

# Mobile Payment Application Security Tests

---

Arnold Kibuuka, Project Officer, ITU

February 2022



# Overview

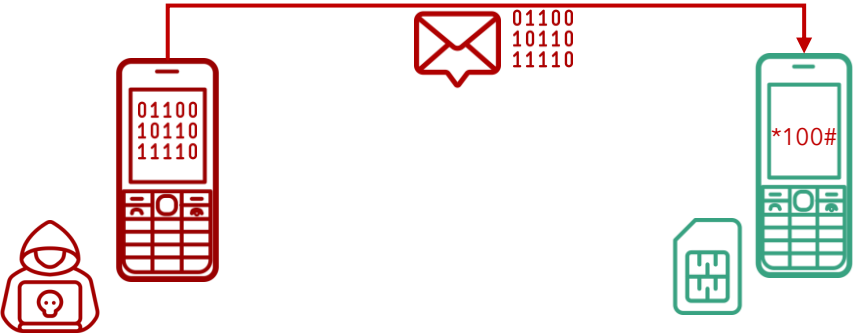
- i. USSD & STK App security tests
- ii. Android App security tests

# USSD and STK App Security Tests

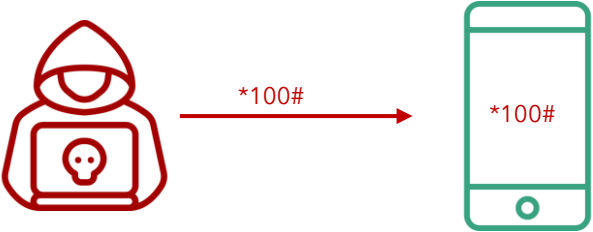
# USSD and STK App Security Tests



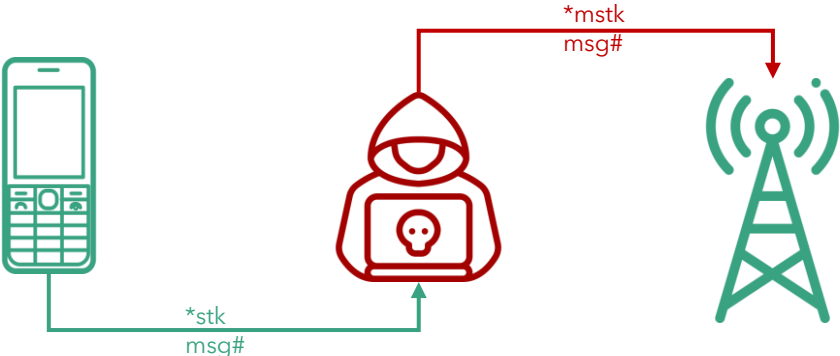
a. **SIM Swap** and **SIM cloning**



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

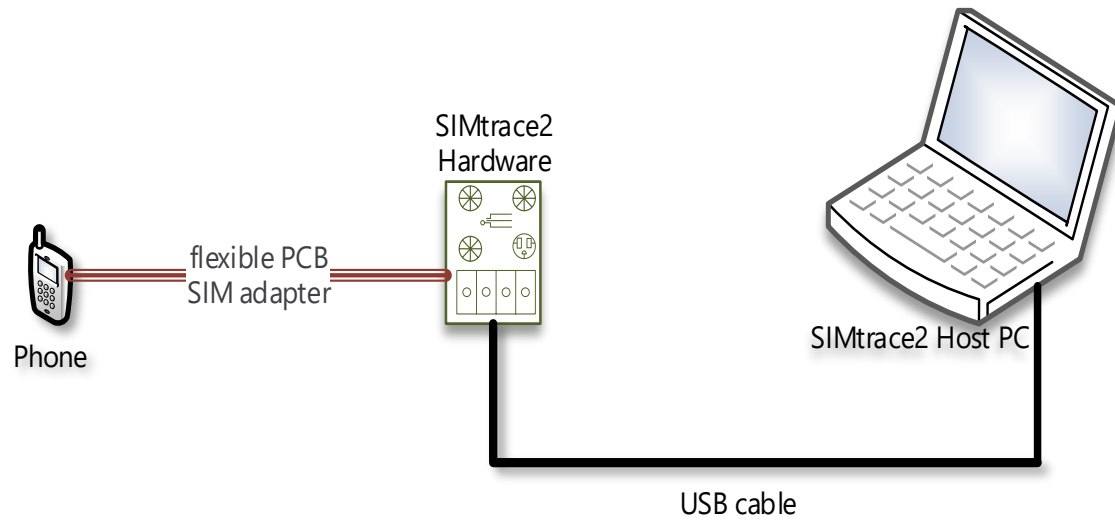


c. **remote USSD execution attacks**



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

# 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)

```

```

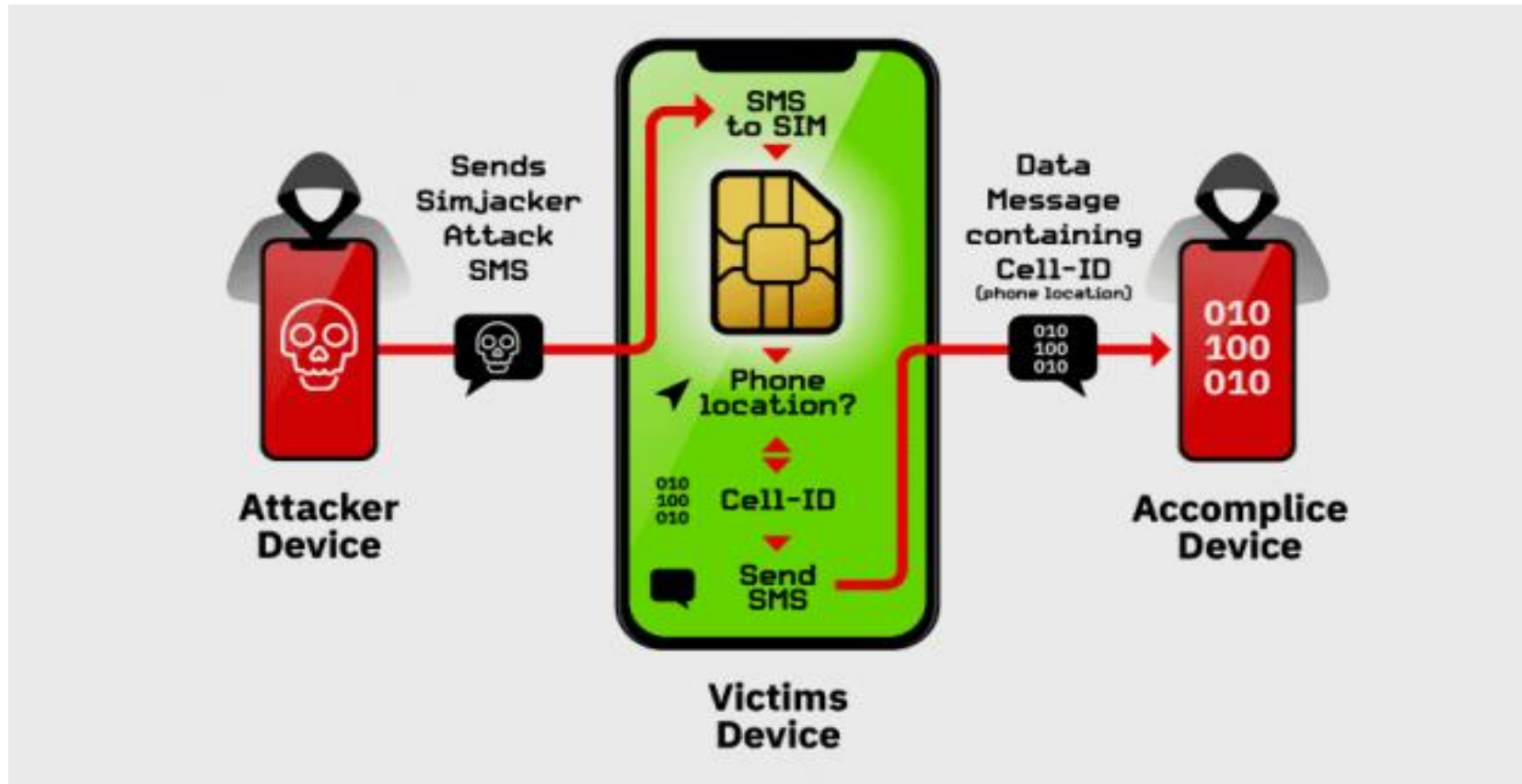
v Command details: 012304
  Command Number: 0x01
  Command Type: GET INPUT (0x23)
  Command Qualifier: 0x04
v Device identity: 8281
  Source Device ID: Terminal (Card Reader) (0x82)
  Destination Device ID: SIM / USIM / UICC (0x81)
v Result: 00
  Result: Command performed successfully (0x00)
v Text string: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

```

DFS PIN from captured data



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



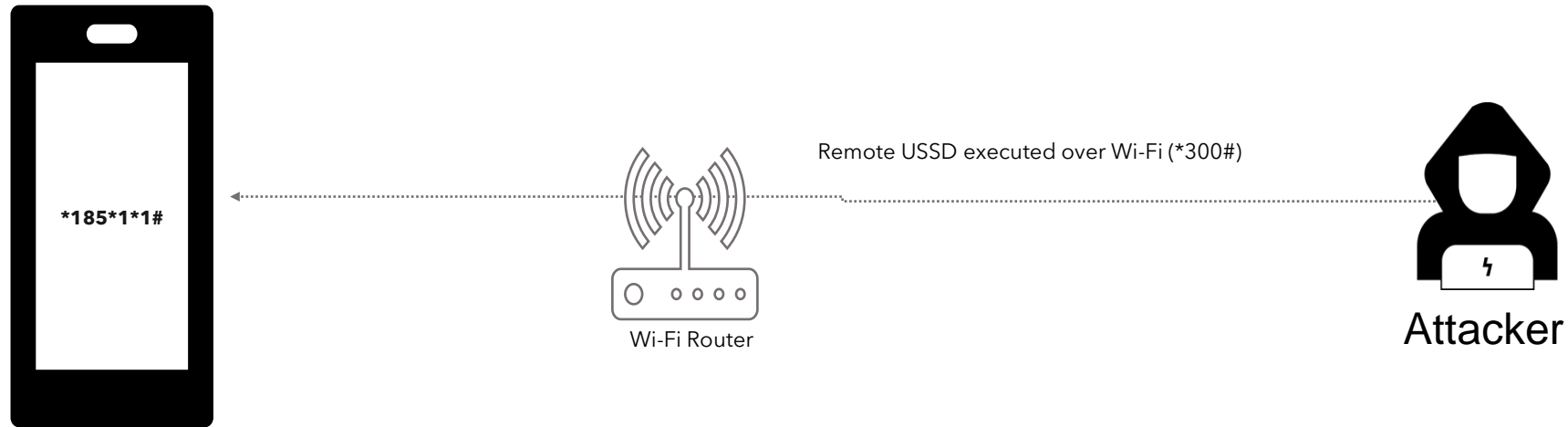
A binary OTA message can instruct the SIM to:

- 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 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

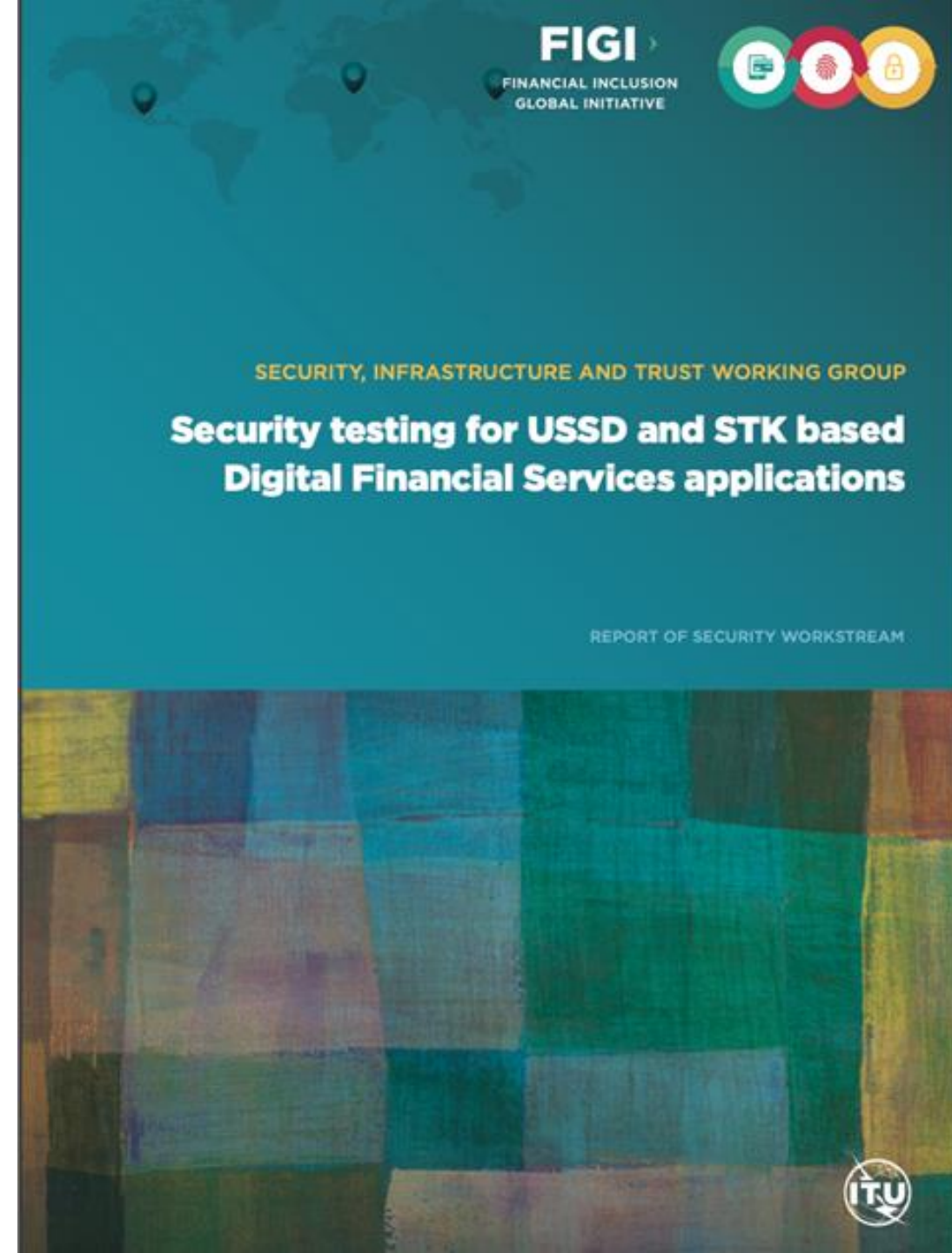
- Binary OTA SMS filtering & blocking.
- SMS home routing.
- SIM card security

## 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)



# 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

# Android App Security Tests



## Introduction

### **The Open Web Application Security Project**

A collaborative, non-for-profit foundation that works to improve the security of web applications

Also works on security of mobile applications.

### **OWASP Mobile Top Ten**

OWASP project that aims to identify and document the top ten vulnerabilities of mobile applications

### **Lab methodology**

18 tests organized according to OWASP mobile top ten

# Android tests

- Our tests are organized according to the subjects of the OWASP Mobile Top Ten:
  - M1 Improper Platform Usage
  - M2 Insecure Data Storage
  - M3 Insecure Communication
  - M4 Insecure Authentication
  - M5 Insufficient Cryptography
  - M6 *Insecure Authorization*
  - M7 *Client Code Quality*
  - M8 Code Tampering
  - M9 Reverse Engineering
  - M10 *Extraneous Functionality*
- M6, M7, M10 out of scope because they would need access to the source code or require collaboration with the editor

# M1 Improper Platform Usage

*The application should make correct use of the features of the platform (phone's operating system)*

## T1.1 Android:allowBackup

- Backup of the application and its data into the cloud should be disabled

## T1.2 Android:debuggable

- Debugging features of the application should be disabled

## T1.3 Android:installLocation

- The application should be installed in the internal, more secure, memory

## T1.4 Dangerous permissions

- The application should not require dangerous permissions, as defined by Android.

| PERMISSION                                | STATUS    | INFO                            | DESCRIPTION   |
|---|-----------|---------------------------------|---|
| android.permission.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. |
| android.permission.ACCESS_FINE_LOCATION   | dangerous | fine (GPS) location             | Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.     |



# M2 Insecure Data Storage

```
<uses-sdk android:minSdkVersion="16" android:targetSdkVersion="28" />
<uses-feature android:name="android.hardware.telephony" android:required="false" />
<uses-feature android:name="android.hardware.telephony.cdma" android:required="false" />
<uses-feature android:name="android.hardware.telephony.gsm" android:required="false" />
<uses-feature android:name="android.hardware.camera" android:required="false" />
<uses-feature android:name="android.hardware.camera.autofocus" android:required="false" />
<uses-feature android:name="android.hardware.camera.flash" android:required="false" />
<uses-feature android:name="android.hardware.camera.front" android:required="false" />
<uses-feature android:name="android.hardware.camera.any" android:required="false" />
<uses-feature android:name="android.hardware.bluetooth" android:required="false" />
<uses-feature android:name="android.hardware.location" android:required="false" />
<uses-feature android:name="android.hardware.location.network" android:required="false" />
<uses-feature android:name="android.hardware.location.gps" android:required="false" />
<uses-feature android:name="android.hardware.microphone" android:required="false" />
<uses-feature android:name="android.hardware.wifi" android:required="false" />
<uses-feature android:name="android.hardware.wifi.direct" android:required="false" />
<uses-feature android:name="android.hardware.screen.landscape" android:required="false" />
<uses-feature android:name="android.hardware.screen.portrait" android:required="false" />
<uses-feature android:glEsVersion="0x00020000" android:required="true" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.USE_FINGERPRINT" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.WRITE_CALENDAR" />
<uses-permission android:name="android.permission.CAMERA" />
<uses-permission android:name="android.permission.FLASHLIGHT" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<supports-screens android:largeScreens="true" android:xlargeScreens="true" />
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE" />
```

*Data should be stored in a way that limits the risks in case of loss or compromise of the phone*

## T2.1 Android.permission.WRITE\_EXTERNAL\_STORAGE

- No permission to write to a removable memory card

## T2.2 Disabling screenshots

- If not disabled, screen shots are done automatically to generate thumbnails for task switching

# M3 Insecure Communication

*Protect against eavesdropping and manipulation of traffic*

## T3.1 Application should only use HTTPS connections

- Test by sniffing traffic

## T3.2 Application should detect Machine-in-the-Middle attacks with untrusted Certificates

- Would allow anybody to intercept traffic
- Test by intercepting traffic with proxy

## T3.3 Application should detect Machine-in-the-Middle attacks with trusted certificate

- Would allow authorities to intercept traffic
- Test by installing root certificate on phone, intercept with proxy

## T3.4 App manifest should not allow clear text traffic

The screenshot displays the Burp Suite interface. The top menu includes 'Burp Project', 'Intruder', 'Repeater', 'Window', 'Help', 'Logger++', and 'Backslash'. Below the menu is a toolbar with various tools like 'Errors', 'Espresso', 'ExFTool', 'JSON Beautifier', 'Deserialization Scanner', 'Logger++', 'Paramalyzer', 'Versions', 'Software Vulnerability Scanner', and 'Additional Scanner Checks'. The main window shows a list of intercepted items with columns for '#', 'Host', 'Method', 'URL', 'Params', 'Edited', 'Status', 'Length', 'MIME type', 'Extension', 'Title', 'Comment', 'TLS', 'IP', 'Cookies', and 'Time'. A row is highlighted in orange, corresponding to a POST request to '/smartphone/service/v11/orders/p2p/send'. Below this, the 'Request' and 'Response' tabs are visible, with the 'Request' tab selected. The request details show a POST to '/smartphone/service/v11/orders/p2p/send' with headers like 'Accept-Encoding: gzip, deflate', 'Accept: application/json', and 'Content-Type: application/json; charset=UTF-8'. The body of the request is a JSON object containing fields like 'amount', 'currency', 'certificateFingerprint', 'moneyReceiver', 'moneyReceiverMobileNumber', 'moneySender', 'orderId', 'reservationDate', 'sendMoneyEvenIfCustomerUnknown', and 'signature'.

Burp Project Intruder Repeater Window Help Logger++ Backslas...

Errors EsPReSSO ExifTool JSON Beautifier Deserialization Scanner Logger++ Paramalyzer Versions Software Vulnerability Scanner Additional Scanner Checks

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options AuthMatrix Bypass WAF CO2

Intercept HTTP history WebSockets history Options

Filter: Hiding out of scope items

| #   | Host               | Method | URL  | Params | Edited | Status | Length | MIME type | Extension | Title | Comment | TLS | IP         | Cookies | Time     |
|-----|--------------------|--------|--|--------|--------|--------|--------|-----------|-----------|-------|---------|-----|------------|---------|----------|
| 148 | https://[REDACTED] | GET    | /iizwlm?_=1594371899392                        |        | ✓      | 200    | 491    | JSON      |           |       |         | ✓   | [REDACTED] |         | 11:04:54 |
| 145 | https://[REDACTED] | GET    | /iizwlm?_=1594371717242                        |        | ✓      | 200    | 491    | JSON      |           |       |         | ✓   | [REDACTED] |         | 11:01:51 |
| 144 | https://[REDACTED] | GET    | /iizwlm?_=1594371530169                        |        | ✓      | 200    | 491    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:58:40 |
| 141 | https://[REDACTED] | GET    | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...  |        | ✓      | 200    | 576    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:55:41 |
| 139 | https://[REDACTED] | POST   | /smartphone/service/v11/privateCustomers/me... |        | ✓      | 200    | 1480   | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:55:21 |
| 138 | https://[REDACTED] | GET    | /smartphone/service/v11/privateCustomers/me... |        | ✓      | 200    | 870    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:55:20 |
| 137 | https://[REDACTED] | POST   | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...  |        | ✓      | 200    | 805    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:55:12 |
| 136 | https://[REDACTED] | POST   | /smartphone/service/v11/orders/p2p/send        |        | ✓      | 200    | 777    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:55:09 |
| 135 | https://[REDACTED] | GET    | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...  |        | ✓      | 200    | 576    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:55:00 |
| 134 | https://[REDACTED] | GET    | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...  |        | ✓      | 200    | 576    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:54:47 |
| 133 | https://[REDACTED] | GET    | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...  |        | ✓      | 200    | 576    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:54:17 |
| 132 | https://[REDACTED] | GET    | /smartphone/service/v11/orders?limit=100&pa... |        | ✓      | 200    | 18539  | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:53:47 |
| 131 | https://[REDACTED] | POST   | /smartphone/service/v11/privateCustomers/me... |        | ✓      | 200    | 1480   | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:53:46 |
| 130 | https://[REDACTED] | GET    | /smartphone/service/v11/privateCustomers/me... |        | ✓      | 200    | 870    | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:53:45 |
| 129 | https://[REDACTED] | GET    | /smartphone/service/v11/orders?since=1970-0... |        | ✓      | 200    | 50014  | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:53:45 |
| 128 | https://[REDACTED] | POST   | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...  |        | ✓      | 200    | 1340   | JSON      |           |       |         | ✓   | [REDACTED] |         | 10:53:44 |

Request Response

Raw Params Headers Hex JSON JSON Beautifier

```

1 POST /smartphone/service/v11/orders/p2p/send HTTP/1.1
2 Accept-Encoding: gzip, deflate
3 Accept: application/json
4 Accept-Language: fr_CH
5 X-TWINT-WALLETAPP-LIB-VERSION: 15.3.0.18
6 Cookie: Navajo=UNBjXyUG2vyu2A3NYol+qgo/M3ThiBT8PhA944Z6Do/24f5NEDkkahF2VEohHy0zNKx2UuZivUg-
7 Content-Type: application/json; charset=UTF-8
8 Content-Length: 764
9 Host: [REDACTED]
10 Connection: close
11 User-Agent: okhttp/3.12.0
12 ADRUM_1: isMobile:true
13 ADRUM: isAjax:true
14
15 {
  "amount": {
    "amount": 20,
    "currency": "CHF"
  },
  "certificateFingerprint": "ef[REDACTED]417b",
  "moneyReceiver": {
    "firstName": [REDACTED],
    "lastName": [REDACTED]
  },
  "moneyReceiverMobileNumber": "+4179[REDACTED]",
  "moneySender": {
    "firstName": [REDACTED],
    "lastName": [REDACTED]
  },
  "orderId": "13976b6e-a57c-448a-8535-51d97f01928d",
  "reservationDate": "2020-07-10T08:55:12",
  "sendMoneyEvenIfCustomerUnknown": true,
  "signature": "gu2DEXJ5pqGx+0c6vQm0cU04MmYqyb+RIHT8iZ4jHGcul/Jx8iIwV1m6WU64G58oJnnEGH8WArldOmmc61/bZEjOEF3fRXR/2kffAreQNhE01Uc18sJFxx96iAt3Hfe336yHehB0qZ9zTKgtMZwGu8s3tzJNRpvrRszio2QCk5X7SIh26Ai04KD047uFmKEPThC
  }
  
```

# M4 Insecure Authentication

*Prevent unauthorized access to the application*

T4.1 Authentication required before accessing sensitive information

- Application must require PIN or fingerprint

T4.2 The application should have an inactivity timeout

T4.3 If a new fingerprint is added, authentication with fingerprints should be temporarily disabled

- User should provide PIN to enable fingerprints again
- Prevents attacks where an attacker adds their fingerprint to access the application

T4.4 It should not be possible to replay intercepted requests (e.g. a money transfer)

- An attacker intercepting a request for a money transfer could replay it to steal money from the victim.

# M5: Insufficient Cryptography

```
..  
"moneyReceiverMobileNumber": "+4179 [REDACTED]  
"moneySender": {  
  "firstName": [REDACTED]  
  "lastName": [REDACTED]  
},
```

*Cryptography can only protect confidentiality and integrity of data if correctly implemented*

```
112. }  
113.  
114. @TargetApi(8)  
115. public static File b(Context context) {  
116.     if (bl.a()) {  
117.         return context.getExternalCacheDir();  
118.     }  
119.     return new File(Environment.getExternalStorageDirectory().getPath() + "  
120. }  
121.  
122. public static String b(String str) {  
123.     try {  
124.         MessageDigest instance = MessageDigest.getInstance("SHA-1");  
125.         instance.update(str.getBytes());  
126.         return a(instance.digest());  
127.     } catch (NoSuchAlgorithmException unused) {  
128.         return String.valueOf(str.hashCode());  
129.     }  
130. }  
131.  
132. @TargetApi(9)  
133. public static boolean b() {  
134.     if (bl.b()) {  
135.         return Environment.isExternalStorageRemovable();  
136.     }  
137. }
```

T5.1 The app should not use unsafe crypto primitives

- E.g., MD5, SHA-1, RC4, DES, 3DES, Blowfish, ECB
- Search for these in the code
- Detection of these primitives does not imply that they are used for protecting critical information!

T5.2 The HTTPS connections should be configured according to best practices

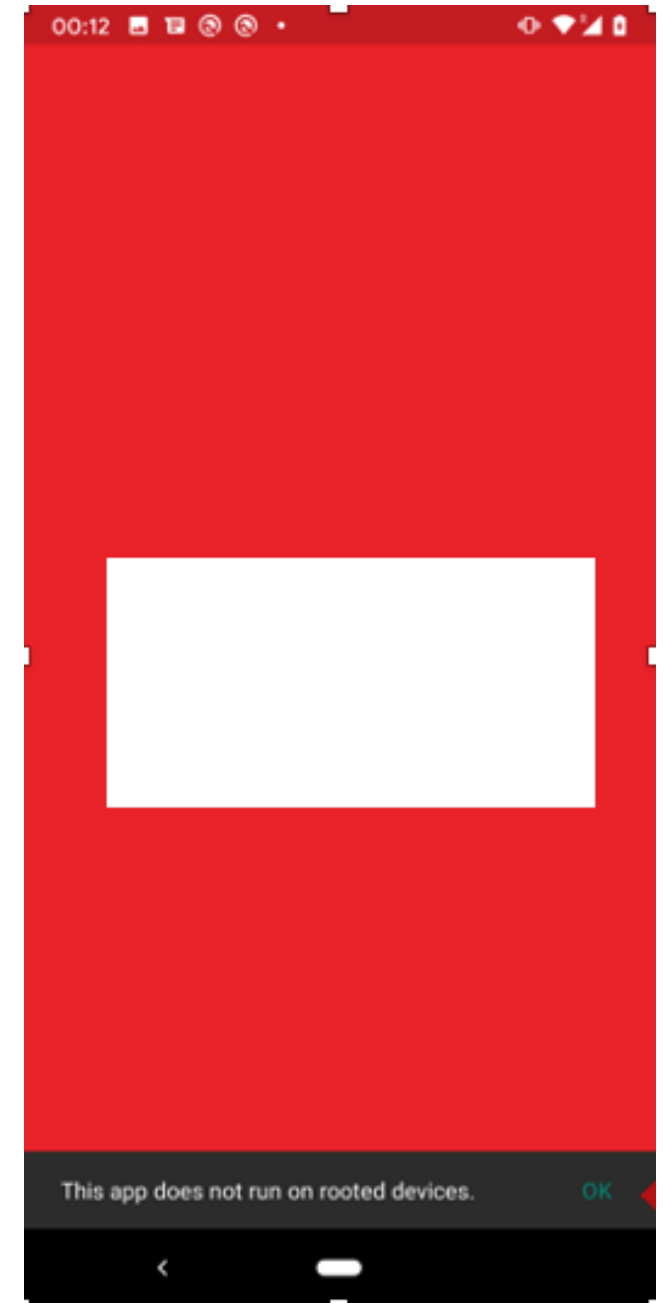
- Watch where the app connects to, use Qualys SSL labs to evaluate configuration, expect a grade of B or more

# M8: Code Tampering

*Prevent an attacker from tampering the code on the telephone*

T8.1 The application should refuse to run on a rooted device

- On a rooted device, users can manipulate the code of the application



# M9 Reverse engineering

```
125.         instance.upuade(str.getBytes());
126.         return a(instance.digest());
127.     } catch (NoSuchAlgorithmException unused) {
128.         return String.valueOf(str.hashCode());
129.     }
130. }
131.
132. @TargetApi(9)
133. public static boolean b() {
134.     if (bl.b()) {
135.         return Environment.isExternalStorageRemovable();
136.     }
137.     return true;
138. }
139.
140. public Bitmap a(String str) {
141.     dt<String, Bitmap> dtVar = this.d;
142.     if (dtVar != null) {
143.         return dtVar.a(str);
144.     }
145.     return null;
146. }
147.
148. public void a() {
149.     synchronized (this.g) {
150.         if (this.c == null || this.c.a()) {
151.             File file = this.f.c;
152.             if (this.f.g && file != null) {
153.                 if (!file.exists()) {
154.                     file.mkdirs();
155.                 }
156.             }
157.         }
158.     }
159. }
```

*Prevent attackers from analyzing the logic of the application*

## T9.1 The code should be obfuscated

- When the code is obfuscated, it is much more difficult to understand the logic of the code
- This makes it more difficult to manipulate the code or to find potential vulnerabilities
- Decompile the code and assess its readability

# Tests summary

| TEMPLATE FOR APPLICATION SECURITY BEST PRACTICES    | Corresponding tests  |
|---|--|
| 9.1 Device integrity                                | T1.2 Android:debuggable<br>T1.4 Dangerous permissions<br>T8.1 The application should refuse to run on a rooted device  |
| 9.2 Communication Security and Certificate Handling | T3.1 Application should only use HTTPS connections<br>T3.2 Application should detect Machine-in-the-Middle attacks with untrusted certificates<br>T3.3 Application should detect Machine-in-the-Middle attacks with trusted certificates<br>T3.4 App manifest should not allow clear text traffic<br>T5.1 The app should not use unsafe crypto primitives<br>T5.2 The HTTPS connections should be configured according to best practices<br>T5.3 The app should encrypt sensitive data that is sent over HTTPS |
| 9.3 User authentication                             | T4.1 Authentication required before accessing sensitive information<br>T4.2 The application should have an inactivity timeout<br>T4.3 If a fingerprint is added, authentication with fingerprints should be disabled<br>T4.4 It should not be possible to replay intercepted requests  |
| 9.4 Secure Data Handling                            | T1.1 Android:allowBackup<br>T1.3 Android:installLocation<br>T2.1 Android.permission.WRITE_EXTERNAL_STORAGE<br>T2.2 Disabling screenshots   |
| 9.5 Secure Application Development                  | T9.1 The code of the app should be obfuscated  |



# What we need to test your DFS app



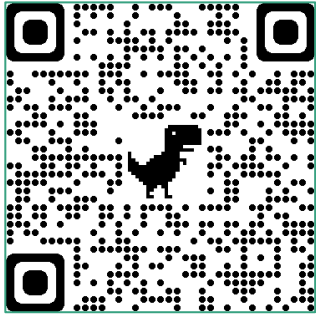
## USSD and STK tests

- 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](mailto:dfssecuritylab@itu.int)



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



[www.itu.int](http://www.itu.int)