Mobile Payment Application Security Tests

Arnold Kibuuka, Project Officer, ITU

07 December 2021

Android Attack Points

- ❑ Data Storage
  - Keystores
  - Application Filesystem
  - Application Database
  - Configuration files

- ❑ Binary source code
  - Reverse engineering
  - Look for vulnerabilities in source code
  - Embedded credentials
  - Key generation routines

- ❑ Platform
  - Malware installation
  - Mobile botnets

Data storage, source code and platform are interrelated and a weakness in one can lead to exploitation in another.

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

Elements of the lab used for the tests

Smartphones, one rooted, one not rooted

- Rooting software:
  - Magisk
  - Frida

Workstation

- WiFi adapter to create hotspot
- Android Debug Bridge
- Static analysis software: Mobile Security Framework (MobSF), Androguard
- Interception software: Burp proxy, Bettercap, apk-mitm

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

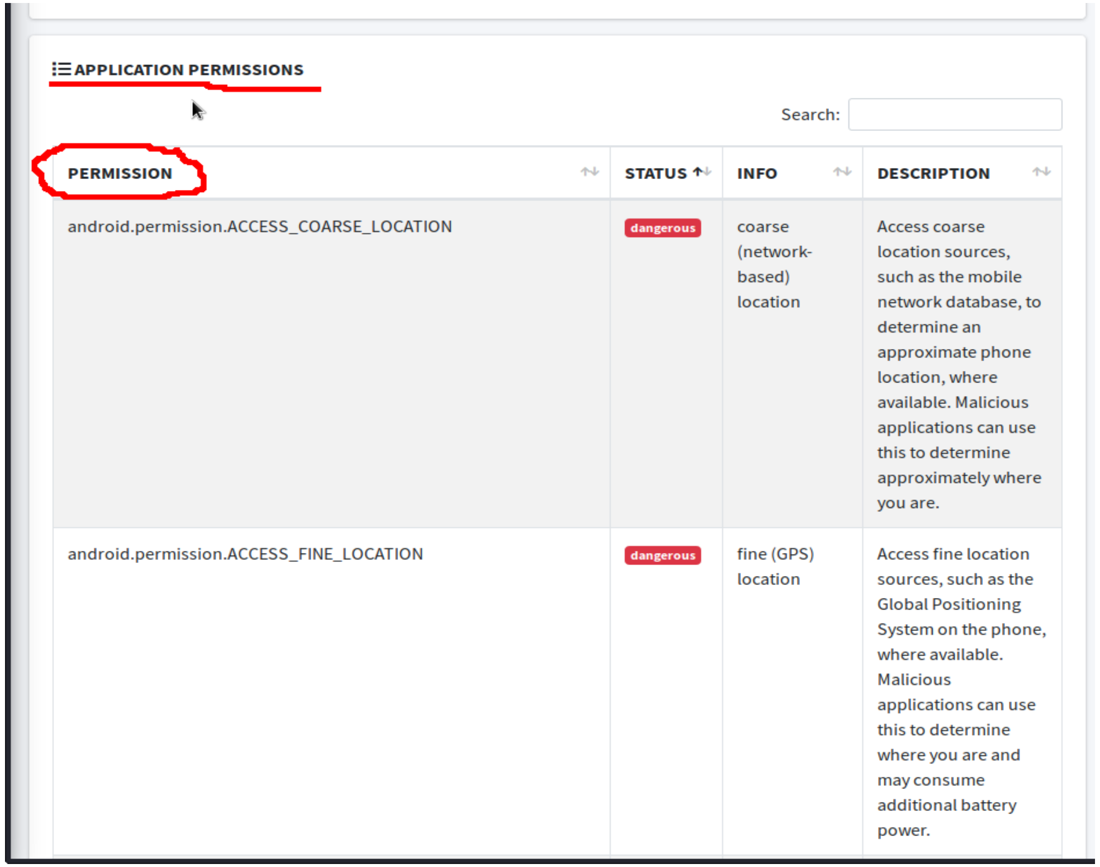
- Debugging features of the application should be disabled

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.

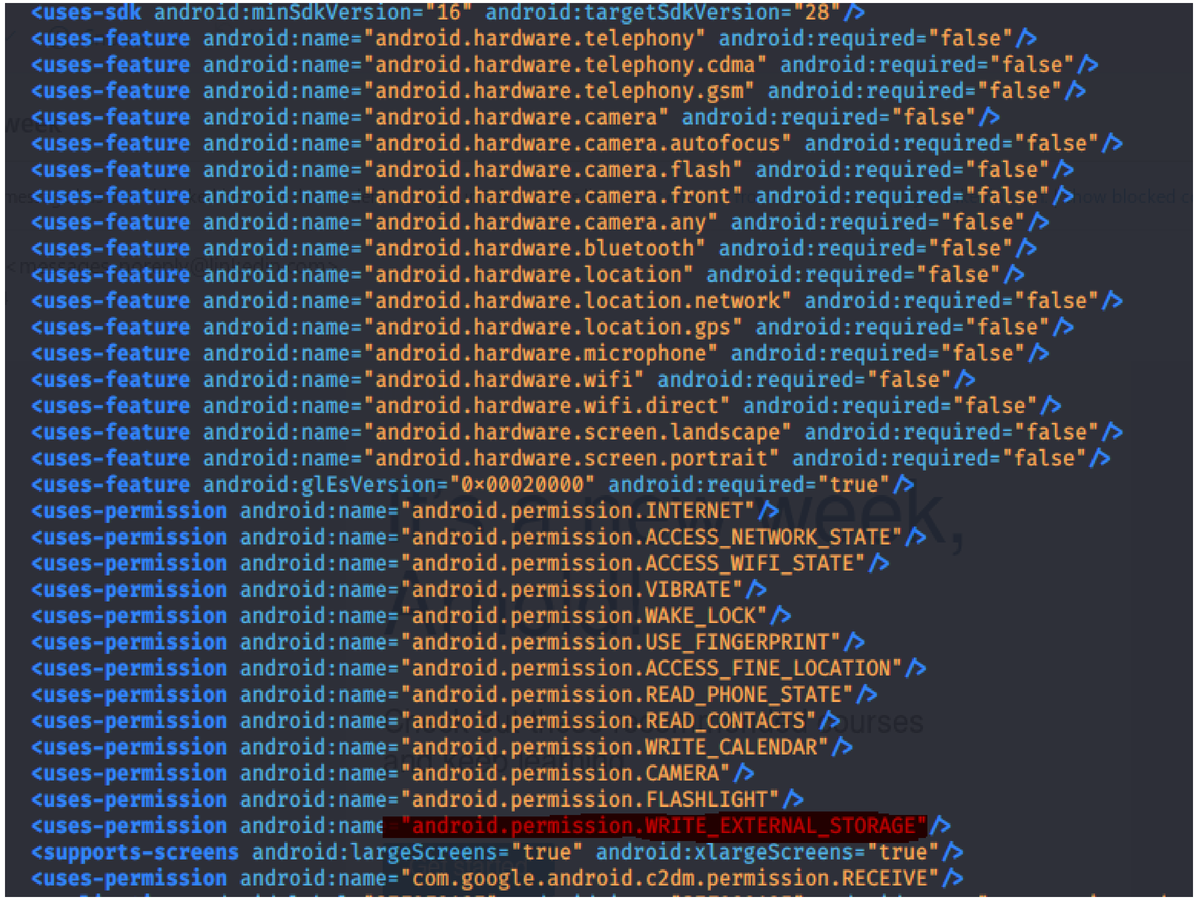


APPLICATION PERMISSIONS

Search:

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

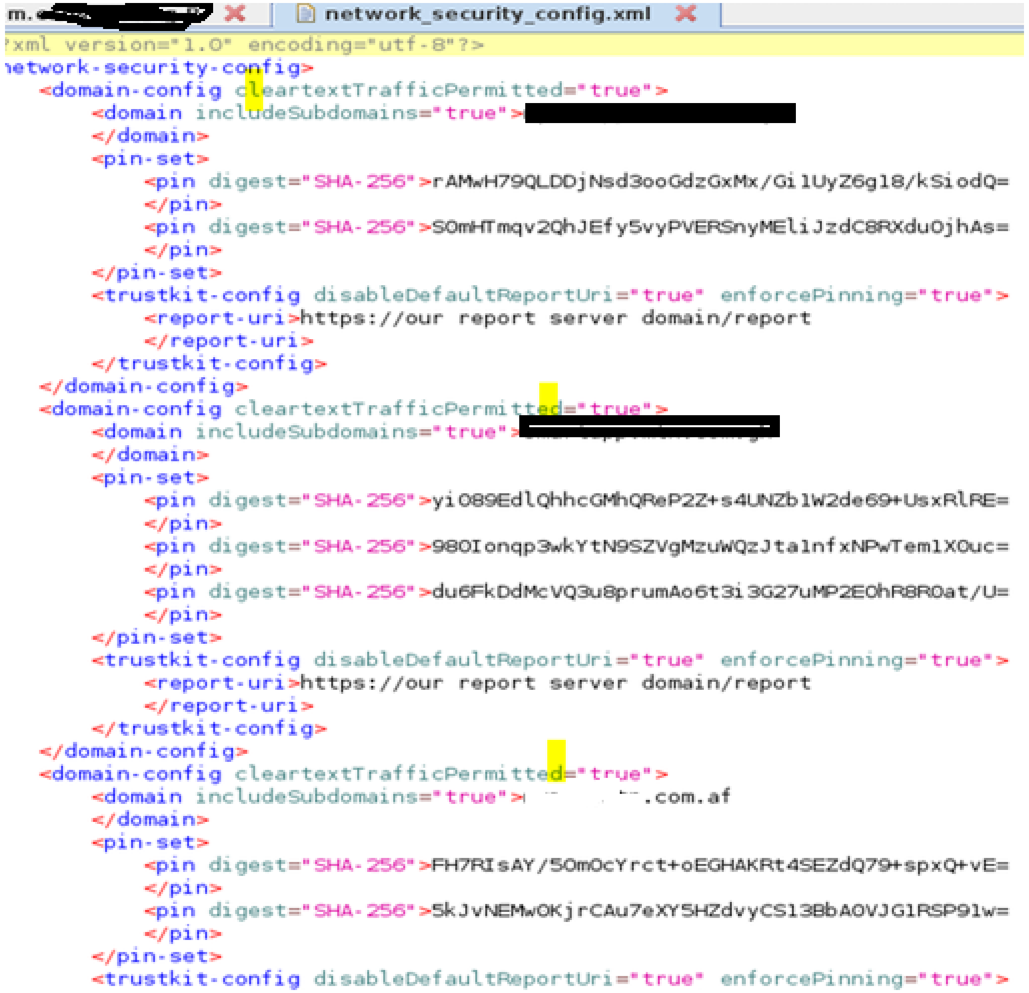
T3.2 Application should detect Machine-in-the-Middle attacks with untrusted Certificates

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

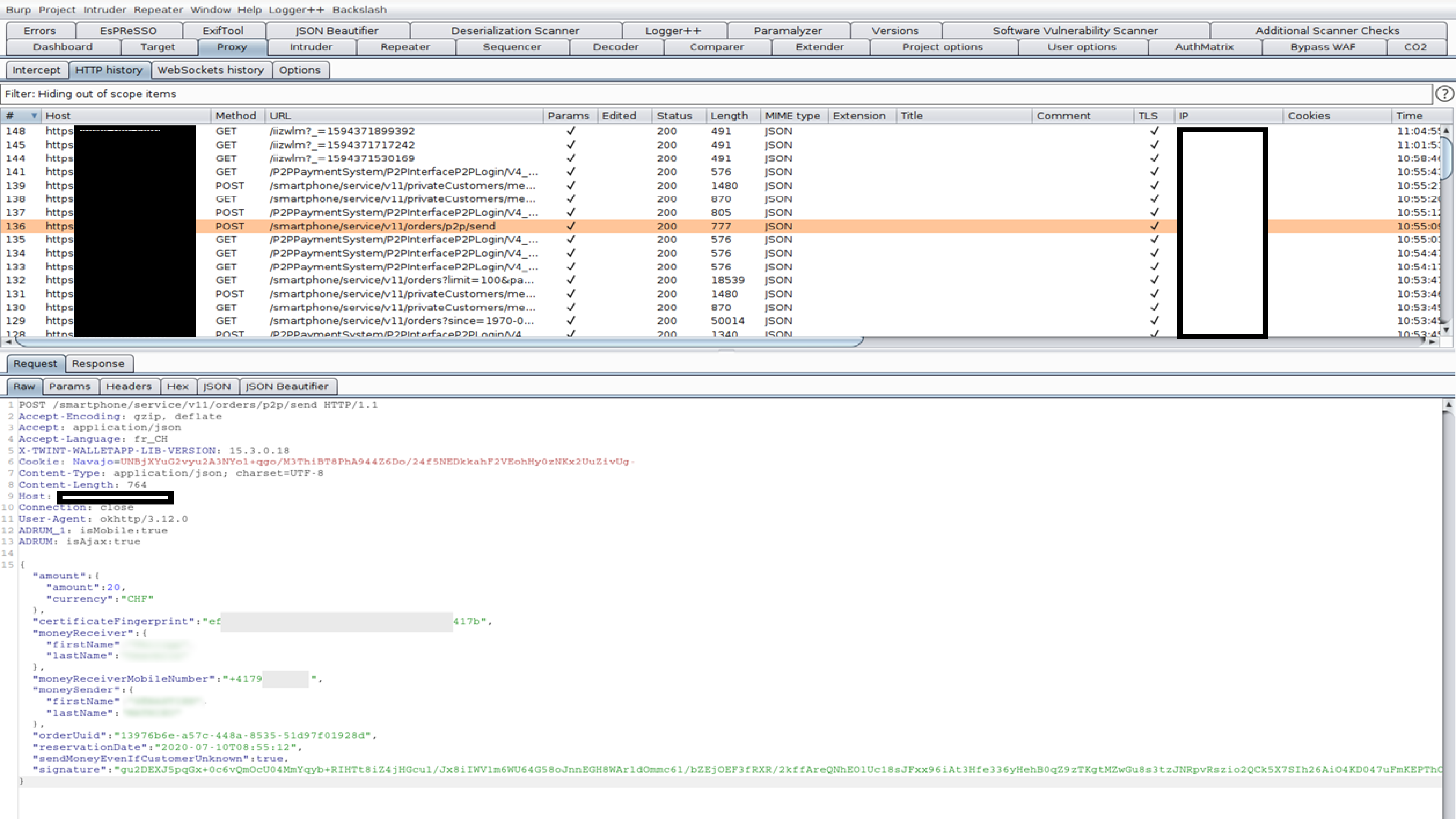
T3.3 Application should detect Machine-in-the-Middle attacks with trusted certificate

- 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



```
?xml version="1.0" encoding="utf-8"?>
etwork-security-config>
  <domain-config cleartextTrafficPermitted="true">
      <domain includeSubdomains="true">[redacted]
      </domain>
      <pin-set>
          <pin digest="SHA-256">rAMwH79QLDDjNsd3ooGdzGxMx/Gi1UyZ6g18/kSiodQ=
          </pin>
          <pin digest="SHA-256">SOmHTmqv2QhJEfy5vyPVERSnyMEliJzdC8RXduOjhAs=
          </pin>
      </pin-set>
      <trustkit-config disableDefaultReportUri="true" enforcePinning="true">
          <report-uri>https://our report server domain/report
          </report-uri>
      </trustkit-config>
  </domain-config>
  <domain-config cleartextTrafficPermitted="true">
      <domain includeSubdomains="true">[redacted]
      </domain>
      <pin-set>
          <pin digest="SHA-256">yi089EdlQhhcGMhQReP2Z+s4UNZb1W2de69+UsxRlRE=
          </pin>
          <pin digest="SHA-256">980IonqpJwkYtN9SZVgMzuWQzJta1nfxNPwTem1XOuc=
          </pin>
          <pin digest="SHA-256">du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U=
          </pin>
      </pin-set>
      <trustkit-config disableDefaultReportUri="true" enforcePinning="true">
          <report-uri>https://our report server domain/report
          </report-uri>
      </trustkit-config>
  </domain-config>
  <domain-config cleartextTrafficPermitted="true">
      <domain includeSubdomains="true">[redacted].com.af
      </domain>
      <pin-set>
          <pin digest="SHA-256">FH7RIsAY/5OmOcYrct+oEGHAKRt4SEZdQ79+spxQ+vE=
          </pin>
          <pin digest="SHA-256">5kJvNEMwOKjrCAu7eXY5HZdvyCS13BbA0VJG1RSP91w=
          </pin>
      </pin-set>
      <trustkit-config disableDefaultReportUri="true" enforcePinning="true">
```



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]		11:04:5
145	https [redacted]	GET	/iizwlm?_=1594371717242	✓		200	491	JSON				✓	[redacted]		11:01:5
144	https [redacted]	GET	/iizwlm?_=1594371530169	✓		200	491	JSON				✓	[redacted]		10:58:4
141	https [redacted]	GET	/P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...	✓		200	576	JSON				✓	[redacted]		10:55:4
139	https [redacted]	POST	/smartphone/service/v11/privateCustomers/me...	✓		200	1480	JSON				✓	[redacted]		10:55:2
138	https [redacted]	GET	/smartphone/service/v11/privateCustomers/me...	✓		200	870	JSON				✓	[redacted]		10:55:2
137	https [redacted]	POST	/P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...	✓		200	805	JSON				✓	[redacted]		10:55:1
136	https [redacted]	POST	/smartphone/service/v11/orders/p2p/send	✓		200	777	JSON				✓	[redacted]		10:55:0
135	https [redacted]	GET	/P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...	✓		200	576	JSON				✓	[redacted]		10:55:0
134	https [redacted]	GET	/P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...	✓		200	576	JSON				✓	[redacted]		10:54:4
133	https [redacted]	GET	/P2PPaymentSystem/P2PInterfaceP2PLogin/V4_...	✓		200	576	JSON				✓	[redacted]		10:54:1
132	https [redacted]	GET	/smartphone/service/v11/orders?limit=100&pa...	✓		200	18539	JSON				✓	[redacted]		10:53:4
131	https [redacted]	POST	/smartphone/service/v11/privateCustomers/me...	✓		200	1480	JSON				✓	[redacted]		10:53:4
130	https [redacted]	GET	/smartphone/service/v11/privateCustomers/me...	✓		200	870	JSON				✓	[redacted]		10:53:4
129	https [redacted]	GET	/smartphone/service/v11/orders?since=1970-0...	✓		200	50014	JSON				✓	[redacted]		10:53:4
128	https [redacted]	POST	/P2PPaymentSystem/P2PInterfaceP2PLogin/V4	✓		200	1340	JSON				✓	[redacted]		10:53:4

~~~
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=UNBjXYuG2vyu2A3NYo1+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[redacted]417b",
  "moneyReceiver":{
    "firstName"[redacted]
    "lastName":[redacted]
  },
  "moneyReceiverMobileNumber":"+4179[redacted]",
  "moneySender":{
    "firstName"[redacted]
    "lastName":[redacted]
  },
  "orderUuid":"13976b6e-a57c-448a-8535-51d97f01928d",
  "reservationDate":"2020-07-10T08:55:12",
  "sendMoneyEvenIfCustomerUnknown":true,
  "signature":"gu2DEXJ5pqGx+0c6vQmOcU04MmYqyb+RIHTt8iZ4jHGcul/Jx8iIWV1m6WU64G58oJnnEGH8WAr1dOmmc61/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

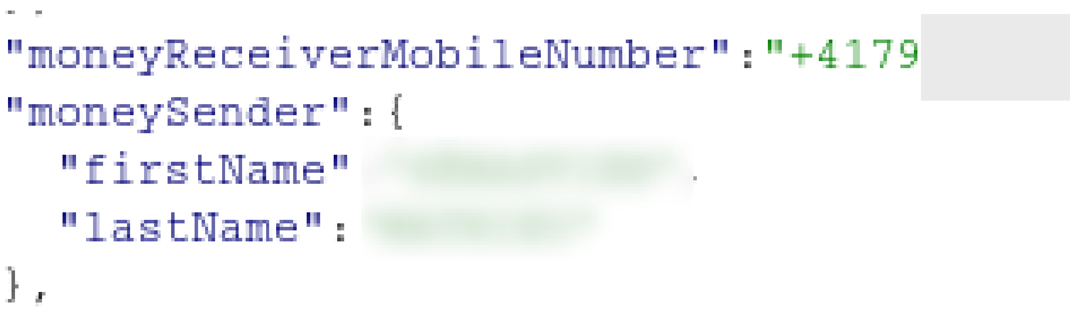
T4.3 If a new fingerprint is added, authentication with fingerprints should be temporarily disabled

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

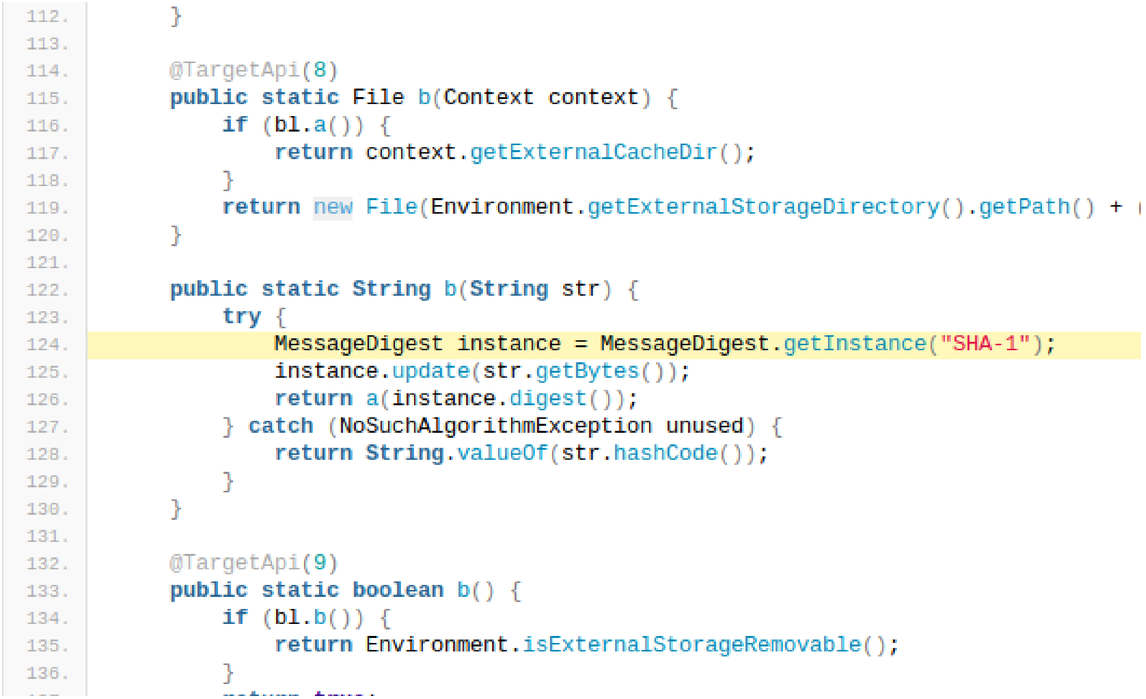
T4.4 It should not be possible to replay intercepted requests (e.g. a money transfer)

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

M5: Insufficient Cryptography



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



```
    }

    @TargetApi(8)
    public static File b(Context context) {
        if (bl.a()) {
            return context.getExternalCacheDir();
        }
        return new File(Environment.getExternalStorageDirectory().getPath() +
    }

    public static String b(String str) {
        try {
            MessageDigest instance = MessageDigest.getInstance("SHA-1");
            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();
        }
```

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

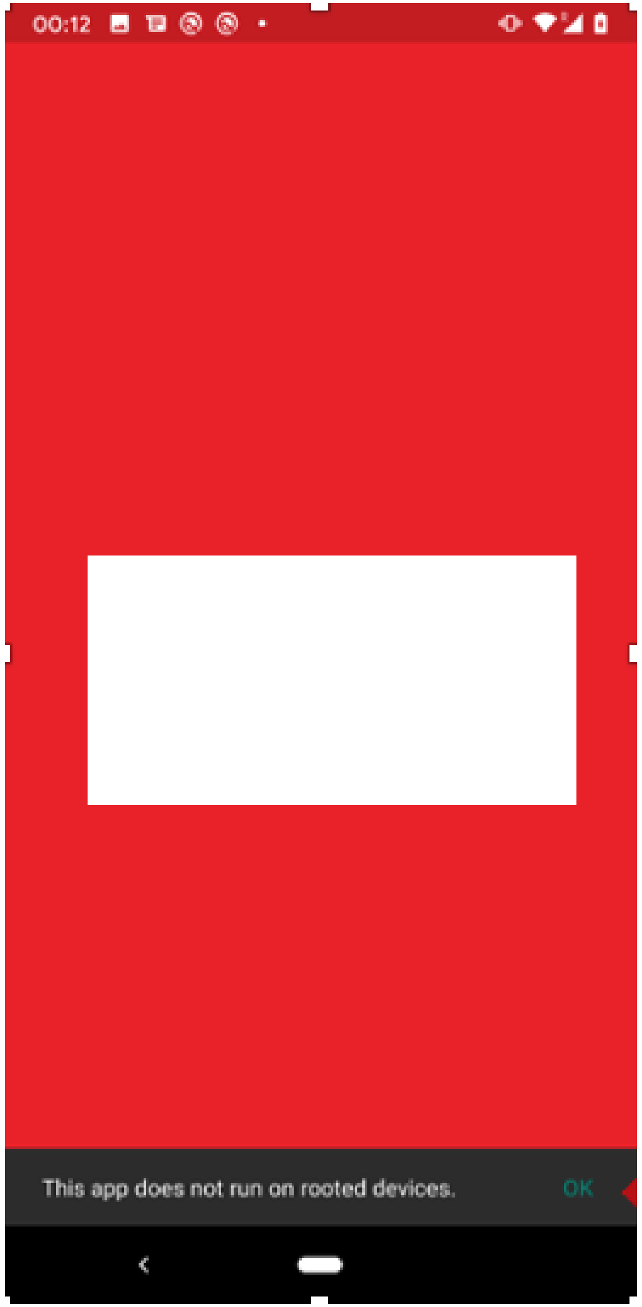
- Watch where the app connects to, use Qualys SSL labs to evaluate configuration, expect a grade of B or more

M8: Code Tampering

Prevent an attacker from tampering the code on the telephone

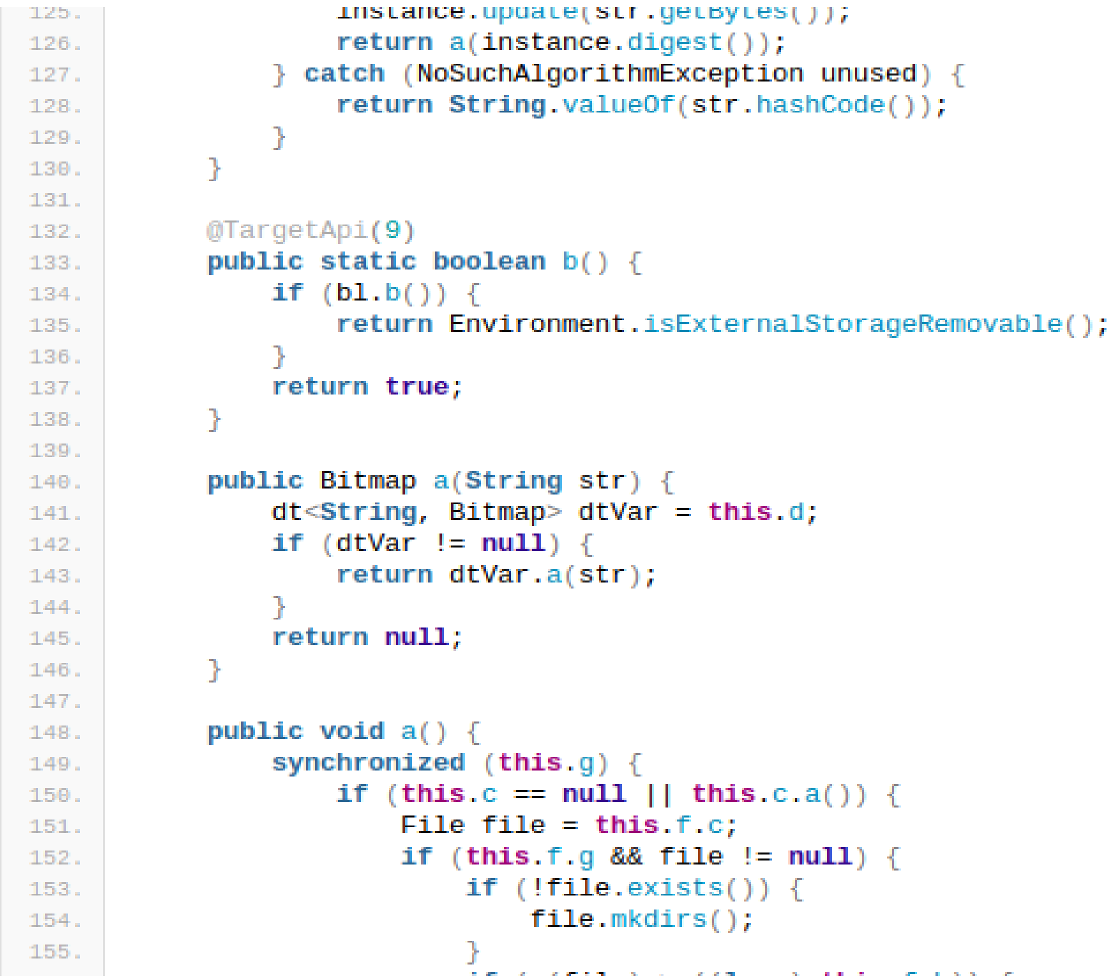
T8.1 The application should refuse to run on a rooted device

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



This app does not run on rooted devices.

M9 Reverse engineering

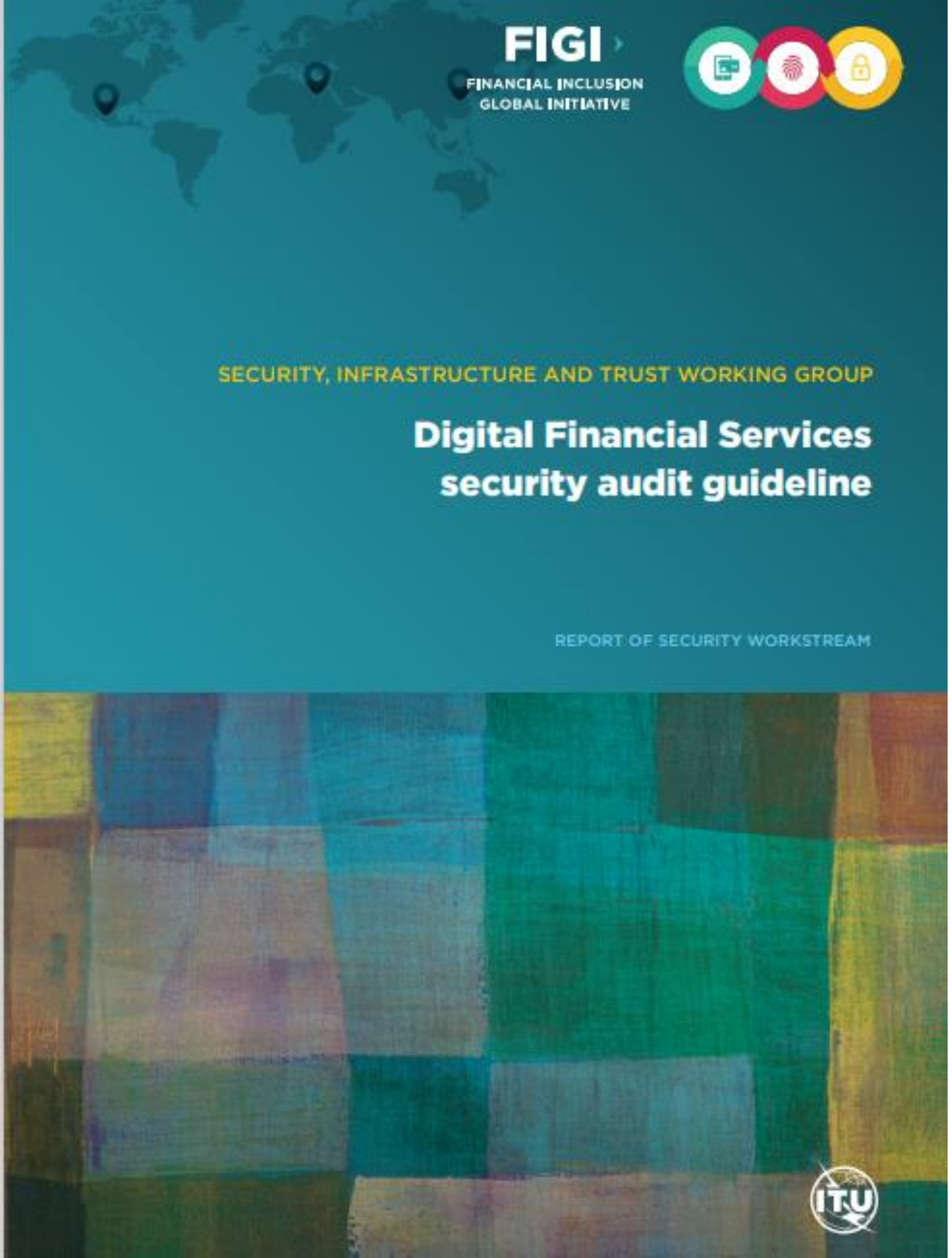


```
            instance.update(str.getBytes());
            return a(instance.digest());
        } catch (NoSuchAlgorithmException unused) {
            return String.valueOf(str.hashCode());
        }
    }

    @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



FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services
security audit guideline

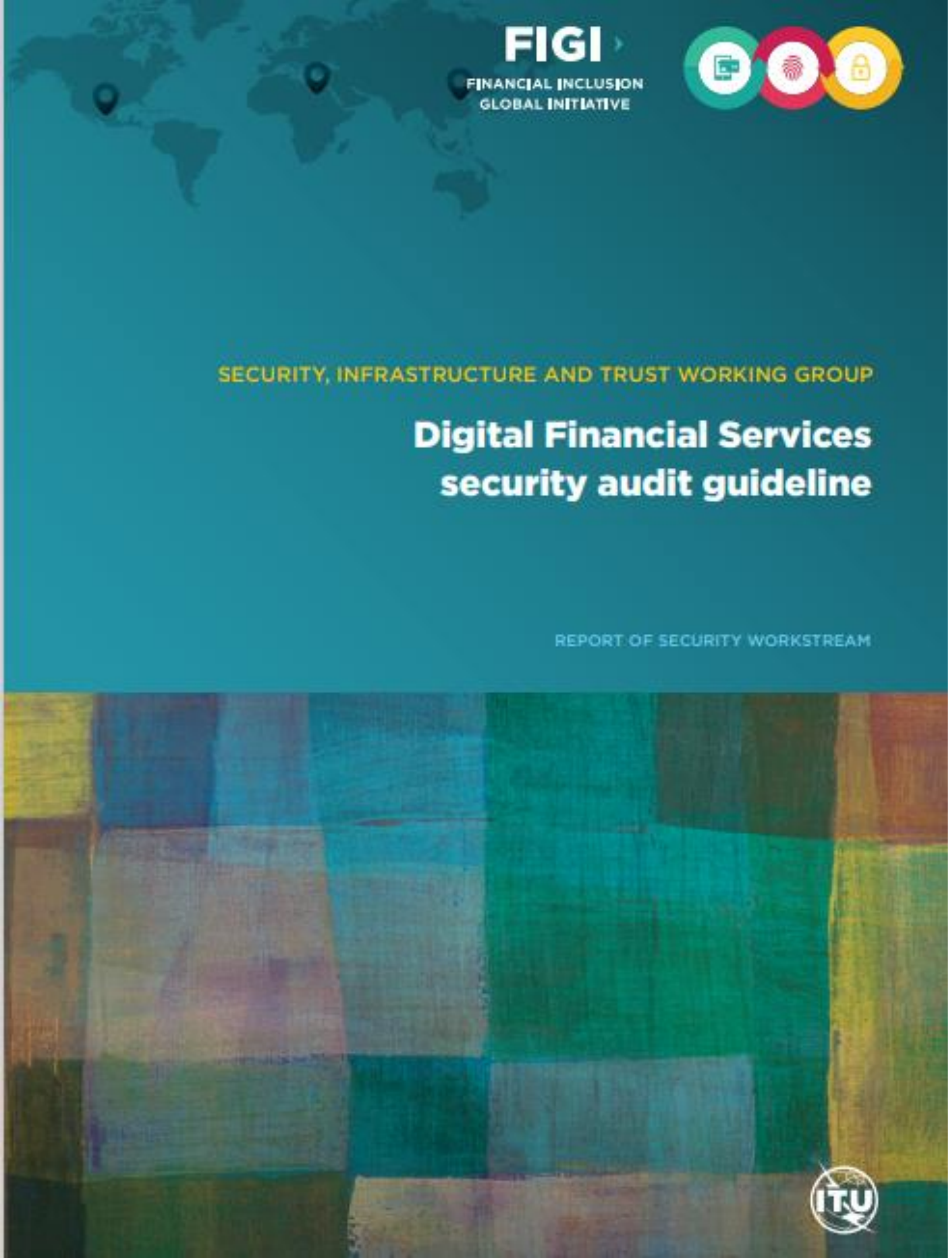
REPORT OF SECURITY WORKSTREAM

ITU

Tests summary

Template For Application Security Best Practices	Corresponding tests
9.1 Device integrity	T1.2 Android:debuggable T1.4 Dangerous permissions 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 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
9.3 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

www.figi.itu.int/figi-resources/dfs-security-lab/



FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services
security audit guideline

REPORT OF SECURITY WORKSTREAM

Tests summary

Template for application security best practices	Corresponding tests
9.4 Secure Data Handling	T1.1 Android:allowBackup T1.3 Android:installLocation T2.1 Android.permission.WRITE_EXTERNAL_STORAGE 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

JSSD 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/

ITU

www.itu.int