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.

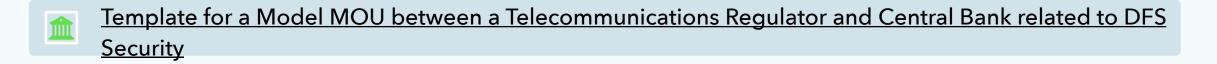
Recap: DFS Security Recommendations



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



<u>Recommendations to mitigate SS7 vulnerabilities</u>







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

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

connections

T3.3 Application should detect Machine-inthe-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



Handling

.....

Secure Application Development

T9.1 The code of the app should be obfuscated

T1.1 Android:allowBackup T1.3 Android:installLocation T2.1 Android.permission.WRIT E_EXTERNAL_STORAGE T2.2 Disabling screenshots

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

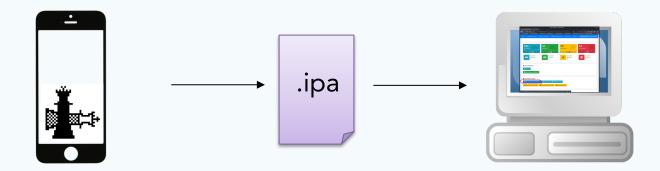
EQUIPMENT	QTY	COMMENT	TESTS
Desktop/laptop	2	32 GB RAM, 1TB, 4+ core 64-bit processor	All
Mobile smartphone (Android OS).	2	Google Pixel	Android
Wi-Fi router	1		All
iOS Device	2	(One of the iPhones MUST run iOS 14)	iOS
Kali Linux		Opensource	All
Wireshark		Opensource	All
Magisk		Opensource	All
Frida		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.		10	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

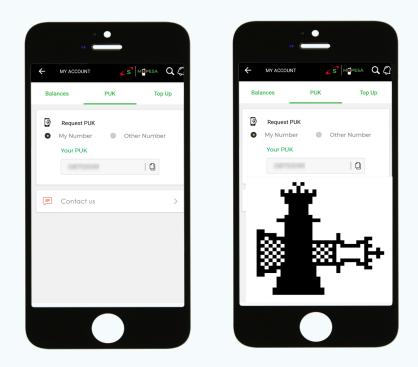
Static tests

- 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.

N	Search:						
PERMISSION	↑↓ STATUS	t INFO ↑	DESCRIPTION				
android.permission.ACCESS_COARSE_LOCATION	dangerou	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	dangerou	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-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="0×00020000" 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 <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

D	ors EsPReSSO	ExifTool	JSON Bea	utifier	Deserialization S	canner	Logger++	P	Paramalyzer	Versions	Software Vulneral	bility Scanner		Additional Scanner Ch	ecks
	ashboard Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Co	mparer	Extender	Project optic	ons User op	tions	AuthMatrix	Bypass WAF	CC
erc	ept HTTP history WebSe	ockets history	Options												
r: F	Hiding out of scope items														
	Host	Method				Params Edited	Status		MIME type Exter	nsion Title	Comment	t TLS	IP	Cookies	Tin
	https	GET	/iizwlm?_=159			1	200	491	JSON			1			11:
	https	GET	/iizwlm?_=159			1	200	491	JSON			1			11:
	https https	GET	/iizwlm?_=159		ceP2PLogin/V4	1	200	491 576	JSON JSON			1			10
	https	POST			eCustomers/me	1	200	1480	ISON			1	1		10
	https	GET			eCustomers/me	1	200	870	ISON			1			10
	https	POST			ceP2PLogin/V4	1	200	805	JSON			1			10
	https	POST		ervice/v11/orders		1	200	777	JSON			1			10
	https	GET			ceP2PLogin/V4	1	200	576	JSON			~			10
	https	GET			ceP2PLogin/V4	~	200	576	JSON			1			10
	https	GET			ceP2PLogin/V4	1	200	576	JSON			1	1		10
	https	GET POST			?limit=100&pa	1	200	18539 1480	JSON JSON			1			10
	https	GET			eCustomers/me eCustomers/me	1	200	870	ISON			~			10
	https	GET			?since=1970-0	1	200	50014	ISON			1			10
	https	POST		vstem/P2PInterfa		1	200	1340	ISON					_	10
			N Beautifier												
POST	T /smartphone/service/v ept-Encoding: gzip, dev ept: application/json	v11/orders/		P/1.1											
	T /smartphone/service/v ept-Encoding: gzip, der ept: application/json ept-Language: fr_CH WINT-WALLETAPP-LIB-VERS	v11/orders/; flate SION: 15.3.	p2p/send HTT1 0.18												
	T /smartphone/service/v ept-Encoding: gzip, dei ept: application/json ept-Language: fr_CH WINT WALLETAPP-LIB-VER(kie: Navajo=UNBjXYuG2vy	v11/orders/ flate SION: 15.3. yu2A3NYo1+q	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkahF2VEohHy	0zNKx2UuZivUg-									
	T /smartphone/service/v ept-Encoding: gzip, der ept: application/json ept-Language: fr_CH WINT-WALLETAPP-LIB-VERS	v11/orders/ flate SION: 15.3. yu2A3NYo1+q	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkahF2VEohHy	0zNKx2UuZivUg-									
	<pre>/ /smartphone/service/ ept:Encoding:gzip.dei ept:application/json ept:Language:fr_CH NINT-WALLETAPP-LIB-VERK kie: Navajo=UNBjXYuG2vy tent-Type: application, tent-Length: 764 t:</pre>	v11/orders/ flate SION: 15.3. yu2A3NYo1+q	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkahF2VEohHy	0zNKx2UuZivUg-									
	<pre>T /smartphone/service/ ept-Encoding; gzip, dej ept: application/json ept-Language: fr_CH WINT-WALLETAPP-LIB-VERK kie: Navajo=UNBjXYuG2vy tent-Type: application, tent-Length: 764 t: nection: close</pre>	SION: 15.3. yu2A3NYol+q /json; char	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkahF2VEohHy	0 zNKx2UuZivUg -									
	<pre>/ smartphone/service/ opt-Encoding: gzip, det ept: application/json ept-language: fr_CH MINT-MALLETAPP-LIB-VER kie: Navajo=UNBjXYuG2vy tent-Type: application, tent-Length. 754 t: tent-Length.754 t: ection: close r-Agent; okhttp/3.12.0</pre>	SION: 15.3. yu2A3NYol+q /json; char	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkahF2VEohHy	0zNKx2UuZivUg-									
	<pre>/ smartphone/service/ ept-Encoding: gzip, de ept-language: fr_CH WINT-WALLETAPP.LIB-VER Kie: Navajo-UNBSYY0027- tent-Type: application, tent-Length: 764 ection: close r-Agent: okhtp/3.12.0</pre>	SION: 15.3. yu2A3NYol+q /json; char	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkah F2 VEohHy	02NKx2UuZivUg-									
	<pre>/ smartphone/service/ opt-Encoding: gzip, det ept: application/json ept-language: fr_CH MINT-MALLETAPP-LIB-VER kie: Navajo=UNBjXYuG2vy tent-Type: application, tent-Length. 754 t: tent-Length.754 t: ection: close r-Agent; okhttp/3.12.0</pre>	SION: 15.3. yu2A3NYol+q /json; char	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkahF2VEohHy	0zNKx2UuZivUg-									
ont ont ont ont ont ont ont ont ont ont	<pre>/ smartphone/service/ opt-Encoding: gzip, det ept: application/json ept-language: fr_CH MINT-MALLETAPP-LIB-VER kie: Navajo=UNBjXYuG2vy tent-Type: application, tent-Length. 754 t: tent-Length.754 t: ection: close r-Agent; okhttp/3.12.0</pre>	SION: 15.3. yu2A3NYol+q /json; char	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkahF2VEohHy	0zNKx2OuZivOg-									
IST ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice The ice ice ice ice ice Ice Ice Ice Ice Ice Ice Ice Ice Ice I	<pre>7 /martphone/service/ ppt-Bnoding: wrip.de ppt-Application/json ppt-Application/json ppt-Application/json ppt-Application, test:Napplication, test:Napplication, test:Napplication, test:Long-loss r-Agent: okhttp/3:12.0 Wi_l:iskbietrue UM: iskbietrue UM: iskbietrue IM: iskjaxitrue</pre>	SION: 15.3. yu2A3NYol+q /json; char	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDkkahF2VEohHy	0 zNKx20uZivUg-									
Ce C	<pre>7 /martphone/service/ ppt-Bnoding: wrip.de ppt-Application/json ppt-Application/json ppt-Application/json ppt-Application, test:Napplication, test:Napplication, test:Napplication, test:Long-loss r-Agent: okhttp/3:12.0 Wi_l:iskbietrue UM: iskbietrue UM: iskbietrue IM: iskjaxitrue</pre>	vil/orders/; flate SION: 15.3. yu2A3MYol+q /json; char	p2p/send HTTP 0.18 go/M3ThiBT8PP		NEDKKahF2VEohHy 417b*,	02NKX2UuZivUg-									
ST CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC	<pre>7 /martphone/service/ ppt-Encoding; uzip, de ppt-Indrugaer fr.CH HINT-KALLETAPP-LIN-VER HINT-KALLETAPP-LIN-VER tent-Length-FLIN-VER tent-Length-Gase -Agent: okhttp/3.12.0 Williskolletrue OK: iskjax:true amount*:("amount*:0, "amount*:0, "amount*:0,</pre>	vil/orders/; flate SION: 15.3. yu2A3MYol+q /json; char	p2p/send HTTP 0.18 go/M3ThiBT8PP			OzNKx2UuZivUg-									
RI P	<pre>/ /mattphone/service/ / /mattphone/service/ / /mattphone/service/ pp: appuges fr_dH MINT MALLETAPP-LIS-VEW tent-Type: application tent.tength: 764 t: mattphicks //mattphicks //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattphick //mattp</pre>	":"ef	p2p/send HTT/ 0.18 go/MJThiBT8P! set=UTF-8			0zNKx2UuZivUg-									
RT)	<pre>7 /martphone/service/ ppt-Encoding; grip, dep is application/sec Mitr MallintAPP-LIE-VEE tent.Pope: application tent.Pope: application tent.Length; 764 t; enturned tent. exclose icose exclose icose c.Agent: okhttp/3.12.0 (M_1) is%bolietrue UM; isÅjaxitrue amount*:("amount*:0, "aurency":"CEP" evurrency":"CEP" "istName"; "istName"; "istName"</pre>	<pre>U1/ordrs/ flate SION: 15.3. yu2A3WY01-q /json; char ":"ef ber":"+4179</pre>	p2p/send HTT/ 0.18 go/MJThiBT8P! set=UTF-8			OzNKx2UuZivUg-									
SSI CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC	<pre>7 /martphone/service/ ppt splat up. / ppt splat up. / ppt splat up. / ppt splat up. / ppt splat up. / / / / / / / / / / / / / / / / / / /</pre>	11/07ders/ 11/07ders/ 11ate STON: 15.3. yu233W201-g yjson; char *:*ef ber*:*+4179	p2p/send HTT/ 0.18 go/NTTN1BTSPP set=UTF-8	544426Do/24f5		OzNKx2UuZivUg-									

Burp Project Intruder Repeater Window Help Logger++ Backslash

Errors EsPReSSO ExifTo		ExifTool	JSON Beaut	tifier	Deserialization Scann	Logger++	Paramalyzer		Versions	Software Vulnerability Scanner				Additional Scanner Checks			
Dashboard		Target	Proxy	Intruder Repeat		Sequencer	Sequencer Decoder		Comparer Exten		Project options		User options Auth		atrix	Bypass WAF	CO2
Intercept HTTP history WebSockets history		Options															

Filter: Hiding out of scope items										?					
# •	Host	Met	od 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				~			11:01:5:
144	https	GET	/iizwlm?_=1594371530169	~		200	491	JSON				~			10:58:46
141	https	GET	/P2PPaymentSystem/P2PInterfac	eP2PLogin/V4 🗸		200	576	JSON				~			10:55:4:
139	https	POS	/smartphone/service/v11/private0	Customers/me 🗸		200	1480	JSON				~			10:55:2
138	https	GET	/smartphone/service/v11/private0	Customers/me 🗸		200	870	JSON				~			10:55:20
137	https	POS	/P2PPaymentSystem/P2PInterfac	eP2PLogin/V4 🗸		200	805	JSON				~			10:55:1:
136	https	POS	/smartphone/service/v11/orders/;	p2p/send ✓		200	777	JSON				~			10:55:05
135	https	GET	/P2PPaymentSystem/P2PInterfac	eP2PLogin/V4 🗸		200	576	JSON				~			10:55:0:
134	https	GET	/P2PPaymentSystem/P2PInterfac	eP2PLogin/V4 V		200	576	JSON				~			10:54:4:
133	https	GET	/P2PPaymentSystem/P2PInterfac	eP2PLogin/V4 V		200	576	JSON				~			10:54:11
132	https	GET	/smartphone/service/v11/orders?	limit=100&pa ✓		200	18539	JSON				~			10:53:4:
131	https	POS	/smartphone/service/v11/private0	Customers/me 🗸		200	1480	JSON				~			10:53:40
130	https	GET	/smartphone/service/v11/private0	Customers/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	POS	/P2PPavmentSystem/P2PInterfac	eP2PLoninA/4 J		200	1340	ISON	,			7			10.53.4

Request Response

Raw	Params Headers Hex JSON JSON Beautifier	
1 PO	ST /smartphone/service/v11/orders/p2p/send HTTP/1.1	
	cept-Encoding: gzip, deflate	- m
	cept: application/json	
	cept-Language: fr_CH	
	TWINT-WALLETAPP-LIB-VERSION: 15.3.0.18	
	okie: Navajo=UNBjXYuG2vyu2A3NYol+qgo/M3ThiBT8PhA944Z6Do/24f5NEDkkahF2VEohHy0zNKx2UuZivUg-	
	ntent-Type: application/json; charset=UTF-8	
	ntent-Length: 764	
	st:	
	nection: close	
	er-Agent: okhtp/3.12.0	
	RUM_1: iMobile:true	
	RUM_ isJaxificture RUM: isJaxificture	
14	ROM: ISAJAXICIGE	
15 {		
	"amount": (
	"amount": 20,	
	"currency": "CHF"	
	<pre>/, "certificateFingerprint":"ef 417b",</pre>	
	"moneyReceiver": {	
	"firstName"	
	"lastName":	
	1.	
	"moneyReceiverMobileNumber":"+4179 ",	
	"moneySender": {	
	"firstName"	
	"lastName":	
	3.	
	"orderUuid": "13976b6e-a57c-448a-8535-51d97f01928d",	
	"reservationDate":"2020-07-10T08:55:12",	
	"sendMoneyEvenIfCustomerUnknown":true,	
	"signature": "gu2DEXJ5pqGx+0c6vQm0cU04MmYqyb+RIHTt8iZ4jHGcu1/Jx8iIWV1m6WU64G58oJnnEGH8WAr1d0mmc61/bZEj0EF3fRXR/2kffAreQNhE01Uc18sJFxx96iAt3Hfe336yHehB0qZ9zTKgtMZwGu8s3tzJNRpvRszio2QCk5X7SIh26Ai04KD047uFmKEPT	hC
}		

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

```
@TargetApi(8)
114.
           public static File b(Context context) {
115.
116.
               if (bl.a()) {
                   return context.getExternalCacheDir();
118.
               return new File(Environment.getExternalStorageDirectory().getPath() +
119.
120.
           public static String b(String str) {
               try
                   MessageDigest instance = MessageDigest.getInstance("SHA-1");
124.
                   instance.update(str.getBytes());
                   return a(instance.digest());
               } catch (NoSuchAlgorithmException unused) {
                   return String.valueOf(str.hashCode());
129.
           @TargetApi(9)
           public static boolean b() {
               if (bl.b()) {
134.
                   return Environment.isExternalStorageRemovable();
136.
               nature truck
```

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

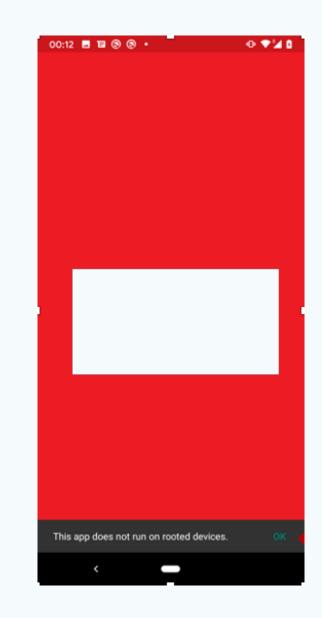
 Watch where the app connects to, use Qualys SSL labs to evaluate configuration, expect a grade of B or more

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



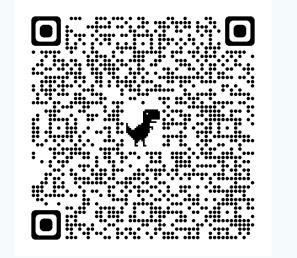
M9 Reverse engineering

```
instance.update(str.getBytes());
126.
                   return a(instance.digest());
               } catch (NoSuchAlgorithmException unused) {
                   return String.valueOf(str.hashCode());
128.
129.
           @TargetApi(9)
           public static boolean b() {
134.
               if (bl.b()) {
                   return Environment.isExternalStorageRemovable();
136.
               return true;
138.
139.
140.
           public Bitmap a(String str) {
               dt<String, Bitmap> dtVar = this.d;
               if (dtVar != null) {
                   return dtVar.a(str);
144.
               return null;
146.
147.
           public void a() {
148.
               synchronized (this.g) {
150.
                   if (this.c == null || this.c.a()) {
                        File file = this.f.c;
                        if (this.f.g && file != null) {
                            if (!file.exists()) {
154.
                                file.mkdirs();
                            te a aere su are sur ensur ensur
```

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!