# Mobile App Security Best Security Practices

Arnold Kibuuka, Project Officer, ITU
dfssecuritylab@itu.int

11 April 2024

# Overview

1. Mobile application security framework
2. DFS app security tests
    - Android App and
    - iOS Mobile Payment

# Objectives of the Recommendations

- **Enhance Security**: Implement robust security measures to protect against SS7 vulnerabilities, SIM risks, and SIM swap fraud.
- **Promote Best Practices**: Encourage the adoption of best practices in mobile financial services application security.
- **Foster Collaboration**: Strengthen collaboration between Telecommunications Regulators and Central Banks through a model MOU.
- **Improve Consumer Competency**: Enhance DFS consumer competency through a structured framework.
- **Advance Financial Inclusion**: Use these recommendations as tools to advance financial inclusion by making DFS safer and more secure for all users.

# Recap: DFS Security Recommendations

Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling

Recommendations to mitigate SS7 vulnerabilities

Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security

Mobile Application Security Best practices

ITU DFS Consumer Competence Framework

# Mobile Payment App Security framework

# Mobile Application Security best practices

## Device and Application Integrity

T1.2 Android:debuggable

T1.4 Dangerous permissions

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

## Communication Security and Certificate Handling

T3.1 Application should only use HTTPS connections

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

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

T3.4 App manifest should not allow clear text traffic

T5.1 The app should not use unsafe crypto primitives

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

T5.3 The app should encrypt sensitive data that is sent over HTTPS

## User Authentication

T4.1 Authentication required before accessing sensitive information

T4.2 The application should have an inactivity timeout

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

T4.4 It should not be possible to replay intercepted requests

## Secure Data Handling

T1.1 Android:allowBackup

T1.3 Android:installLocation

T2.1 Android.permission.WRITE_EXTERNAL_STORAGE

T2.2 Disabling screenshots

## Secure Application Development

T9.1 The code of the app should be obfuscated

# Android & iOS App DFS 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 on Android organized according to OWASP mobile top 10.

21 tests on iOS DFS applications

# iOS and 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

# DFS lab hardware and software

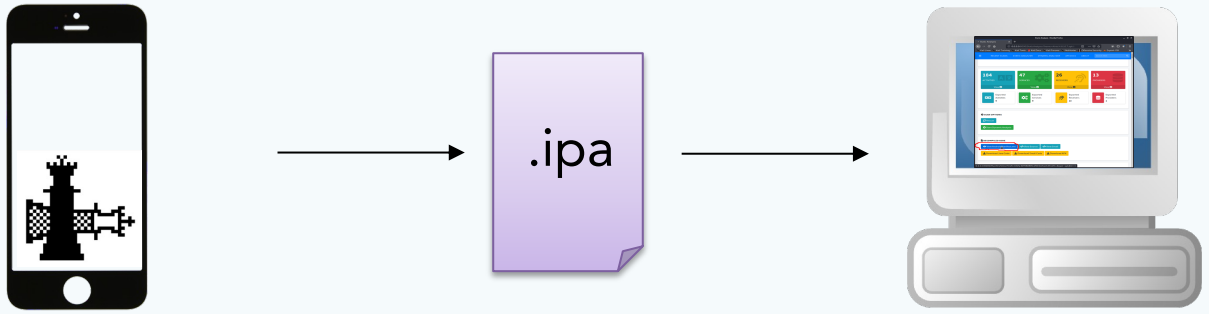
| EQUIPMENT | QTY | COMMENT | TESTS |
|---|---|---|---|
| Desktop/laptop | 2 | 32 GB RAM, 1TB, 4+ core 64-bit processor | All |
| Mobile smartphone (Android OS). | 2 | Google Pixel | Android |
| Wi-Fi router | 1 | | All |
| iOS Device | 2 | (One of the iPhones MUST run iOS 14 ) | iOS |
| Kali Linux | | Opensource | All |
| Wireshark | | Opensource | All |
| Magisk | | Opensource | All |
| Frida | | Opensource | All |
| MobSF | | Opensource | All |
| Androguard | | Opensource | All |
| Burp proxy | | Opensource/licenced | All |
| Objection | | | iOS |
| Checkra1n | | | iOS |
| Bettercap | | Opensource | All |
| apk-mitm | | Opensource | All |
| Personnel | | Security professionals with at least 3 years technical security experience | All |
| DFS Apps, SIM cards to be tested. | | | All |

# Summary of the tests

- 22 iOS and 18 Android tests organized according to OWASP mobile top ten
- Tests with jailbroken/rooted and non jailbroken/non rooted phones
- Static analysis of apps on a workstation
- Dynamic analysis with a man-in-the-middle proxy

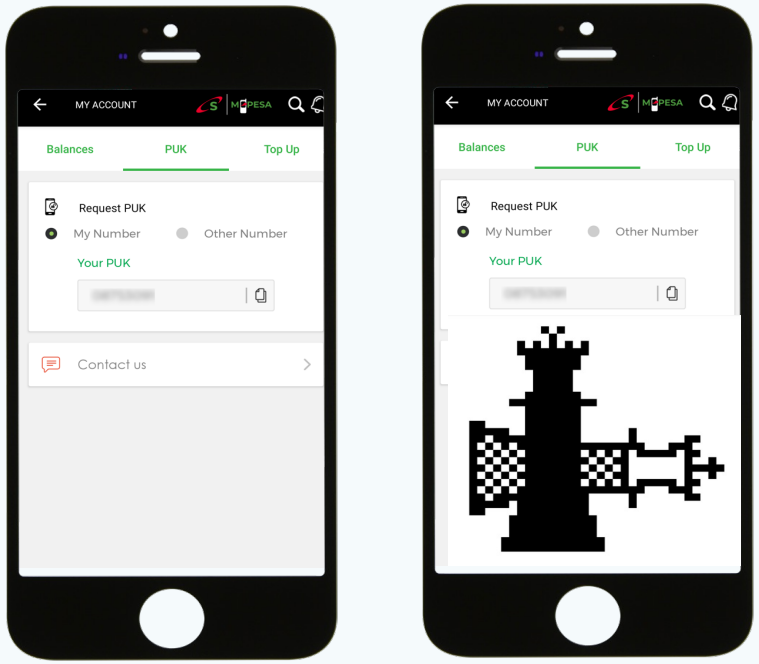
# Static tests

- Extract application package (apk/ipa) from a rooted/jailbroken phone
- Analyse the package on  workstation with different tools (Mobsf, Jadx)



# Functionality tests

Test security features on standard phone and on rooted phone



# Interception tests

- Use the workstation as man-in-the-middle between phone and server contacted by the application
  - Use Bettercap to force traffic through the workstation
  - Replace certificate on phone
  - Disable certificate pinning (on jailbroken phone only)
  - Use Burp proxy to analyse, modify, replay traffic

# Test details

# 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

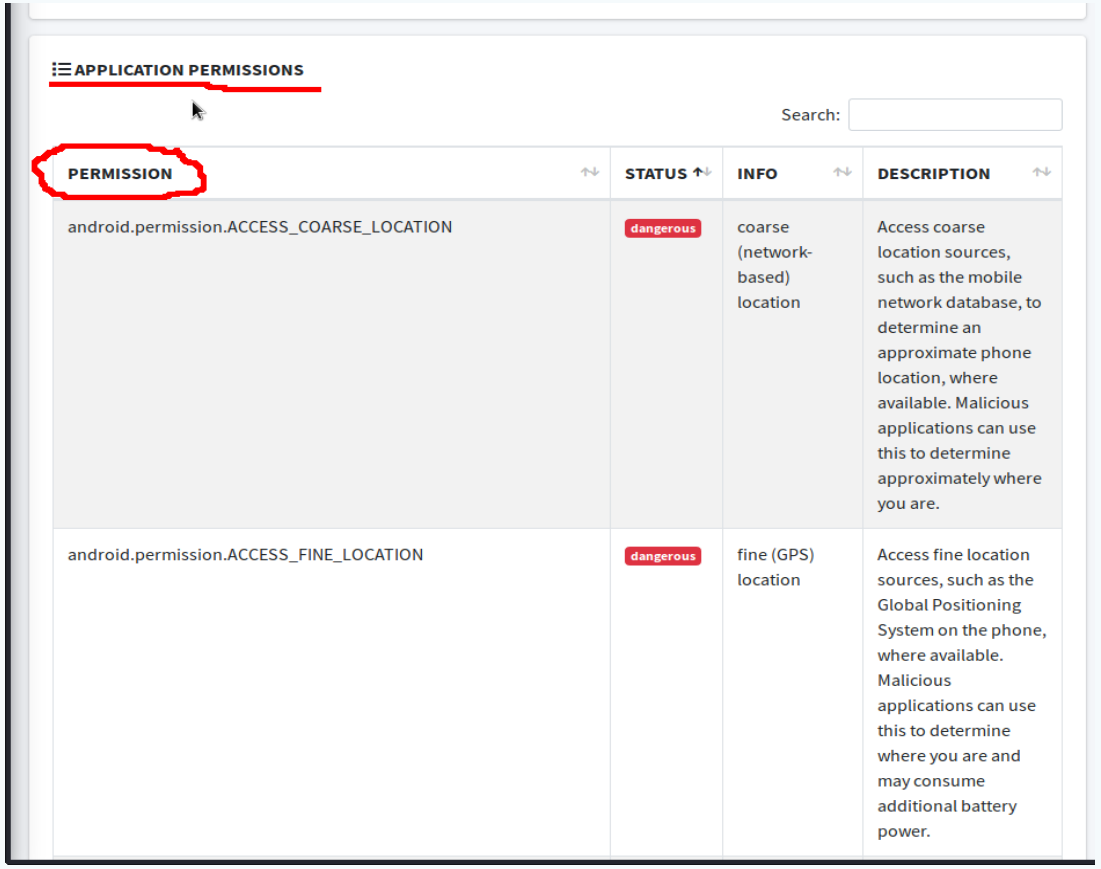
- Debugging features of the application should be disabled

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.



# M2 Insecure Data Storage


*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

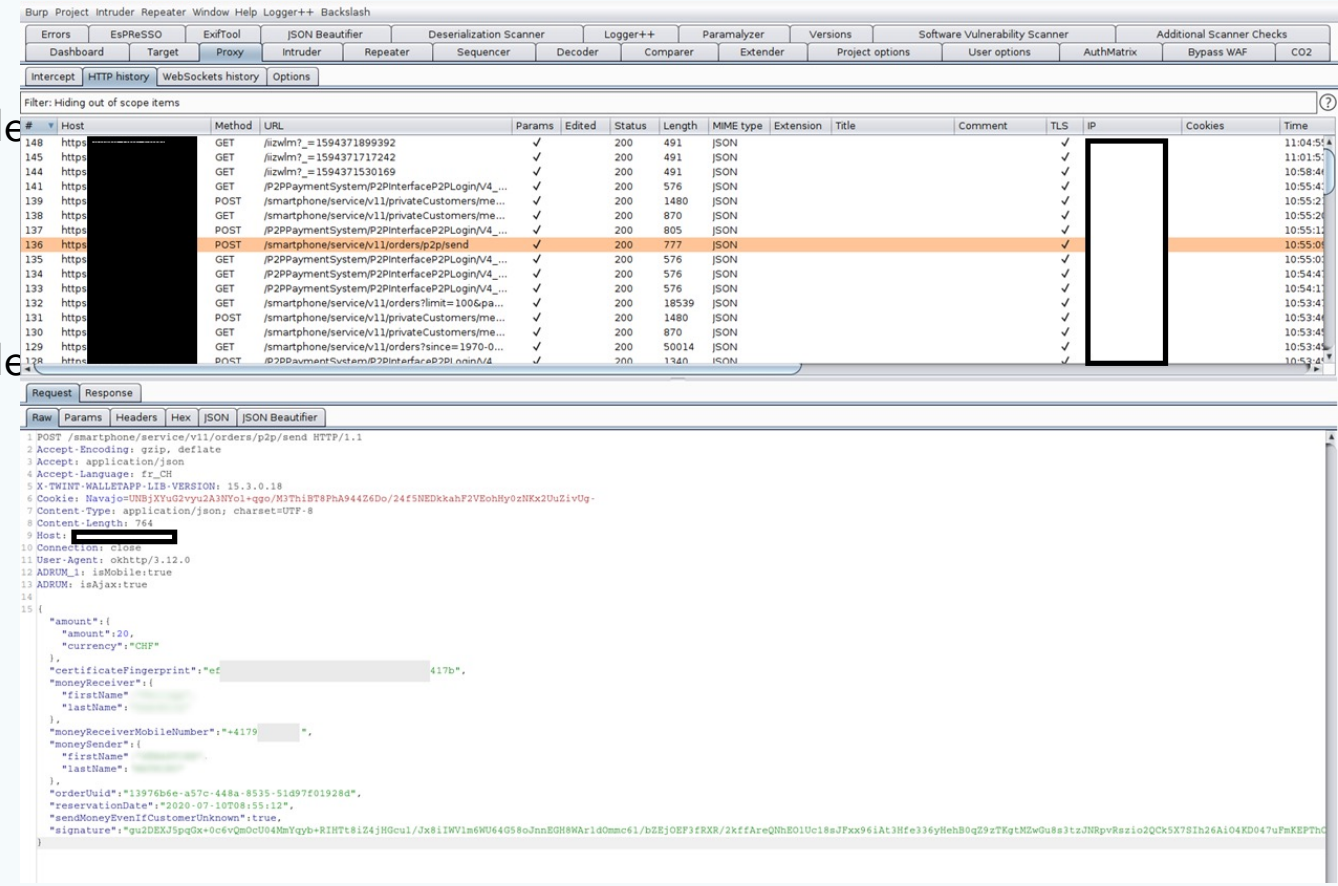
T3.2 Application should detect Machine-in-the-Middle attacks with untrusted Certificates

- 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



Burp Project Intruder Repeater Window Help Logger++ Backslash

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 | GET | /iizwlm?_=1594371899392 | ✓ | | 200 | 491 | JSON | | | | ✓ | | | 11:04:55 |
| 145 | https | GET | /iizwlm?_=1594371717242 | ✓ | | 200 | 491 | JSON | | | | ✓ | | | 11:01:53 |
| 144 | https | GET | /iizwlm?_=1594371530169 | ✓ | | 200 | 491 | JSON | | | | ✓ | | | 10:58:46 |
| 141 | https | GET | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_... | ✓ | | 200 | 576 | JSON | | | | ✓ | | | 10:55:43 |
| 139 | https | POST | /smartphone/service/v11/privateCustomers/me... | ✓ | | 200 | 1480 | JSON | | | | ✓ | | | 10:55:27 |
| 138 | https | GET | /smartphone/service/v11/privateCustomers/me... | ✓ | | 200 | 870 | JSON | | | | ✓ | | | 10:55:26 |
| 137 | https | POST | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_... | ✓ | | 200 | 805 | JSON | | | | ✓ | | | 10:55:12 |
| 136 | https | POST | /smartphone/service/v11/orders/p2p/send | ✓ | | 200 | 777 | JSON | | | | ✓ | | | 10:55:09 |
| 135 | https | GET | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_... | ✓ | | 200 | 576 | JSON | | | | ✓ | | | 10:55:03 |
| 134 | https | GET | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_... | ✓ | | 200 | 576 | JSON | | | | ✓ | | | 10:54:47 |
| 133 | https | GET | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4_... | ✓ | | 200 | 576 | JSON | | | | ✓ | | | 10:54:17 |
| 132 | https | GET | /smartphone/service/v11/orders?limit=100&pa... | ✓ | | 200 | 18539 | JSON | | | | ✓ | | | 10:53:47 |
| 131 | https | POST | /smartphone/service/v11/privateCustomers/me... | ✓ | | 200 | 1480 | JSON | | | | ✓ | | | 10:53:46 |
| 130 | https | GET | /smartphone/service/v11/privateCustomers/me... | ✓ | | 200 | 870 | JSON | | | | ✓ | | | 10:53:45 |
| 129 | https | GET | /smartphone/service/v11/orders?since=1970-0... | ✓ | | 200 | 50014 | JSON | | | | ✓ | | | 10:53:45 |
| 128 | https | POST | /P2PPaymentSystem/P2PInterfaceP2PLogin/V4... | ✓ | | 200 | 1340 | JSON | | | | ✓ | | | 10:53:45 |

Request | Response

Raw | Params | Headers | Hex | JSON | JSON Beautifier

```
POST /smartphone/service/v11/orders/p2p/send HTTP/1.1
Accept-Encoding: gzip, deflate
Accept: application/json
Accept-Language: fr_CH
X-TWINT-WALLETAPP-LIB-VERSION: 15.3.0.18
Cookie: Navajo=UNBjXYuG2vyu2A3NYol+qgo/M3ThiBT8PhA944Z6Do/24f5NEDkkahF2VEohHy0zNKx2UuZivUg-
Content-Type: application/json; charset=UTF-8
Content-Length: 764
Host: [redacted]
Connection: close
User-Agent: okhttp/3.12.0
ADRUM_1: isMobile:true
ADRUM: isAjax:true

{
  "amount":{
    "amount":20,
    "currency":"CHF"
  },
  "certificateFingerprint":"ef                                417b",
  "moneyReceiver":{
    "firstName"
    "lastName":
  },
  "moneyReceiverMobileNumber":"+4179      ",
  "moneySender":{
    "firstName"
    "lastName":
  },
  "orderUuid":"13976b6e-a57c-448a-8535-51d97f01928d",
  "reservationDate":"2020-07-10T08:55:12",
  "sendMoneyEvenIfCustomerUnknown":true,
  "signature":"gu2DEXJ5pqGx+0c6vQmOcU04MmYqyb+RIHTt8iZ4jHGcul/Jx8iIWVlm6WU64G58oJnnEGH8WArldOmmc61/bZEjOEF3fRXR/2kffAreQNhEO1Uc18sJFxx96iAt3Hfe336yHehB0qZ9zTKgtMZwGu8s3tzJNRpvRszio2QCk5X7SIh26AiO4KD047uFmKEPThC
}
```

# 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

```
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.         }
```

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

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

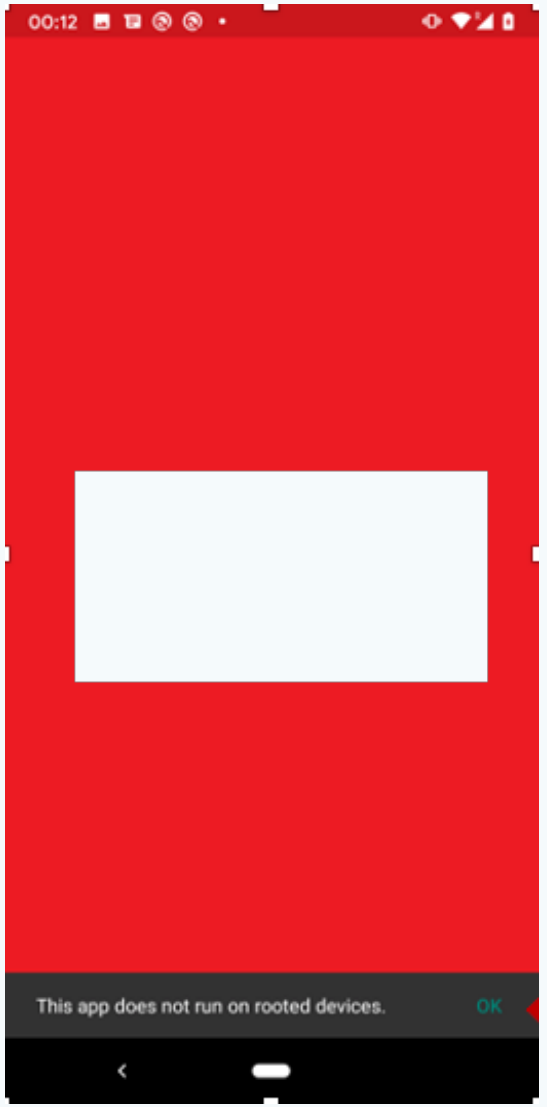
- Watch where the app connects to, use Qualys SSL labs to evaluate configuration, expect a grade of B or more

# 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



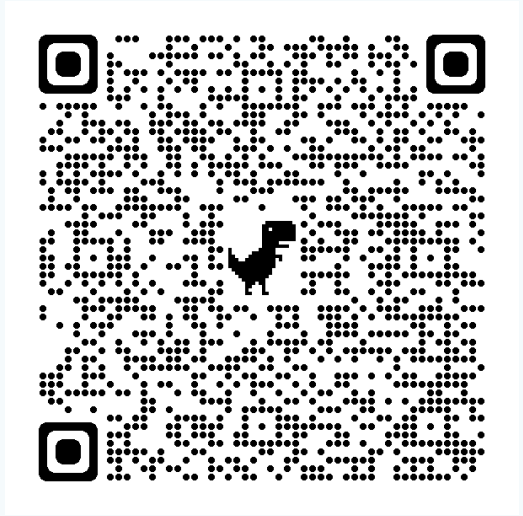
# M9 Reverse engineering

```
            instance.update(str.getBytes());
            return a(instance.digest());
        } catch (NoSuchAlgorithmException unused) {
            return String.valueOf(str.hashCode());
        }
    }

    @TargetApi(9)
    public static boolean b() {
        if (bl.b()) {
            return Environment.isExternalStorageRemovable();
        }
        return true;
    }

    public Bitmap a(String str) {
        dt<String, Bitmap> dtVar = this.d;
        if (dtVar != null) {
            return dtVar.a(str);
        }
        return null;
    }

    public void a() {
        synchronized (this.g) {
            if (this.c == null || this.c.a()) {
                File file = this.f.c;
                if (this.f.g && file != null) {
                    if (!file.exists()) {
                        file.mkdirs();
                    }
```

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



http://www.itu.int/go/dfssl

**Contact:** dfssecuritylab@itu.int

# Thank you!