

Mobile Payment Application Security Tests


Arnold Kibuuka, Project Officer, ITU

23 October 2021




Outline

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



ITU FIGI resources

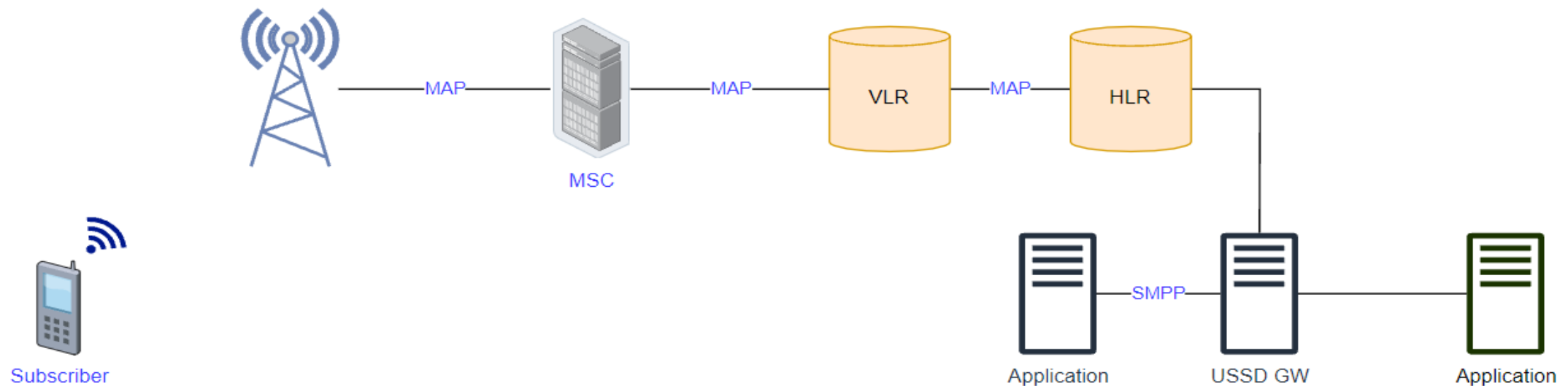


A blue rectangular box containing a white lightbulb icon in the top left corner, the text "ITU FIGI resources" in white, and a large QR code in the center. The QR code has a small blue dinosaur silhouette in the middle of it.

Introduction to USSD and STK

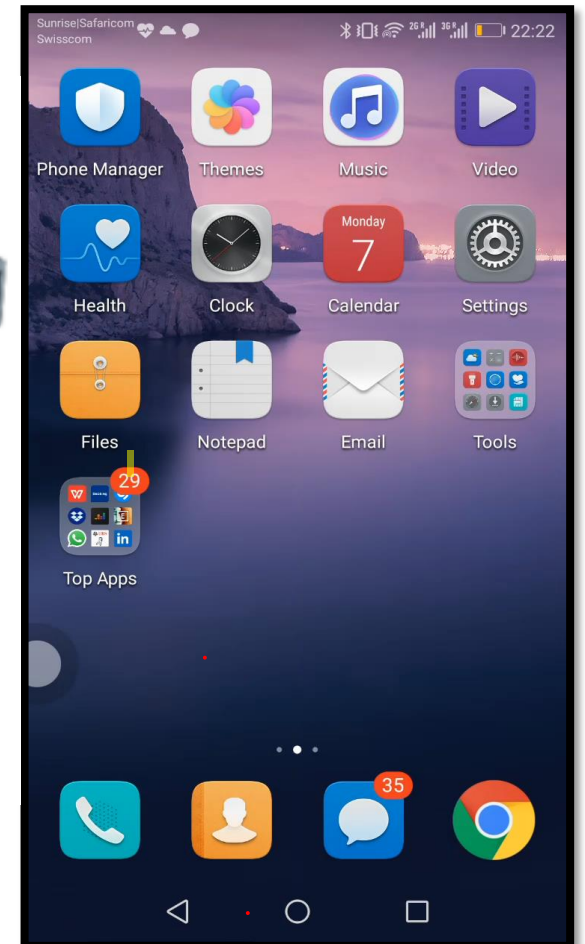
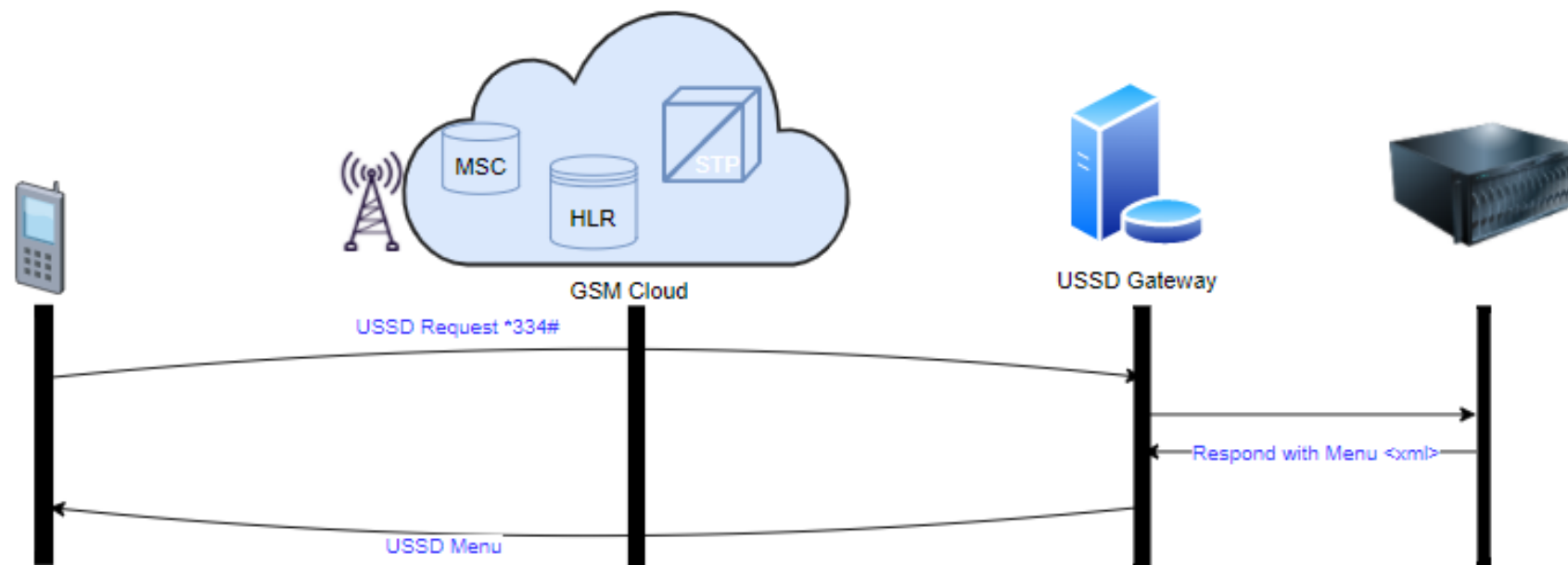
USSD

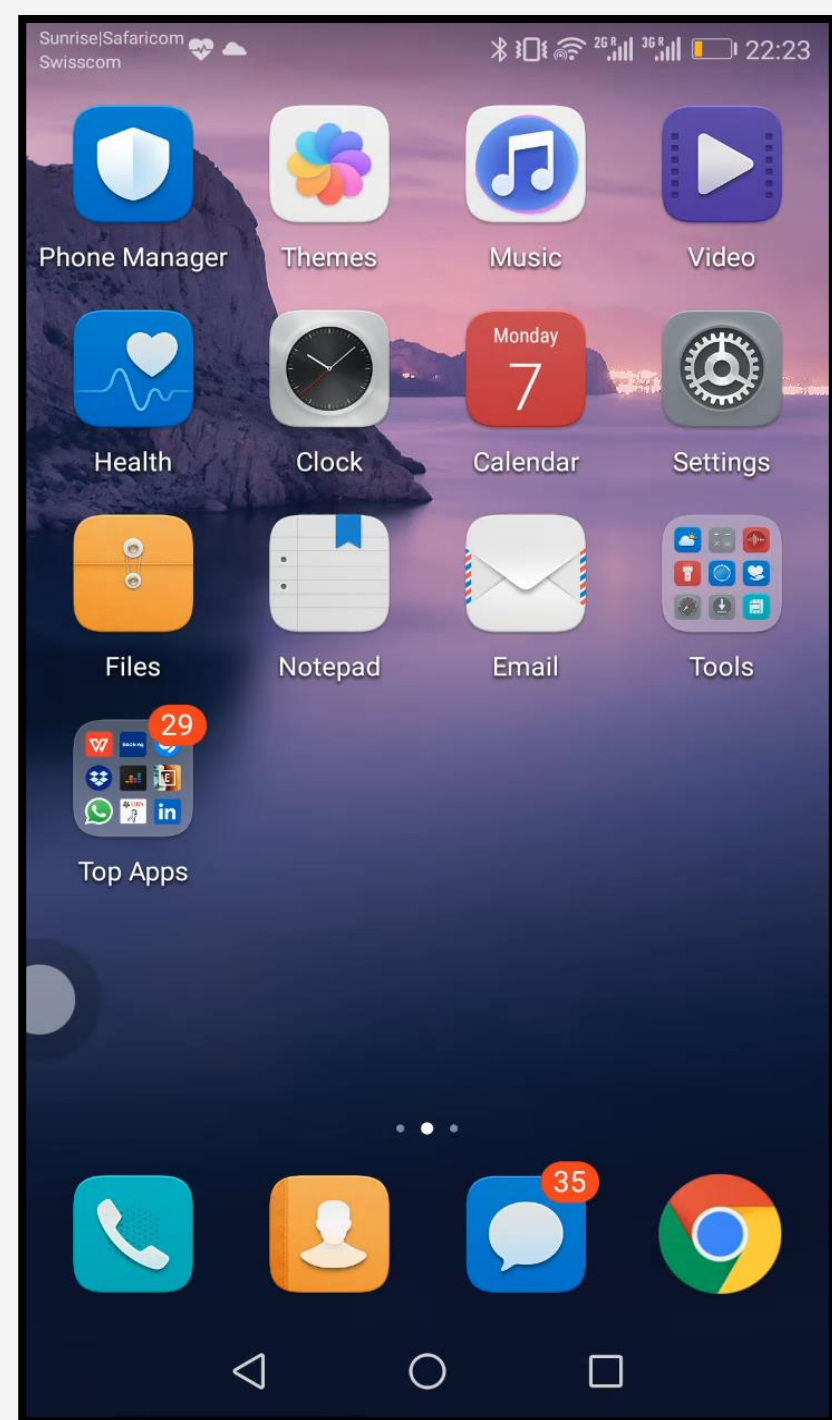
- **U**nstructured **S**upplementary **S**ervice **D**ata
- Most popular platform for mobile money services in developing countries & works on basic phones, feature phones and smartphones.
- Developed in 1994 and patented by Ericsson based on GSM specifications, further developed by Special Mobile Group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

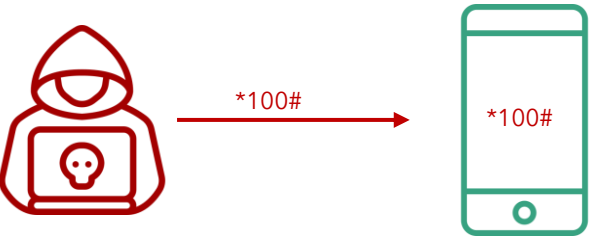
USSD and STK App Security Tests



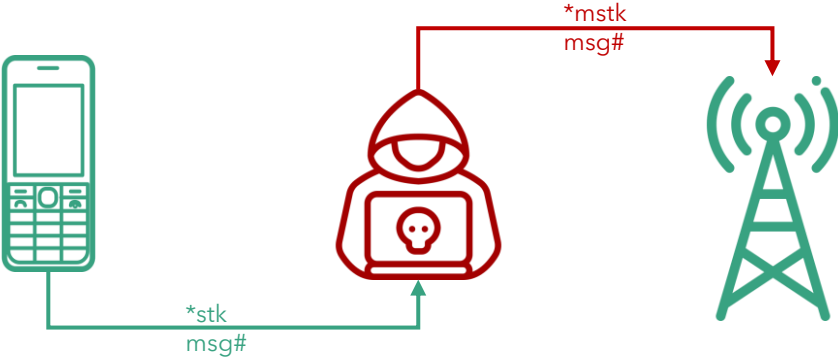
a. **SIM Swap** and **SIM cloning**



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



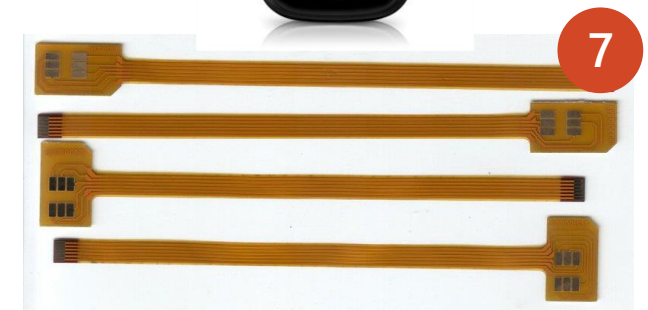
c. **remote USSD** execution attacks



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

Hardware for security testing of USSD and STK based DFS

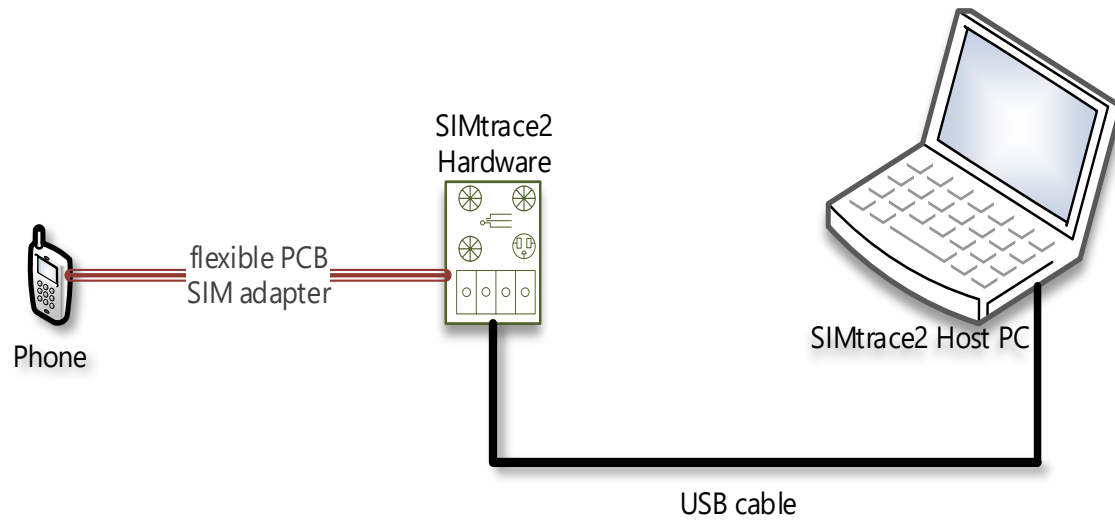
1. Laptop
2. Mobile Android smartphone, Samsung S4
3. Card reader
4. SIM card adapter
5. Mobile featurephone, Samsung 1200
6. Programmable/blank SIMs
7. SIMtrace microSIM & SIM (3FF) FPC Cab
8. SIMtrace2 Hardware Kit
9. Wi-Fi router - Synology RT2600AC



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

```

405 125.... lo... lo... GSM ... 65 ETSI TS 102.221 STATUS : Terminal should repeat command, Leng... 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)

```

```

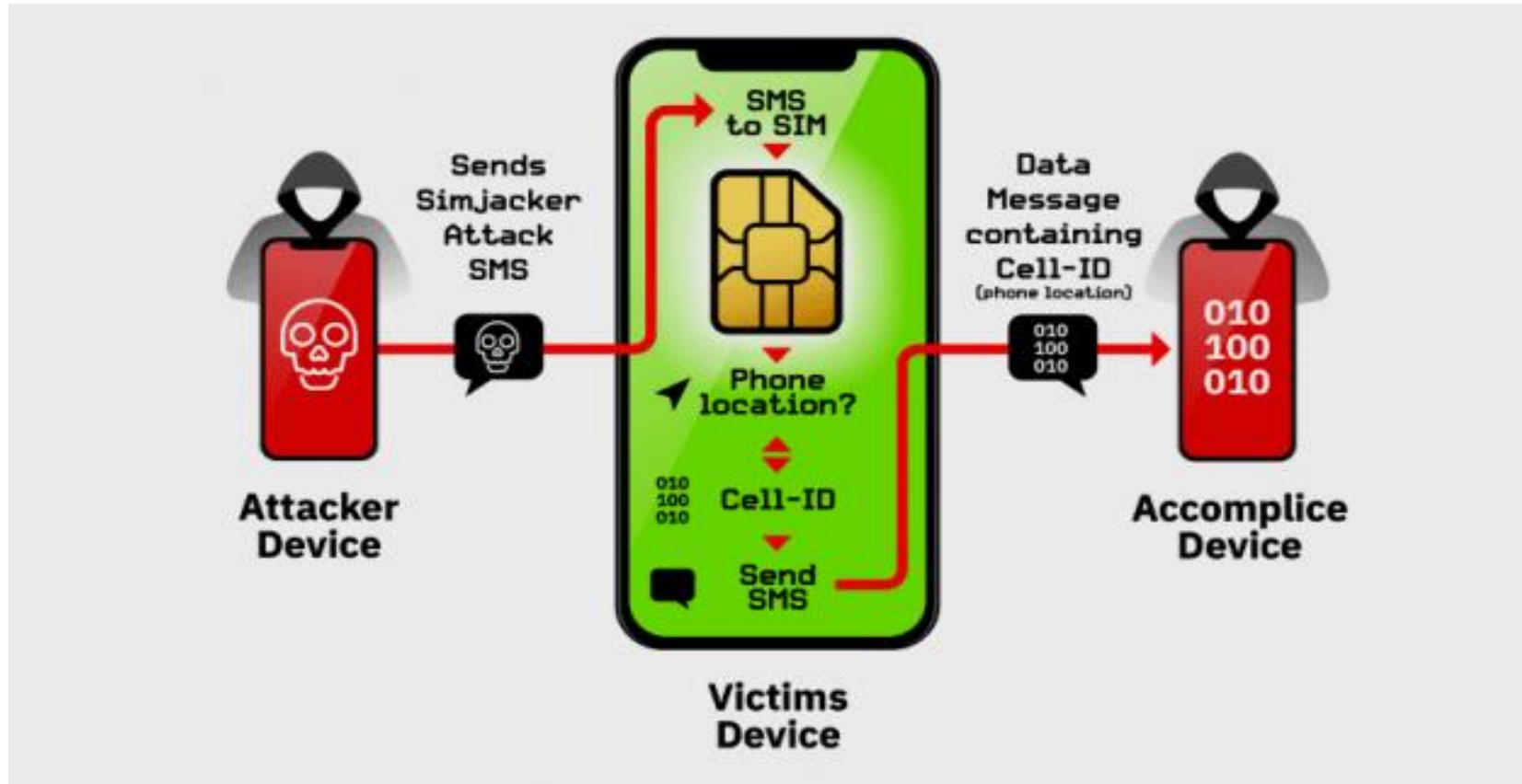
v Command details: 012304
  Command Number: 0x01
  Command Type: GET INPUT (0x23)
  Command Qualifier: 0x04
v Device identity: 8281
  Source Device ID: Terminal (Card Reader) (0x82)
  Destination Device ID: SIM / USIM / UICC (0x81)
v Result: 00
  Result: Command performed successfully (0x00)
v Text string: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

```

DFS PIN from captured data



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



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](https://cve.mitre.org/cve/2019/16256/))

Source: Adaptive Mobile

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:

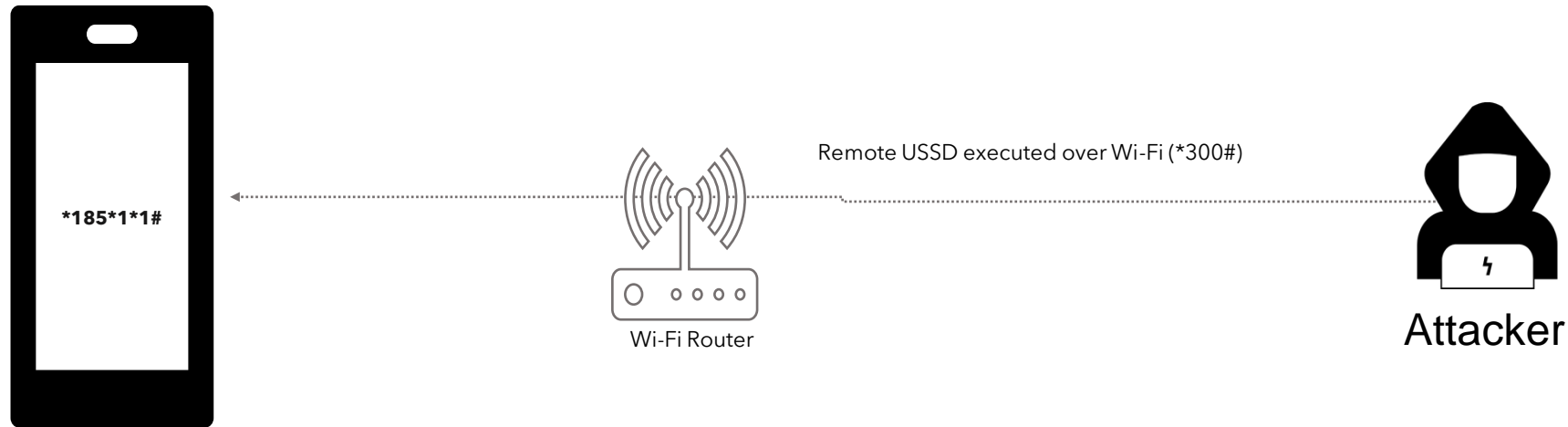
TAR	keyset	Response packets
313131	1	027100000B0A31313100000000010002 027100000B0A31313100000000000000 027100000B0A31313100000000010000
313131	2	027100000B0A31313100000000010000 027100000B0A31313100000000010002 027100000B0A31313100000000000000
313131	3	027100000B0A31313100000000010000 027100000B0A31313100000000010002 027100000B0A31313100000000000000
313131	4	027100000B0A31313100000000010002 027100000B0A31313100000000010000 027100000B0A31313100000000000000
313131	5	027100000B0A31313100000000010002 027100000B0A31313100000000010000 027100000B0A31313100000000000000
494D45	1	027100000B0A494D4500000000010002 027100000B0A494D4500000000010000 027100000B0A494D4500000000000000
494D45	2	027100000B0A494D4500000000010002 027100000B0A494D4500000000010000 027100000B0A494D4500000000000000
494D45	3	027100000B0A494D4500000000010002 027100000B0A494D4500000000010000 027100000B0A494D4500000000000000
494D45	4	027100000B0A494D4500000000010000 027100000B0A494D4500000000010002 027100000B0A494D4500000000000000
494D45	5	027100000B0A494D4500000000010002 027100000B0A494D4500000000010000 027100000B0A494D4500000000000000
505348	1	027100000B0A50534800000000000000 027100000B0A50534800000000010000 027100000B0A50534800000000010002
505348	2	027100000B0A50534800000000000000 027100000B0A50534800000000010000 027100000B0A50534800000000010002
505348	3	027100000B0A50534800000000010000 027100000B0A50534800000000010002 027100000B0A50534800000000000000
505348	4	027100000B0A50534800000000010002 027100000B0A50534800000000010000 027100000B0A50534800000000000000
505348	5	027100000B0A50534800000000010000 027100000B0A50534800000000010002 027100000B0A50534800000000000000
524144	1	027100000B0A52414400000000000000 027100000B0A52414400000000010000 027100000B0A52414400000000010002
524144	2	027100000B0A52414400000000000000 027100000B0A52414400000000010002 027100000B0A52414400000000010000
524144	3	027100000B0A52414400000000000000 027100000B0A52414400000000010002 027100000B0A52414400000000010000
524144	4	027100000B0A52414400000000000000 027100000B0A52414400000000010002 027100000B0A52414400000000010000
524144	5	027100000B0A52414400000000000000 027100000B0A52414400000000010002 027100000B0A52414400000000010000
534054	1	027100000B0A53405400000000010002 027100000B0A53405400000000010000 027100000B0A53405400000000000000
534054	2	027100000B0A53405400000000010000 027100000B0A53405400000000010002 027100000B0A53405400000000000000
534054	3	027100000B0A53405400000000010000 027100000B0A53405400000000010002 027100000B0A53405400000000000000
534054	4	027100000B0A53405400000000010002 027100000B0A53405400000000010000 027100000B0A53405400000000000000
534054	5	027100000B0A53405400000000010000 027100000B0A53405400000000010002 027100000B0A53405400000000000000

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
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

SHODAN android debug bridge product:"Android Debug Bridge"

Exploits Maps Like 1 Download Results Create Report

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.netnavigator.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

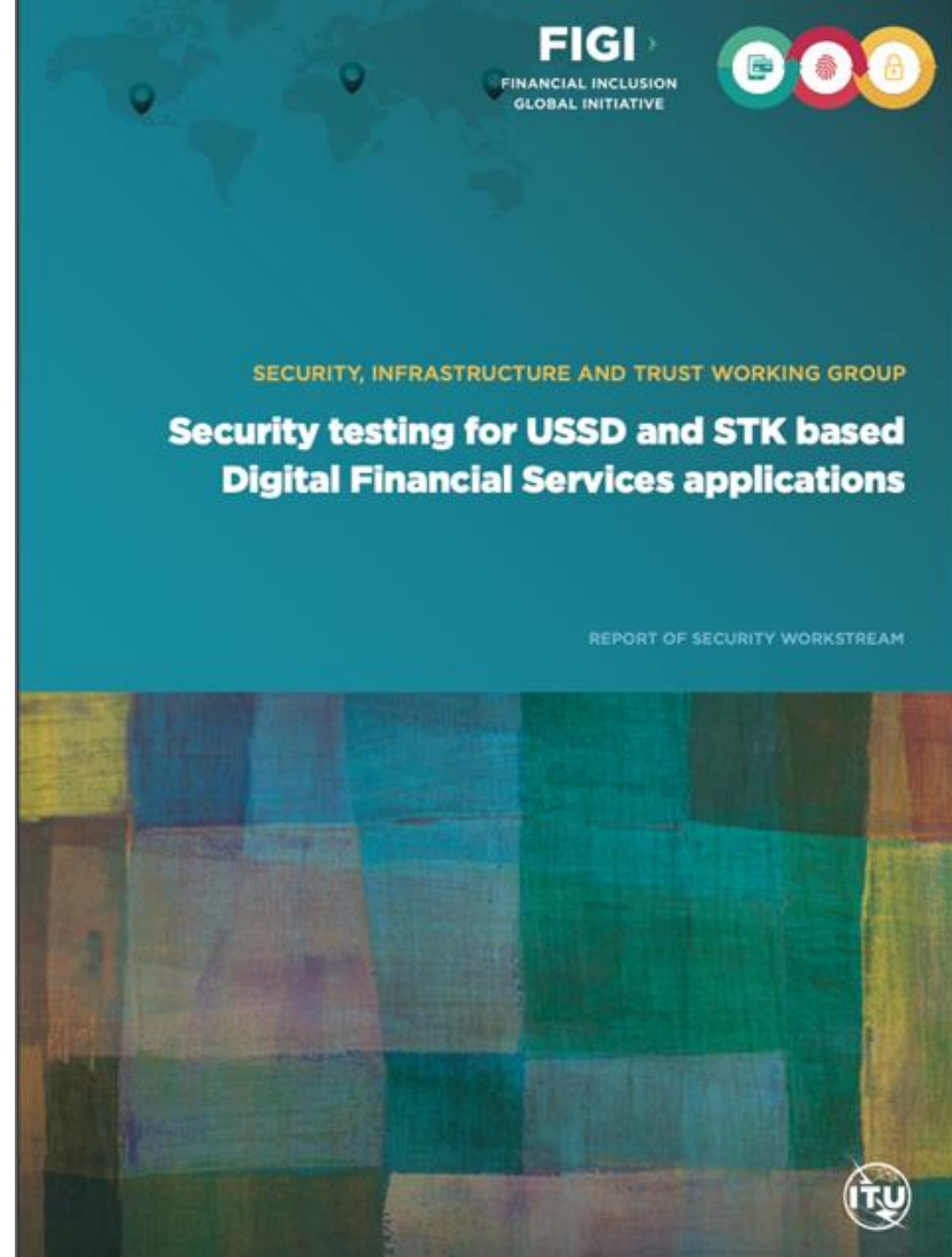
- Binary OTA SMS filtering & blocking.
- SMS home routing.
- SIM card security

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)



What we need to test your DFS app



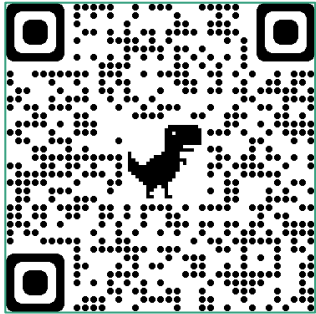
USSD and STK tests

- 2 SIM cards for the MNO networks to be tested.
- Active DFS account on each SIM
- PIN codes of the active wallets
- Prepaid mobile credit on the SIM cards.
- Include the USSD codes for each of the DFS providers.
- DFS credit on the DFS wallets (To be used for the tests).

Android app testing

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

Get in touch



dfssecuritylab@itu.int



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



www.itu.int