TS 102.221 TERMINAL RESPONSE DISPLAY TEXT                  38229 (38229),gsmtap (4729)
345    80.2…  lo…  lo… GSM …   84 ETSI TS 102.221 TERMINAL RESPONSE GET INPUT                     38229 (38229),gsmtap (4729)
403   121.…  lo…  lo… GSM …   84 ETSI TS 102.221 TERMINAL RESPONSE GET INPUT                     38229 (38229),gsmtap (4729)
157    33.4…  lo…  lo… GSM …   81 ETSI TS 102.221 TERMINAL RESPONSE POLL INTERVAL                 38229 (38229),gsmtap (4729)
351    86.0…  lo…  lo… GSM …   87 ETSI TS 102.221 TERMINAL RESPONSE PROVIDE LOCAL INFORMATION     38229 (38229),gsmtap (4729)
409   129.…  lo…  lo… GSM …   87 ETSI TS 102.221 TERMINAL RESPONSE PROVIDE LOCAL INFORMATION     38229 (38229),gsmtap (4729)
332    62.8…  lo…  lo… GSM …   80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                   38229 (38229),gsmtap (4729)
336    65.0…  lo…  lo… GSM …   77 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                   38229 (38229),gsmtap (4729)
338    68.3…  lo…  lo… GSM …   80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                   38229 (38229),gsmtap (4729)
340    71.5…  lo…  lo… GSM …   80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                   38229 (38229),gsmtap (4729)
396   111.…  lo…  lo… GSM …   80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                   38229 (38229),gsmtap (4729)
401   116.…  lo…  lo… GSM …   80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                   38229 (38229),gsmtap (4729)
370    89.9…  lo…  lo… GSM …   77 ETSI TS 102.221 TERMINAL RESPONSE SEND SHORT MESSAGE            38229 (38229),gsmtap (4729)
428   133.…  lo…  lo… GSM …   77 ETSI TS 102.221 TERMINAL RESPONSE SEND SHORT MESSAGE            38229 (38229),gsmtap (4729)
121    33.2…  lo…  lo… GSM …   77 ETSI TS 102.221 TERMINAL RESPONSE SET UP EVENT LIST             38229 (38229),gsmtap (4729)

  Command details: 012304
      Command Number: 0x01
      Command Type: GET INPUT (0x23)
      Command Qualifier: 0x04
  Device identity: 8281
      Source Device ID: Terminal (Card Reader) (0x82)
      Destination Device ID: SIM / USIM / UICC (0x81)
  Result: 00
      Result: Command performed successfully (0x00)
  Text string: 0435343533
      Text String Encoding: GSM default alphabet, 8 bits (0x04)
      Text String: 5453
Status Word: 911c Normal e          f command with info from proactive SIM
```

DFS PIN from captured data

Thin SIM

Analysis of trace packets from SIMtrace device

Testing susceptibility to binary OTA attacks (SIMjacker, WIB attacks)



Source: Adaptive Mobile

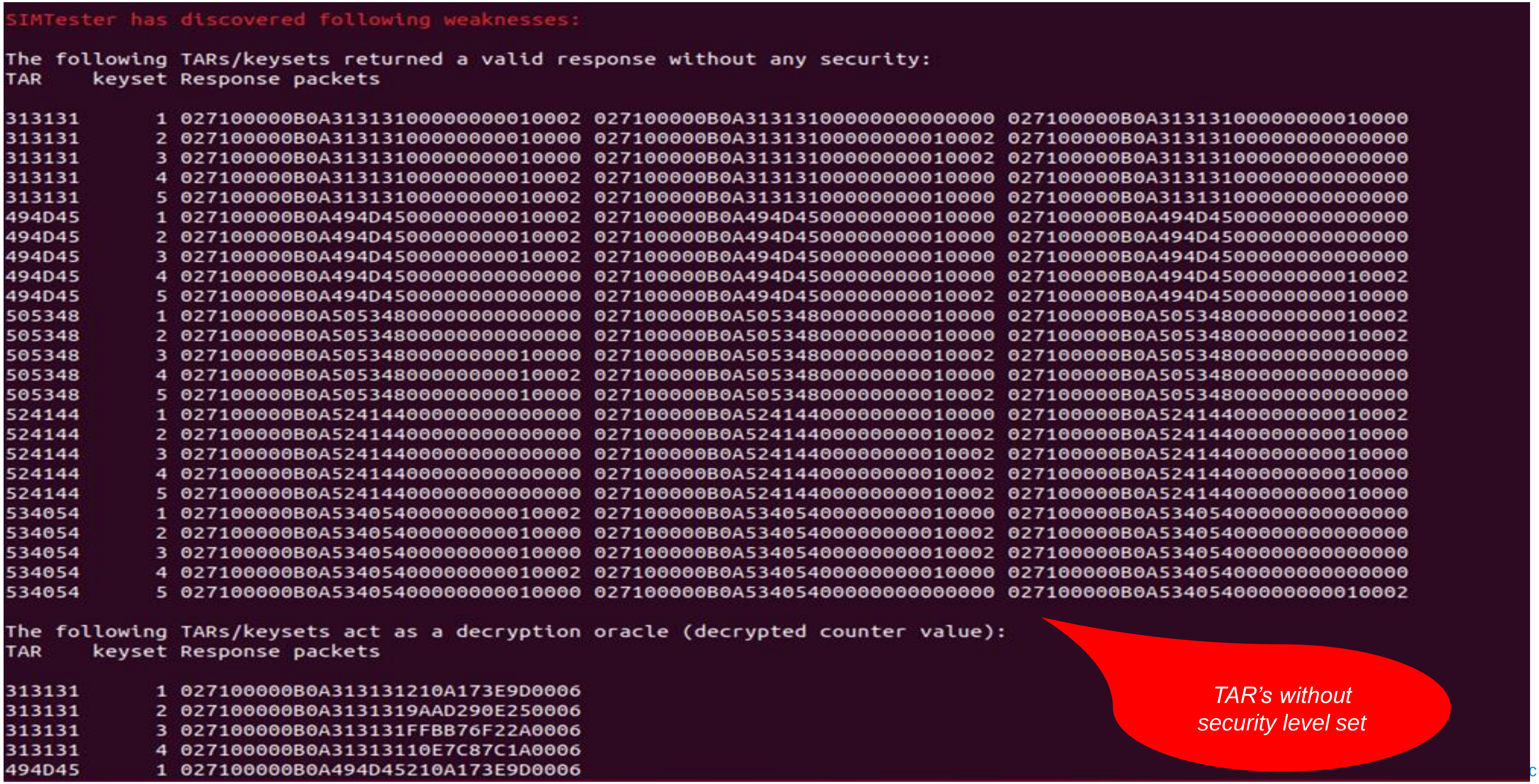
A binary OTA message can instruct the SIM to:

- initiate SS,
- Send SMS
- Initiate a phone call

on a vulnerable SIM and will affect both USSD and STK apps.

(see CVE-2019-16256)

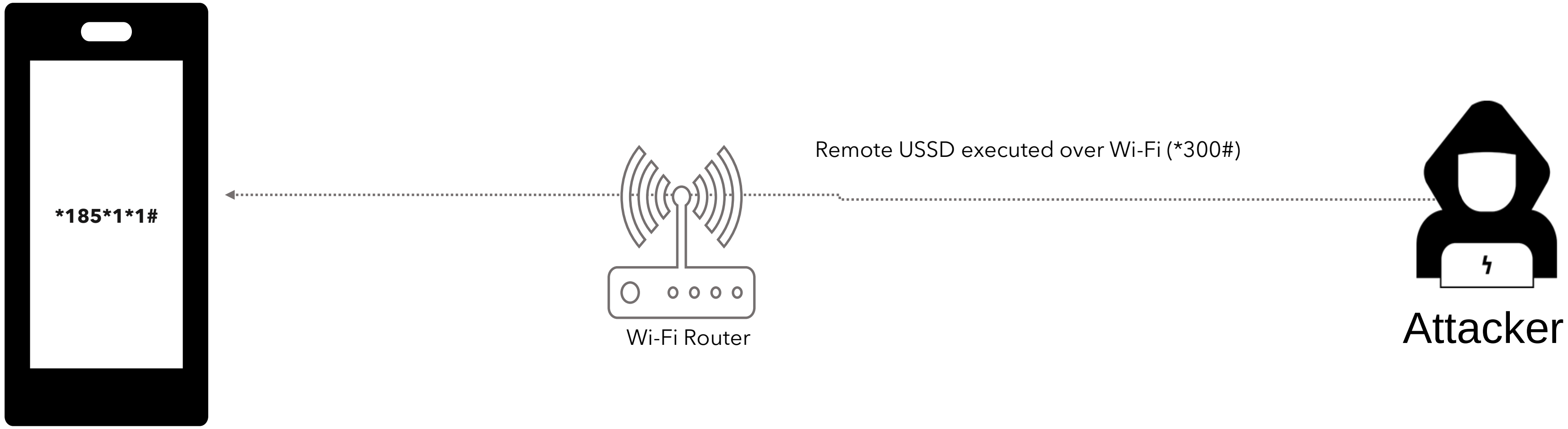
Testing susceptibility to binary OTA attacks (SIMjacker, WIB attacks)



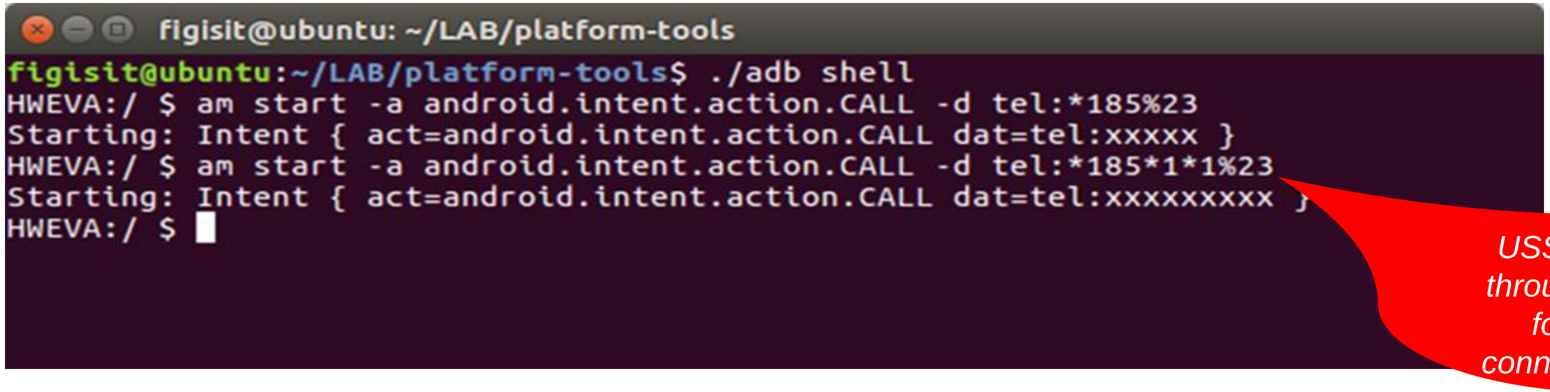
```
SIMTester has discovered following weaknesses:

The following TARs/keysets returned a valid response without any security:
TAR    keyset Response packets

313131      1 027100000B0A3131310000000000010002 027100000B0A3131310000000000000000 027100000B0A3131310000000000010000
313131      2 027100000B0A3131310000000000010000 027100000B0A3131310000000000010002 027100000B0A3131310000000000000000
313131      3 027100000B0A3131310000000000010000 027100000B0A3131310000000000010002 027100000B0A3131310000000000000000
313131      4 027100000B0A3131310000000000010002 027100000B0A3131310000000000010000 027100000B0A3131310000000000000000
313131      5 027100000B0A3131310000000000010002 027100000B0A3131310000000000010000 027100000B0A3131310000000000000000
494D45      1 027100000B0A494D450000000000010002 027100000B0A494D450000000000010000 027100000B0A494D450000000000000000
494D45      2 027100000B0A494D450000000000010002 027100000B0A494D450000000000010000 027100000B0A494D450000000000000000
494D45      3 027100000B0A494D450000000000010002 027100000B0A494D450000000000010000 027100000B0A494D450000000000000000
494D45      4 027100000B0A494D450000000000000000 027100000B0A494D450000000000010000 027100000B0A494D450000000000010002
494D45      5 027100000B0A494D450000000000000000 027100000B0A494D450000000000010002 027100000B0A494D450000000000010000
505348      1 027100000B0A5053480000000000000000 027100000B0A5053480000000000010000 027100000B0A5053480000000000010002
505348      2 027100000B0A5053480000000000000000 027100000B0A5053480000000000010000 027100000B0A5053480000000000010002
505348      3 027100000B0A5053480000000000010000 027100000B0A5053480000000000010002 027100000B0A5053480000000000000000
505348      4 027100000B0A5053480000000000010002 027100000B0A5053480000000000010000 027100000B0A5053480000000000000000
505348      5 027100000B0A5053480000000000010000 027100000B0A5053480000000000010002 027100000B0A5053480000000000000000
524144      1 027100000B0A5241440000000000000000 027100000B0A5241440000000000010000 027100000B0A5241440000000000010002
524144      2 027100000B0A5241440000000000000000 027100000B0A5241440000000000010002 027100000B0A5241440000000000010000
524144      3 027100000B0A5241440000000000000000 027100000B0A5241440000000000010002 027100000B0A5241440000000000010000
524144      4 027100000B0A5241440000000000000000 027100000B0A5241440000000000010002 027100000B0A5241440000000000010000
524144      5 027100000B0A5241440000000000000000 027100000B0A5241440000000000010002 027100000B0A5241440000000000010000
534054      1 027100000B0A5340540000000000010002 027100000B0A5340540000000000010000 027100000B0A5340540000000000000000
534054      2 027100000B0A5340540000000000010000 027100000B0A5340540000000000010002 027100000B0A5340540000000000000000
534054      3 027100000B0A5340540000000000010000 027100000B0A5340540000000000010002 027100000B0A5340540000000000000000
534054      4 027100000B0A5340540000000000010002 027100000B0A5340540000000000010000 027100000B0A5340540000000000000000
534054      5 027100000B0A5340540000000000010000 027100000B0A5340540000000000000000 027100000B0A5340540000000000010002

The following TARs/keysets act as a decryption oracle (decrypted counter value):
TAR    keyset Response packets

313131      1 027100000B0A313131210A173E9D0006
313131      2 027100000B0A3131319AAD290E250006
313131      3 027100000B0A313131FFBB76F22A0006
313131      4 027100000B0A31313110E7C87C1A0006
494D45      1 027100000B0A494D45210A173E9D0006
```

TAR’s without security level set

Testing remote USSD execution attacks



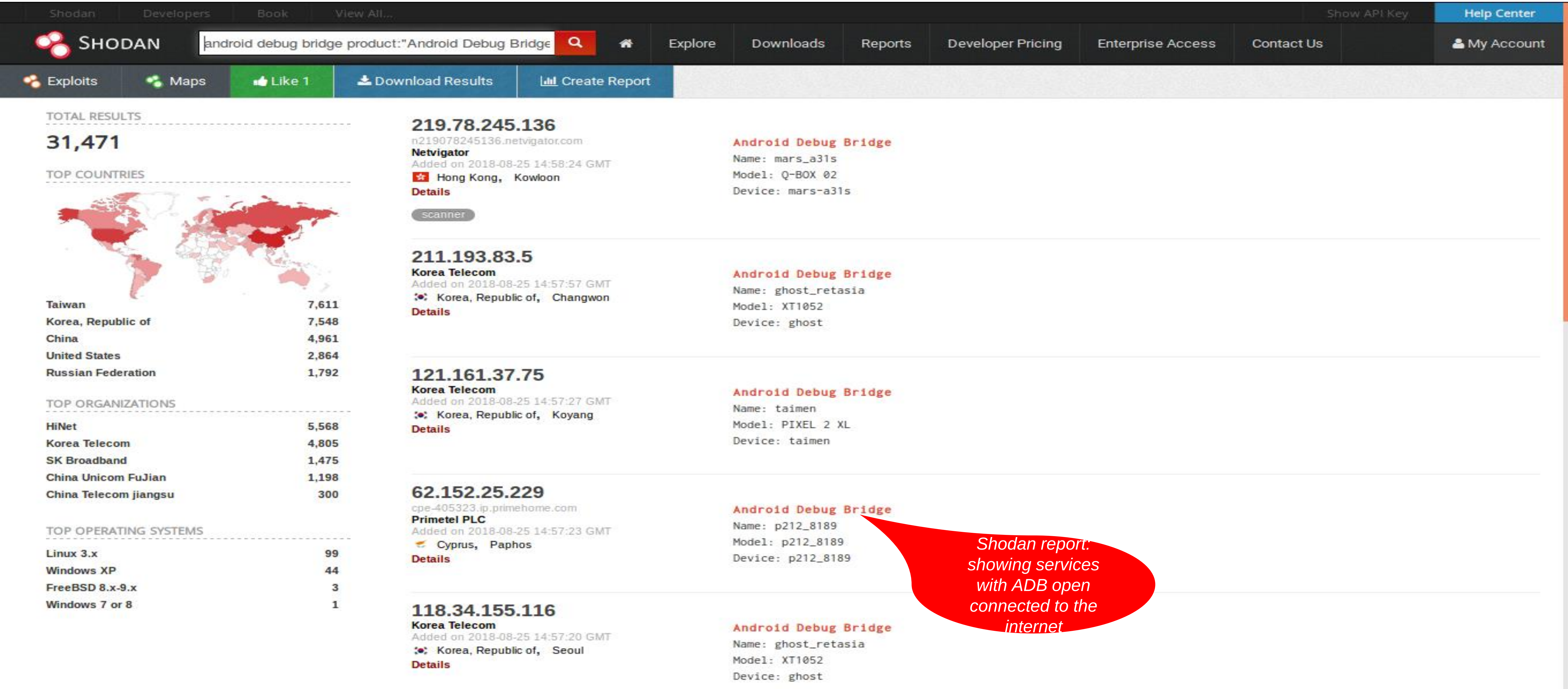
Setup for testing USSD remote attacks through open ADB ports



```
figisit@ubuntu:~/LAB/platform-tools$ ./adb shell
HWEVA:/ $ am start -a android.intent.action.CALL -d tel:*185%23
Starting: Intent { act=android.intent.action.CALL dat=tel:xxxxx }
HWEVA:/ $ am start -a android.intent.action.CALL -d tel:*185*1*1%23
Starting: Intent { act=android.intent.action.CALL dat=tel:xxxxxxxxx }
HWEVA:/ $ 
```

USSD execution through a terminal for a device connected to Wi-Fi

Testing remote USSD execution attacks



TOTAL RESULTS

31,471

TOP COUNTRIES

Taiwan	7,611
Korea, Republic of	7,548
China	4,961
United States	2,864
Russian Federation	1,792

TOP ORGANIZATIONS

HiNet	5,568
Korea Telecom	4,805
SK Broadband	1,475
China Unicom FuJian	1,198
China Telecom jiangsu	300

TOP OPERATING SYSTEMS

Linux 3.x	99
Windows XP	44
FreeBSD 8.x-9.x	3
Windows 7 or 8	1

219.78.245.136
n219078245136.netvigator.com
Netvigator
Added on 2018-08-25 14:58:24 GMT
Hong Kong, Kowloon
Details
scanner

```
Android Debug Bridge
Name: mars_a31s
Model: Q-BOX 02
Device: mars-a31s
```

211.193.83.5
Korea Telecom
Added on 2018-08-25 14:57:57 GMT
Korea, Republic of, Changwon
Details

```
Android Debug Bridge
Name: ghost_retasia
Model: XT1052
Device: ghost
```

121.161.37.75
Korea Telecom
Added on 2018-08-25 14:57:27 GMT
Korea, Republic of, Koyang
Details

```
Android Debug Bridge
Name: taimen
Model: PIXEL 2 XL
Device: taimen
```

62.152.25.229
cpe-405323.ip.primehome.com
Primetel PLC
Added on 2018-08-25 14:57:23 GMT
Cyprus, Paphos
Details

```
Android Debug Bridge
Name: p212_8189
Model: p212_8189
Device: p212_8189
```

118.34.155.116
Korea Telecom
Added on 2018-08-25 14:57:20 GMT
Korea, Republic of, Seoul
Details

```
Android Debug Bridge
Name: ghost_retasia
Model: XT1052
Device: ghost
```

Shodan report: showing services with ADB open connected to the internet

adb can also be used to attack services on IoT devices

Recommendations

Remote USSD execution on devices

- Disable ADB
- User education
- Discourage use rooted devices

SIM exploitation using binary OTA

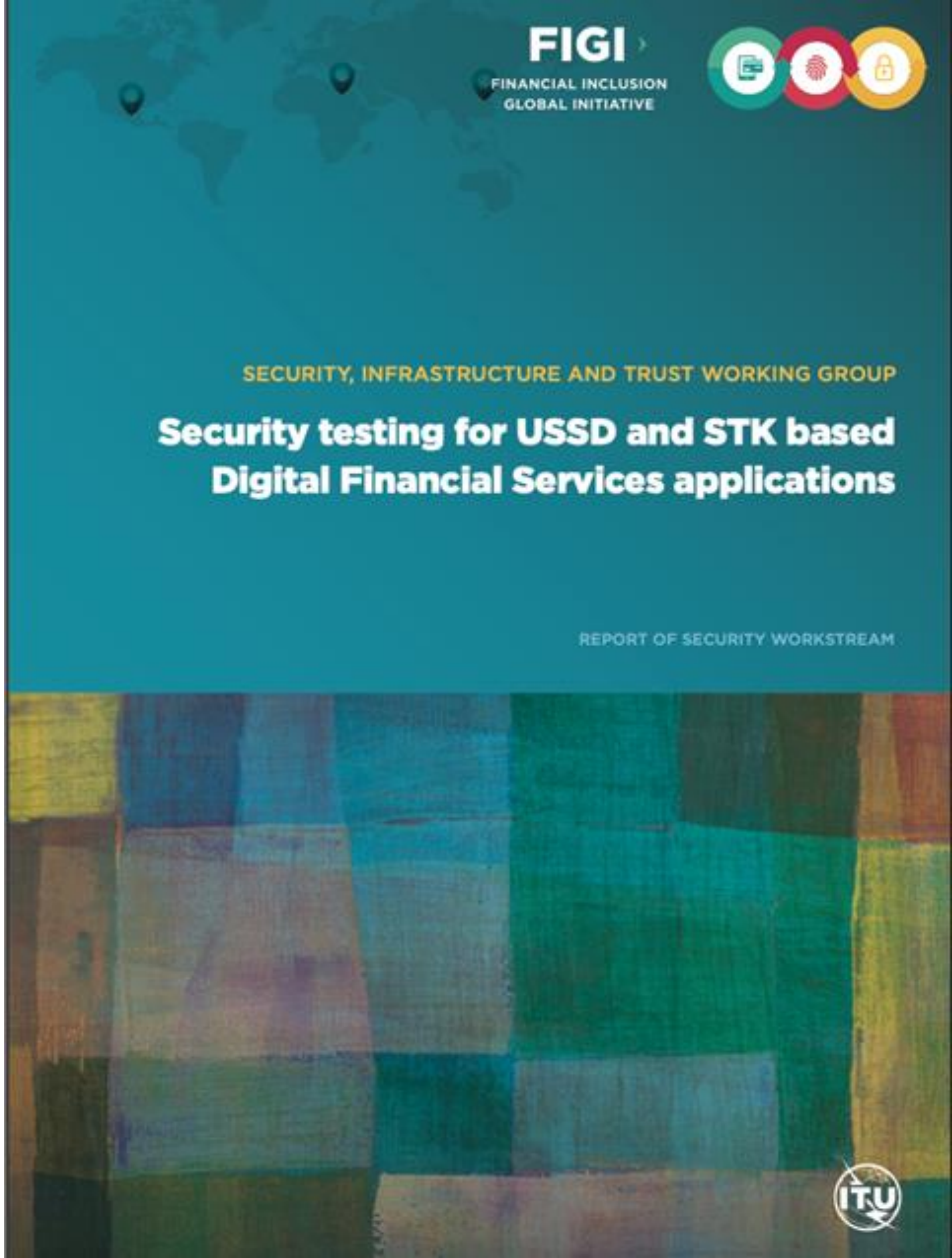
- Binary OTA SMS filtering & blocking.
- SMS home routing.
- SIM card security

Man-in-the-Middle attacks

- Use session timeout
- Secure radio channel communication
- SS7 controls and mitigations

SIM swap and SIM clone attacks

- SIM change detection. (ICCID, IMEI)
- Secure storage of SIM data like IMSI and secret key (KI values)



FIGI

FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security testing for USSD and STK based Digital Financial Services applications

REPORT OF SECURITY WORKSTREAM

What we need to test your DFS app

USSD and STK tests

- 2 SIM cards for the MNO networks to be tested.
- Active DFS account on each SIM

Android app testing

- 2 accounts used for the Android app.
- apps from the Play Store/APK file

Get in touch

dfssecuritylab@itu.int

https://figi.itu.int/figi-resources/dfs-security-lab/

ITU

www.itu.int