FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium
18 May - 24 June, 2021

Security testing for USSD and STK based DFS apps

Arnold Kibuuka, TSB, ITU

figi.itu.int
#financialinclusion

Organized by

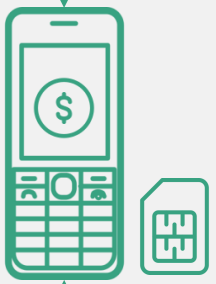
Committee on Payments and Market Infrastructures | BIS | THE WORLD BANK IBRD • IDA | ITU

Overview

- Security Risks to USSD and STK DFS Applications
- Examples of DFS attacks
- USSD & STK DFS Security tests
- Recommendations

Security Risks to USSD and STK DFS Applications

- Social engineering/smishing



- SIM swap and SIM cloning
- Device malware
- Thin SIMs
- Rooted devices

- Man in the middle attacks
- SS7 vulnerability

Examples of DFS attacks

- April 2021, The Standard: **Fraud forces SMEs to slip back to cash payments**
- March 2021, Times Of India, **2 duped of Rs 82k in SIM swap fraud**
- March 2021, Nairobi News: **Police arrest six Sim-swap fraud suspects in Kasarani**
- The Daily Monitor: **Thieves use 2,000 SIM cards to rob banks**
- Ghana Chamber of Telecommunications: **Mobile Money Fraudsters Now Target Bank Accounts Linked To MoMo Accounts**
- February 2021, CNN: **Police arrest eight after celebrities hit by SIM-swapping attacks**

Impact on Consumers

Loss of funds

Service disruption

Loss of consumer trust

DFS Security Lab Objectives

Collaboration with DFS regulators on security

Perform DFS **security audits** of DFS Apps

Encourage adoption of **international standards on DFS security**

Organise **security clinics**

Assist DFS regulators to evaluate the **cyber preparedness** for DFS ecosystem

Knowledge sharing on threats to security of DFS apps

figi.itu.int
#financialinclusion

DFS Security Lab Components

1

Developer resources for strong authentication using **FIDO**

2

Security audit of **Android** DFS apps using **OWASP** Mobile Top 10 Risks.

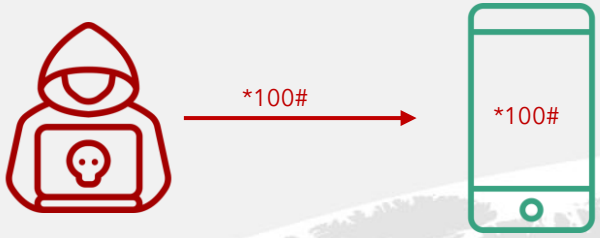
3

Security audits for **USSD** and **STK** based DFS

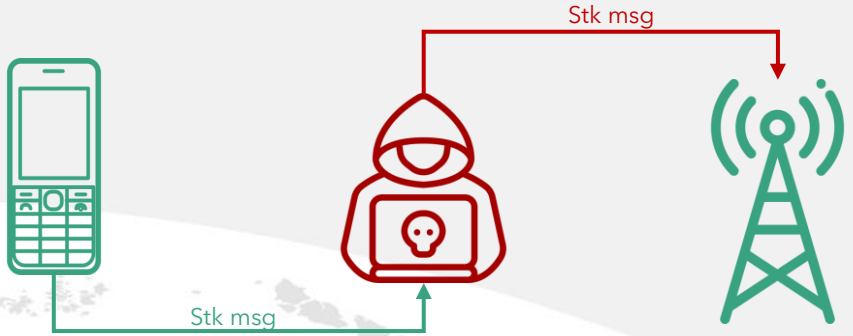
USSD & STK Security Tests

a. **SIM Swap** and **SIM clone** testing

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

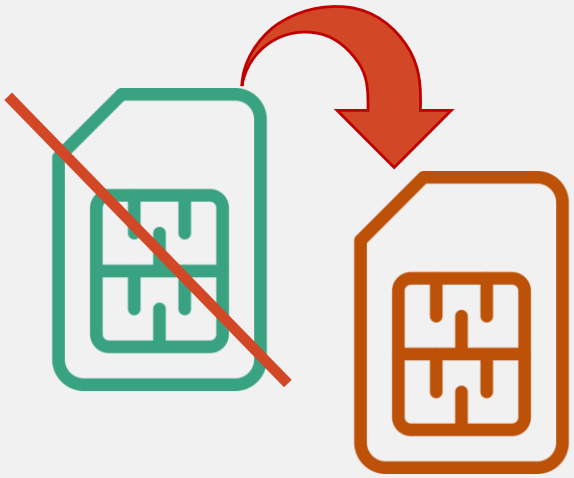


c. Testing **remote USSD** execution attacks



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

SIM Swap and **SIM clone**



a. **SIM Swap** and **SIM clone** testing

- SIM swapping allows a phone number to be ported from one phone to another
- Attackers can abuse this to hijack phone numbers

- Test whether the DFS provider can detect:
  - Change of device(IMEI)
  - Change of IMSI and or SIM number

- In the SIM clone test, we test the we have software to attempt to carry out the actual duplication of the SIM card

Binary over the air attacks

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


```
SIMTester has discovered following weaknesses:

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

313131      1 027100000B0A3131310000000010002 027100000B0A3131310000000000000 027100000B0A3131310000000010000
313131      2 027100000B0A3131310000000010000 027100000B0A3131310000000010002 027100000B0A3131310000000000000
313131      3 027100000B0A3131310000000010000 027100000B0A3131310000000010002 027100000B0A3131310000000000000
313131      4 027100000B0A3131310000000010002 027100000B0A3131310000000010000 027100000B0A3131310000000000000
313131      5 027100000B0A3131310000000010002 027100000B0A3131310000000010000 027100000B0A3131310000000000000
494D45      1 027100000B0A494D450000000010002 027100000B0A494D450000000010000 027100000B0A494D450000000000000
494D45      2 027100000B0A494D450000000010002 027100000B0A494D450000000010000 027100000B0A494D450000000000000
494D45      3 027100000B0A494D450000000010002 027100000B0A494D450000000010000 027100000B0A494D450000000000000
494D45      4 027100000B0A494D450000000000000 027100000B0A494D450000000010000 027100000B0A494D450000000010002
494D45      5 027100000B0A494D450000000000000 027100000B0A494D450000000010002 027100000B0A494D450000000010000
505348      1 027100000B0A505348000000000000 027100000B0A505348000000010000 027100000B0A505348000000010002
505348      2 027100000B0A505348000000000000 027100000B0A505348000000010000 027100000B0A505348000000010002
505348      3 027100000B0A505348000000010000 027100000B0A505348000000010002 027100000B0A505348000000000000
505348      4 027100000B0A505348000000010002 027100000B0A505348000000010000 027100000B0A505348000000000000
505348      5 027100000B0A505348000000010000 027100000B0A505348000000010002 027100000B0A505348000000000000
524144      1 027100000B0A524144000000000000 027100000B0A524144000000010000 027100000B0A524144000000010002
524144      2 027100000B0A524144000000000000 027100000B0A524144000000010002 027100000B0A524144000000010000
524144      3 027100000B0A524144000000000000 027100000B0A524144000000010002 027100000B0A524144000000010000
524144      4 027100000B0A524144000000000000 027100000B0A524144000000010002 027100000B0A524144000000010000
524144      5 027100000B0A524144000000000000 027100000B0A524144000000010002 027100000B0A524144000000010000
534054      1 027100000B0A534054000000010002 027100000B0A534054000000010000 027100000B0A534054000000000000
534054      2 027100000B0A534054000000010000 027100000B0A534054000000010002 027100000B0A534054000000000000
534054      3 027100000B0A534054000000010000 027100000B0A534054000000010002 027100000B0A534054000000000000
534054      4 027100000B0A534054000000010002 027100000B0A534054000000010000 027100000B0A534054000000000000
534054      5 027100000B0A534054000000010000 027100000B0A534054000000000000 027100000B0A534054000000010002

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
```

Remote USSD execution

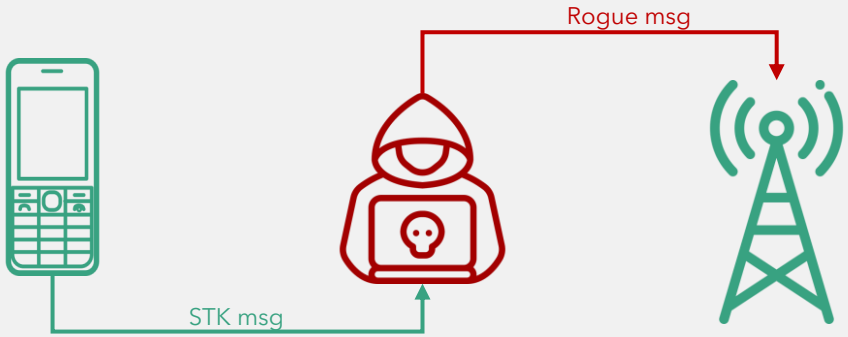
Testing **remote USSD** execution attacks

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:/ $
```

Man-in-the-middle STK attacks

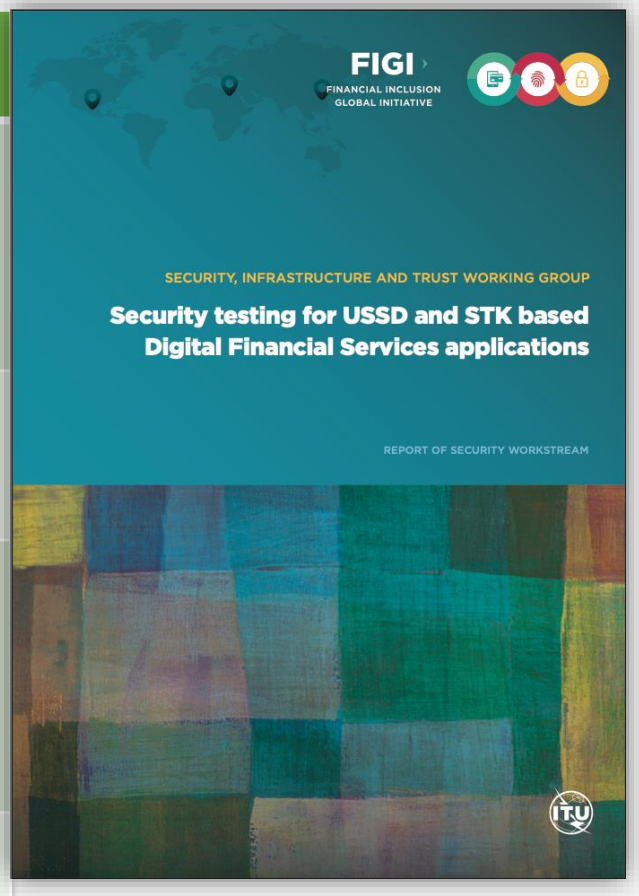
Simulation **Man-in-the-middle attacks** on STK based DFS applications




```
428     133.…  lo…  lo… GSM …    77 ETSI TS 102.221 TERMINAL RESPONSE SEND SHORT MESSAGE
121     33.2…  lo…  lo… GSM …    77 ETSI TS 102.221 TERMINAL RESPONSE SET UP EVENT LIST
<
    ▾ 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 ending of command with info from proactive SIM
```

Mitigation measures

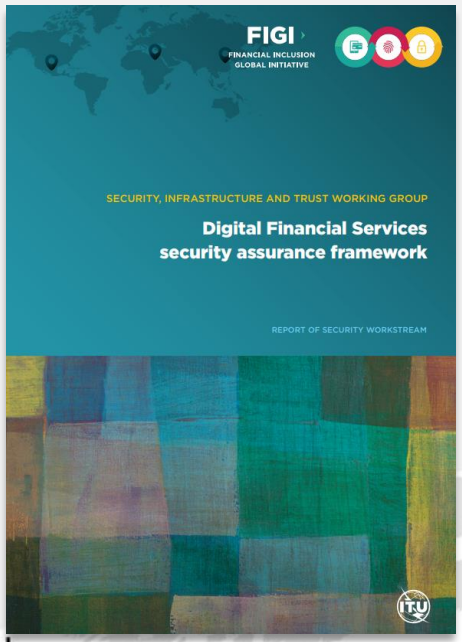
Risk	Recommendations
Remote USSD execution on devices	- Disable ADB - User education - Discourage use rooted devices
SIM exploitation using binary OTA	- Binary OTA SMS filtering & blocking. - SMS home routing. - SIM card security
Man-in-the-Middle attacks	- Secure radio channel communication - Regulatory review were thin SIMs are used - SS7 controls and mitigations - Use session timeout
SIM swap and SIM cloning	- SIM and device change detection. (ICCID, IMEI) - Secure storage of SIM data like IMSI and secret key (KI values)

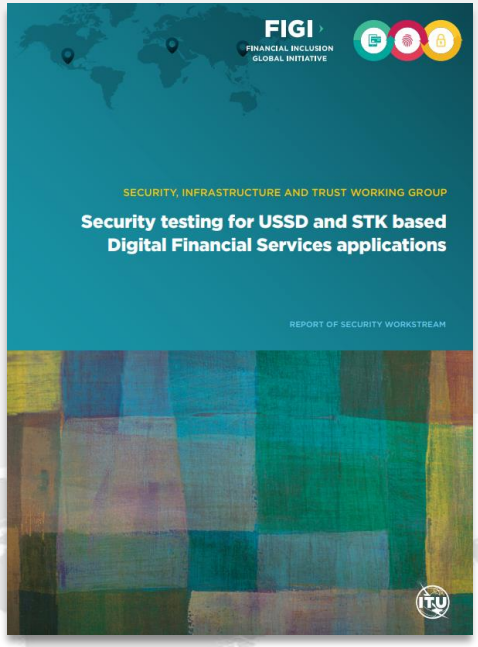


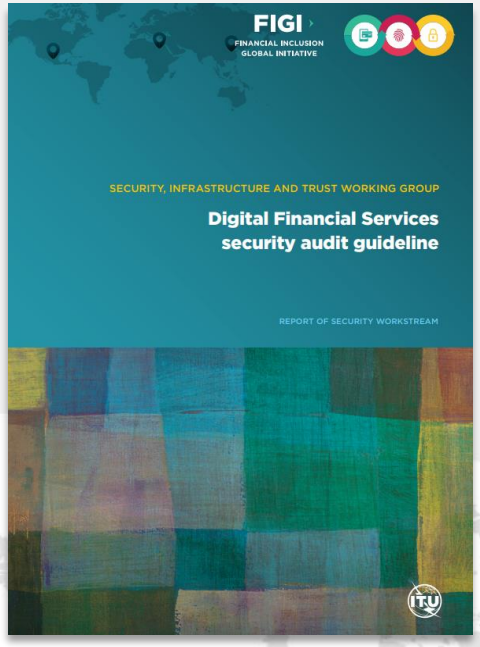
Security testing for USSD and STK based DFS applications

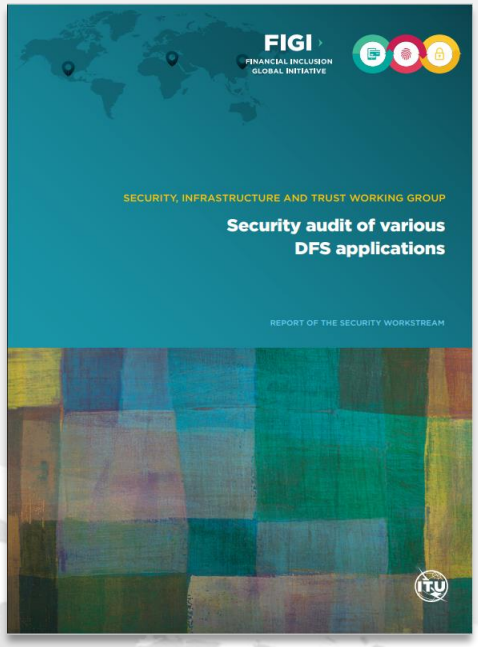
DFS Security Lab resources

Collaborate with DFS regulators and DFS providers to enhance the cybersecurity strategy for DFS and security assurance of the DFS ecosystem by implementing the recommendations in the DFS Security Assurance Framework, methodology for testing of USSD, STK and Android apps and DFS Security Audit Guidelines.









DFS Security Lab

Get in touch

dfssecuritylab@itu.int

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