



Mobile threats incident handling

Toolset, Document for students





European Union Agency for Network and Information Security



About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at <u>www.enisa.europa.eu</u>.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use <u>CERT-Relations@enisa.europa.eu</u>

For media enquires about this paper, please use press@enisa.europa.eu.



Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.



Table of Contents

1	What Will You Learn	1
2	Exercise Task	1
2.1	Task 1: Familiarisation with Android, AVD, and ADB	1
2.2	Task 2: Cloning an Application	8
2.3	Task 3: Analysing Cloned Application	14
2.4	Task 4: Analysing Simplelocker	16
2.5	Task 5 (Optional): Analysing Other Artifacts	16
3	Conclusion	18



1 What Will You Learn

Mobile devices add some additional conditions for the investigator. First, access to the device might be difficult (geography, Bring Your Own Device (BYOD), and other privacy issues). Data access and investigation tools used in other environments might not be working. It might be necessary to adjust implemented incident-handling processes to adapt to these specific platforms. This course will serve as an introduction to Mobile Technologies, and Incident Handling within this field.

2 Exercise Task

The Students will be given 5 main tasks:

- 1. Familiarisation with Android, AVD, and ADB
- 2. Cloning an Application
- 3. Analysing Cloned Application
- 4. Analysing Simplelocker
- 5. (Optional) Analysing Other Artifacts

2.1 Task 1: Familiarisation with Android, AVD, and ADB

2.1.1 Open Android SDK Manager

- cd /android/adt-bundle-linux-x86-20140702/sdk/tools
- ./android

😣 🖻 💷 Android SDK Manager					
SDK Path: /tmp/android-sdk-linux					
Packages					
🖷 Name	API	Rev.	Status		
🔻 🗆 🧰 Tools					
Android SDK Tools		16	🎒 Installed		
🗆 🐳 Android SDK Platform-tools		10	🖊 Not installed		
🔻 🖉 🖹 Android 4.0.3 (API 15)					
🖉 🚞 Documentation for Android SDK	15	1	🖊 Not installed		
🗹 👾 SDK Platform	15	2	🖊 Not installed		
Samples for SDK	15	1	🖊 Not installed	1	
🗹 🟺 ARM EABI v7a System Image	15	1	🖊 Not installed		
🛯 🙀 Google APIs by Google Inc.		1	🖊 Not installed		
🗹 🖻 Sources for Android SDK	15	1	🖊 Not installed		
🕨 🗆 🗃 Android 4.0 (API 14)					
▶ □ 🗟 Apdroid 2.2 (ADI 12)					
Show: 🗹 Updates/New 🗹 Installed 🗌 Obsolete Select <u>New</u> or <u>Updates</u> Install 6 pi					
Sort by: API level Repository Deselect All					
Done loading packages					

Figure 1: Android SDK Manager

2.1.2 Open Android AVD Manager

- cd /android/adt-bundle-linux-20140702/sdk/tools/
- android avd



and the second sec					
Target:	Android 2.3.3 -	API Lev	el 10		
CPU/ABI:	ARM (armeabi)				
SD Card:	Size: 200				MiB 💲
	○ File:				Browse
Snapshot:	Enabled				
Skin:	Built-in:	Defa	ult (WVGA800)	:
	O Resolution:			x	
Hardware:	Property		Value		New
	Abstracted LC	D densi	240		Delete
	Max VM appli	cation h	24		Detere
	Device ram siz	e	256		

Figure 2: Android AVD Manager

2.1.3 Browse /home/enisa/.android

<u>Desktop</u> <u>OS</u>	AVD Data Location
<u>Ubuntu</u>	<pre>/home/<username>/.android/</username></pre>
Max OS X	/Users/ <username>/.android</username>
<u>Windows</u> 7	<u>C:\Users\<username>\.android</username></u>

2.1.4 Browse Enisa AVD folder

- cache.img: disk image of /cache partition
- **sdcard.img**: disk image of SD card (if created during AVD setup)
- userdata-qemu.img: disk image of /data partition



2.1.5	Create an AVD nar	ned "SimpleLockerA	VD" using a	vd managei
2.1.3	Create an AVD har	ieu Jilipielockeir	vu using a	vu managei

🚯 Create nev	v Android Virtual Device (AVD) $-$ + \times			
AVD Name:	SimpleLockerAVD			
Device:	Nexus 7 (2012) (7.0", 800 × 1280: tvdpi) 🗘			
Target:	Android 4.0.3 - API Level 15			
CPU/ABI:	ARM (armeabi-v7a) 2			
Keyboard:	🥑 Hardware keyboard present			
Skin:	WXGA800-7in ‡			
Front Camera:	None ‡			
Back Camera:	None ‡			
Memory Options:	RAM: 256 VM Heap: 32			
Internal Storage:	200 MiB ‡			
SD Card:	• Size: 100 MiB ‡			
	O File: Browse			
Emulation Options:	Snapshot Use Host GPU			
Override the existing AVD with the same name				
	Cancel OK			

Figure 3: Create AVD

2.1.6 Add Hardware and open AVDs

- Modify Nexus 7 Hardware by Cloning Device and modifying the features
- Add GPS to Enisa AVD (Edit) using AVD Manager

ndroid	Virtual Devices Device Definitions	
ist of k	known device definitions. This can later be used to create A	ndroid Virtual Devices.
Device		Create AVD
	Nexus 10 by Google Screen: 10.1", 2560 × 1600, X-Large xhdpi RAM: 1907 MiB	Create Device
	Nexus 4 by Google Screen: 4.7", 768 × 1280, Normal xhdpi RAM: 1907 MiB	Clone Doloto Edit an existing device definit
	Nexus 5 by Google Screen: 5.0", 1080 × 1920, Normal xxhdpi RAM: 2 GiB	Detete
	Nexus 7 by Google Screen: 7.0", 1200 × 1920, Large xhdpi RAM: 2 GiB Used by: SimpleLockerAVD	
	Nexus 7 (2012) by Google Screen: 7.0", 800 × 1280, Large tvdpi RAM: 1024 MiB	
_	Nexus One by Google	Refresh

Figure 4: Device Definitions



0	Clone Device	e	- + ×
Name:	Nexus 7-Mod	Size:	large ‡
Screen Size (in): Resolution (px):	1200 x 1920	Screen Ratio: Density:	xhdpi ‡
Sensors: Cameras Input: RAM:	 Accelerometer Gyroscope GPS Proximity Sensor Front Rear Keyboard No Nav OPad Trackball 256 MiB 1 	Buttons: Device States:	Software Portrait: Fabled Navigation Landscape: Fabled Navigation Portrait with keyboard: Fabled Navigation Landscape with keyboard: Fabled Navigation
A The device "New The device"" "New The device "New The device "New The device	exus 7" will be duplicated into " under the "User" category	☑ Override th	e existing device with the same name Cancel Clone Device

Figure 5: Nexus 7-Mod

• Assign New Device to SimpleLockerAVD



🚺 Edit Ar	ndroid Virtual Device (AVD) - + ×			
AVD Name:	SimpleLockerAVD			
Device:	Nexus 7-Mod (7.02", 1200 × 1920: xhdpi) ‡			
Target:	Android 4.0.3 - API Level 15 ‡			
CPU/ABI:	ARM (armeabi-v7a) ‡			
Keyboard:	🗹 Hardware keyboard present			
Skin:	WXGA800-7in ‡			
Front Camera:	None ‡			
Back Camera:	None ‡			
Memory Options:	RAM: 256 VM Heap: 64			
Internal Storage:	200 MiB ‡			
SD Card:	Size: 100 MiB Browse			
Emulation Options:	Snapshot Use Host GPU			
Override the existing AVD with the same name				
Cancel OK				

Figure 6: Modified Device

Note: Open AVDs (use separate terminals)

- cd ./android/adt-bundle-linux-20140702/sdk/tools/
- ./emulator –avd Enisa -tcpdump dump.pcap
- cd ./android/adt-bundle-linux-20140702/sdk/tools/
- ./emulator –avd SimpleLockerAVD



eniss@10: -/android/adt-bundle-linux-x86-20140702/sdk/tools/ enisa@10: ~^ \$ cd ./android/adt-bundle-linux-x86-20140702/sdk/tools\$./emulator -avd ENISA -tcpdump dump.pcap
enisa@10: -/android/adt-bundle-linux-x86-20140702/sdk/tools
= + *
File Edit Tabs Help enisa@10: -/android/adt-bundle-linux-x86-20140702/sdk/tools
= + *
File Edit Tabs Help
enisa@10: -/ \$ cd ./android/adt-bundle-linux-x86-20140702/sdk/tools\$./emulator - avd SimpleLockerAVD

Note: emulators must be opened on different terminals. These Terminals will be dedicated to the AVD, do not close or write commands in them as this will close the emulator.

2.1.7 Sending commands through telnet:

Connect:

• telnet localhost 5554

Commands:

- power status full
- power status charging
- gsm call 0123456789
- sms send 12345 hello test sms
- geo fix 48 51



2.1.8 Try shortcut keys

Emulated Device Key	Keyboard Key
Home	HOME
Menu (left softkey)	F2 or Page-up button
Star (right softkey)	Shift-F2 or Page Down
Back	ESC
Call/dial button	F3
Hangup/end call button	F4
Search	F5
Power button	F7
Audio volume up button	KEYPAD_PLUS, Ctrl-F5
Audio volume down button	KEYPAD_MINUS, Ctrl-F6
Camera button	Ctrl-KEYPAD_5, Ctrl-F3
Switch to previous layout orientation (for example, portrait, landscape) $% \label{eq:scalar}$	KEYPAD_7, Ctrl-F11
Switch to next layout orientation (for example, portrait, landscape)	KEYPAD_9, Ctrl-F12
Toggle cell networking on/off	F8
Toggle code profiling	F9 (only with -trace startup option)
Toggle fullscreen mode	Alt-Enter
Toggle trackball mode	F6
Enter trackball mode temporarily (while key is pressed)	Delete
DPad left/up/right/down	KEYPAD_4/8/6/2
DPad center click	KEYPAD_5
Onion alpha increase/decrease	KEYPAD_MULTIPLY(*) / KEYPAD_DIVIDE(/)

Figure 8: Basic Emulator Commands¹

2.1.9 Enable USB debugging on emulator

• Developer Options>USB debugging



¹ http://developer.android.com/tools/help/emulator.html



- 2.1.10 List Devices
 - cd /android/adt-bundle-linux-x86-20140702/sdk/tools
 - adb devices

2.1.11 Run command on specific device

- adb -s emulator-5554 shell
- 2.1.12 Browse device folders using shell
 - adb shell
 - cd /data/data
 - Is
 - cd /data/app
 - ls
 - exit

2.1.13 Push and pull file to and from Emulator

- Create file on desktop (test.txt)
- adb push /home/Enisa/Desktop/test.txt /sdcard/testpush.txt
- adb pull/home/Enisa/Desktop/testpull.txt /sdcard/testpush.txt

2.2 Task 2: Cloning an Application

2.2.1 Run the Android emulator

In terminal run commands:

- cd /android/adt-bundle-linux-20140702/sdk/tools/
- ./emulator –avd Enisa -tcpdump dump.pcap

2.2.2 Download and Install MySuperAV

In Android Emulator:

- Go to url: 10.0.2.2/Good.html on Browser
- Click on the download link



Figure 10: Good Store



2.2.3 Install the app



2.2.4 Run the app



Figure 13: App Screenshot

- 2.2.5 Task: use adb pull to get apk file
- 2.2.6 Uninstall the app
- Decode the app 2.2.7
 - apktool d mysuperAV.apk •



Re Edit Taba Help Re Edit Taba Help			
enisa@10:~\$ cd Desktop/Training-Material/Mobile threats <u>IH/</u>			
enisa@10:~/Desktop/Training-Material/Mobile threats IH\$ apktool d mysuperAV.apk			
I: Using Apktool 2.0.0-RC1 on mysuperAV.apk			
I: Loading resource table			
I: Loading resource table			
I: Decoding AndroidManifest.xml with resources			
I: Loading resource table from file: /home/enisa/apktool/framework/1.apk			
I: Regular manifest package			
I: Decoding file-resources File Edit View Bookmarks Go Tools Help			
I: Decoding values */* XMLs			
T: Baksmaling			
I: Copving assets and libs			
1: Conving unknown files			
I: Copying original files			
enisadili - / Deskton / Training Material			
Figure 14: ApkTool Decode			

2.2.8 Inject Code - Classes

• Copy the custom smali folder ('Mods/smali/code') into the decoded app's ('smali/com') folder

	smali - +
File Edit View	Bookmarks Go Tools Help
F < • > /	へ 📓 /home/enisa/Desktop/Training-Material/Mobile_threats_IH/Mods/smali
Places Home Folder Desktop Trash Can Applications	E code
"code" folder	Free space: 10.1 GiB (Total: 22.7 Git
	com - +
File Edit View	Bookmarks Go Tools Help
,+, < ▼ > ,	/ image: home/enisa/Desktop/Training-Material/Mobile_threats_IH/mysuperAV/smali/com
Places	code example
2 items	Free space: 10.1 GiB (Total: 22.7 Gi

Figure 15: Inserting Code

2.2.9 Inject Code - Manifest

 Copy the contents of Mods/manifest/Mods_AndroidManifest.xml into the decoded app's Manifest (mysuperAV/AndroidManifest.xml) (use leafpad and read instructions on Mods_AndroidManifest.xml)

		manifest		$-$ + \times
File Edit View Boo	okmarks Go Tools I	Help		
$f = \langle \cdot, \cdot, \cdot \rangle \rightarrow f = \langle \cdot, \cdot, \cdot \rangle$	Mome/enisa/Deskt	op/Training-Mate	rial/Mobile_threats_IH/Mods/manifest	\$
Places Home Folder Desktop Trash Can Applications	Mods_Andro idManifest.x ml			
1 item (1 hidden)			Free space: 10.1 GiB (Total	: 22.7 GiB)
		mysuperAV		- + ×
File Edit View Boo	okmarks Go Tools	Help		
$\exists \forall \bullet $	📓 /home/enisa/Desk	top/Training-Mate	erial/Mobile_threats_IH/mysuperAV	\$
Places Home Folder Desktop Trash Can Applications	original re	s smali	Android/Mani fest.xml	
5 items			Free space: 10.1 GiB (Total	l: 22.7 GiB)

Figure 16: Manifest Files





Toolset, Document for students

1 Mode AndroidManifest yml	V	a *AndroidManifect vml - + ×
File Edit Search Options Help		File Edit Search Options Help
K- Make sure the following Permissions are included in your manifest (inside manifest tag) <manifest></manifest>		*Xml version="1.0" encoding="utF8" standalone="no"?> <manifest package="com.example.mysuperav" xmlns:android="http://schemas.android.com/apk/res/android"> <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"></uses-permission> <uses-permission android.name="android.permission.WTE_EXTERNAL_STORAGE"></uses-permission></manifest>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"></uses-permission> <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"></uses-permission> <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"></uses-permission> <uses-permission android:name="android.permission.NTERRET"></uses-permission> <uses-permission android:name="android.permission.RECEIVE_SMS"></uses-permission>	PÌ	 <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"></uses-permission> <uses-permission android:name="android.permission.WRITE_EXTENNAL_STORAGE"></uses-permission> <uses-permission android:name="android.permission.RECEIVE_SMS"></uses-permission> <uses-permission android:name="android.permission.RECEIVE_SMS"></uses-permission> <uses-permission android:name="android.permission.READ_PHONE_STATE"></uses-permission> <uses-permission android:name="android.permission.READ_SMS"></uses-permission> <uses-permission android:name="android.permission.READ_SMS"></uses-permission> <uses-permission android:name="android.permission.READ_SMS"></uses-permission> <uses-permission android:name="android.permission.READ_SMS"></uses-permission> <uses-permission android:name="android.permission.READ_CONTACTS"></uses-permission> <uses-permission android:name="android.permission.RECEST_CONTACTS"></uses-permission> <uses-permission android:name="android.permission.RECEST_COARSE_LOCATION"></uses-permission>
 cuses-permission android:name="android.permission.READ_PHONE_STATE"/> <uses-permission android:name="android.permission.READ_SMS"></uses-permission> <uses-permission android:name="android.permission.READ_CONTACTS"></uses-permission> <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"></uses-permission> <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"></uses-permission> 		<application and<br="" android:allowbackup="true" android:debuggable="true" android:icon="@drawable/ic_launcher"><activity android:label="@string/app_name" android:name=".MainActivity"> <intent-filter> <action android:name="android.intent.action.MAIN"></action> <category android:name="android.intent.category.LAUNCHER"></category> </intent-filter> </activity></application>
-d- Make sure the following receivers are included in your manifest (inside application tag) <application> <receiver< p=""> </receiver<></application>		

Figure 17: manifest modification

- 1. Build app
- apktool b mysuperAV



- 2. Move apk to signAPK folder
- Copy apk (mysuperAV/dist/mysuperAV.apk) and places it in the Tools/SignAPK folder



			dist			-
File Edit View B	Bookmarks Go	Tools Help				
\square < \neg > \land	🔪 📓 /home/enis	a/Desktop/	Training-Materia	l/Mobile_th	reats_IH/mysu	perAV/dist
Places Control Places	mysuperAV.a					
"mysuperAV.apk" (385.7 KiB)) Android package				Frees	pace: 10.1 GiB (Total: 22
			SignAPK			-
File Edit View B	ookmarks Go T	ools Help				
[+] < • > ^	/home/enisa	a/Desktop/1	Training-Material	l/Tools/Sign	АРК	
Places 👻	certificate p	kev pk8		signank	signapk jag	signapk-bb
🛗 Trash Can	em	ксурко	pk	зідпарк	Signapk.jai	signapk ob
Applications		SHE		SHE	Free	space: 10.1 GiB (Total: 2)

Figure 19: Placing apk into SingAPK

2.2.10 Sign the apk

• java – jar signapk.jar certificate.pem key.pk8 mysuperAV.apk mysuperAV_signed.apk

File Feit Taby Help	ennang roy bearcopy menning-meterney roomy.	aguers
enisa@10:~/Desktop/T	raining-Material/Tools/Si	gnAPK\$ java -jar signapk.jar cer
tificate.pem key.pk8	mysuperAV.apk mysuperAV_	signed.apk
enisa@10:~/Desktop/T	raining-Material/Tools/Si	anAPK\$
(m	SignAPK	- + ×
File Edit View	Bookmarks Go Tools Help	
(+) < ▼ > /	/home/enisa/Desktop/Training-Material/Tools/SignAPK	3
Places · · · · · · · · · · · · · · · · · · ·		
III Desktop 第 Trash Can	certificate.p key.pk8 mysuperAV.a mysuperAV_ signapik sig em pk signed.apk	gnapkjar
E Applications		r to LGB (Tass) 22 T GB)

Figure 20: Sign apk

2.2.11 Install the app

In Android Emulator:

- Make sure mysuperAV is not installed
- Go to url: 10.0.2.2/Bad.html on Browser
- Click on the Download link
- Install the app







Figure 22: Download apk

2.2.12 Run the app

- Open and run the app. See that all works fine.
- Close the app

2.2.13 Add Contact

- Go to 'People' app
- Click 'Create New Contact'
- Select 'Keep Local'
- Name: Bank
- Phone: +123456789
- Click 'Done'

2.2.14 Send SMS to emulator

- echo sms send +123456789 'This is Confidential' | nc localhost 5554
- echo sms send + 123456789 'your bank pin code is 1234' | nc localhost 5554



2.2.15 View Stolen Data

- Open text file "/var/www/html/myfile.txt" found on the Bad Server! This text file contains the stolen data that was taken from the victims device.
- sudo leafpad /var/www/html/myfile.txt



Figure 24: Stolen Data



2.3 Task 3: Analysing Cloned Application

- 2.3.1 Task: use adb pull to get apk file
- 2.3.2 Analyse network traffic
 - cd /android/adt-bundle-linux-20140702/sdk/tools/
 - wireshark dump.pcap
 - find http post to bad server (/bad.php)

	Stream Content					
about file	POST /index.php HT	TTP/1.1				- 1
about_int	Content-Length: 80	b5 lication/x-www-for	n-urlencoded			
<1000	Host: Stretteres		a di concoaco			
steat	Connection: Keep-/	Alive		41		
about.htn	User-Adent: Apache	e-Httpclient/UNAVA	ILABLE (Java	1.4)		
A dum	878d6f34795005e7b5	5c6d8213e99afe9=bc	e45f0e99f6b708	3b01fe888b7a	acacb0844e9c7458	8dd991cb8e8
	c3a81eb0381a376950	d613837417297270a9	8c94181572c37	52348b5e2144	0f1805121140ce	1f726cece30
	220d26372b5b985d55	50032401b9643df69f	9761fca2db1db5	587d7193449e	835c8fcf6f2d470	0f229641bb3
ette a la serie	be17e46134c04d4a81	11bee3ec95ff98c60d	53dcb66b279d3l	d4693a09d43	8896a8dcf09532cl	bcf223783fe
Filter: tcp.stre	7b810a255582e10d63	347c63411d4b5505a6	3e112c41189ed	7844c812f526	a4a28dfa1b78c6	5c6a2c3182f
	1010F05=35=300/1+bi	00485344454866863344	10707704f00521	10 <i>4</i> #NN=NEOEX	167434036006274	
No. Time	4e10f85a35a2084fb9 96406445f98de0f7a2	9ed853fffaf0cbc344 24090194fd7a4b8f82	de792794f09538 f1a70f4619ee2	384fbbab685t 5ff2174e0f96	016213193b885c20 0197d52e515dfc4	10aa8185cae
No. Time 33 114.9	4e10f85a35a2084fb 96406445f98de0f7a2 bc17ae77a397eee607	9ed853fffaf0cbc344 24090194fd7a4b8f82 7232025f11f190f637	de792794f09538 f1a70f4619ee2 e628bb9e690db	3841bbab685t 5ff2174e0f96 7810762616d5	016213193b885c20 0197d52e515dfc4 0d509bc64170c420	10aa8185cae 6405f64799b
No. Time 33 114.9 40 114.9	4e10185a35a20841b 96406445f98de0f7a bc17ae77a397eee60 90599e6c4a7f73bb36	9ed853fffaf0cbc344 24090194fd7a4b8f82 7232025f11f190f637 602e7283befcc96bbf	de792794f09538 f1a70f4619ee2 e628bb9e690db 34ff09adc57450	3841bbab685t 5ff2174e0f96 7810762616d5 999e0d190a25	5162131935885c24 5197d52e515dfc4 5d509bc64170c424 5b34fb0cc76842d4	10aa8185cae 6405f64799b 43e3f0da575
No. Time 33 114.5 40 114.9 44 115.6 45 115.1	4e10185a35a208410: 96406445f98de0f7a: bc17ae77a397ee60 90599e6c4a7f73b38 d281d1c53512c32HT Date: wed. 18 Jun	9ed853fffaf0cbc344 24090194fd7a4b8f82 7232025f11f190f637 602e7283befcc96bbf TP/1.1 200 0K 2014 06:51:25 GMT	de792794f09538 f1a70f4619ee2 e628bb9e690db7 34ff09adc57450	3841bbab6856 5ff2174e0f96 7810762616d5 999e0d190a25	016213193b885c24 0197d52e515dfc4 0509bc64170c424 0534fb0cc76842d4	10aa8185cae 6405f64799b 43e3f0da575
No. Time 33 114.9 40 114.9 44 115.6 45 115.1 48 117.7	4e10185a35a2084Tbi 96406445f98de0f7a; bc17ae77a397eee60 90599e6c4a7f73bb3 d281d1c53512c32HTT Date: Wed. 18 Jun	9ed853111a10cbc344 24090194fd7a4b8f82 7232025f11f190f637 502e7283befcc96bbf TP/1.1 200 OK 2014 06:51:25 GMT (1364 bytes)	de792794f09538 f1a70f4619ee2 e628bb9e690db 34ff09adc57456	3847bbab685t 5ff2174e0f96 7810762616d5 999e0d190a25	0162f3f93b885c2 0197d52e515dfc4 0d509bc64170c42d 0b34fb0cc76842d	c540161005a 10aa8185cae 6405f64799b 43e3f0da575
No. Time 33 114.5 40 114.5 44 115.6 45 115.1 48 117.7 49 117.7	4e10185a35a2084T0 96406445198de0f7a; bc17ae77a397eee60 90599e6c4a7f73b33 d281d1c53512c32HT1 Date: Wed. 18 Jun Entire conversation	9ed853111a10ebc344 240901944d7a4b8f82 232025f11f190f637 502e7283befcc96bbf TP/1.1 200 0K -7014 06:51:25 GMT (1364 bytes)	de792794f0953 f1a70f4619ee2 e628bb9e690db 34ff09adc57450	3847bbab685f 5ff2174e0f96 7810762616d5 999e0d190a25	0162131930885c2 0197d52e515dfc4 0d509bc64170c424 0b34fb0cc76842d4	10aa8185cae 6405f64799b 43e3f0da575
No. Time 33 114.5 40 114.5 44 115.6 45 115.1 48 117.7 49 117.7 31 114.8	4e10785a35a20847b7 96406445f98de0f7a; bc17ae77a397eee60 96599e6c4a7f73b3d d281d1c53512c32HTT Date: wed 18 Jun Entire conversation Find Save As	9ed833TT1418cbc344 24090194fd7a4b8f82 7232025f11f199f637 502e7283befcc96bbf TP/1.1 200 0K 2014 06:51:75 CMT (1364 bytes) Print O ASCII	de792794f0953 f1a70f4619ee22 e628bb9e690db 34ff09adc57450 O EBCDIC	3847bbab685t 5ff2174e0f9e 7810762616d5 999e0d190a25	0162131930885c2 0197d52e515dfc43 6d509bc64170c424 6b34fb0cc76842d4	0340161005a 10aa8185cae 6405f64799b 43e3f0da575
No. Time 33 114.5 40 114.9 44 115.6 45 115.1 48 117.7 49 117.7 31 114.8 34 114.9	4e10185a35a20841b 99640644519960e77a3 bc17ae77a397eee60 99599e6c4a7f73b3d d281d1c5351c23HT Date: wed. 18 Jun Entire conversation Find Save As	9ed833111418cbc344 24090194fd7a4b8f82 7232025f11f190f637 502e7283befcc96bbf TP/1.1 200 0K 2014 06:51:25 CMT (1364 bytes) Print ASCII	de792794f09533 f1a70f4619ee22 e628bb9e699db7 34ff09adc57450 O EBCDIC	384T bbab6851 5ff2174e0f96 7810762616d5 999e0d190a25	0162737930885627 1097d52e515dfc41 d569bc64170c42d 5b34fb0cc76842d4	0340161005a 10aa8185cae 6405f64799b 43e3f0da575
No. Time 33 114.5 40 114.9 44 115.6 45 115.1 48 117.7 49 117.7 31 114.8 34 114.9 39 114.9 115.6	4e10185a35a20841b 964064451980e07a2 bc17ae77a397ece60 905996c4a4773bb3 d28101c53512c32HT Date: wed. 18 Jun Entire conversation Find Save As Help	9ed831T14T6C6344 2490194f044b8f82 7232025f11f190f637 692e7283befcc96bbf 2814 86:51:75 (MT (1364 bytes) Print ASCII	de792794f09533 f1a70f4619ee21 6628b96690db 34ff09adc57450 O EBCDIC	384Tbbab685t 5ff2174e0f90 5ff2056d5d 399e0d190a25 O Hex Dum; ter Out This SI	016273193088562 11970526515dfc41 5d509bc64170c42d bb34fb0cc76842d p O C Arrays tream	(Close
No. Time 33 114.9 40 114.9 44 115.0 45 115.1 48 117.7 49 117.7 31 114.8 34 114.9 39 114.9 43 115.0 46 115.1	4-01835333-2884 Fb 964864459804697a bc17ae77a397eee60 965996-C4a4773b33 d281d1c53512c324FT Dafe: wed. 18 Jun Entire conversation Find Save As Help	9ed8331114160c344 2439019410744b8f82 2732025111199f637 729025111199f637 729114 06:51:2/5 GMT (1364 bytes) Print ASCII	de792794f09533 f1a70f4619ee21 e628bb9e690db3 34ff09adc57450 O EBCDIC	384 fbbab6851 6f 2174e0 f96 7810762616d 999e0d190a25 O Hex Dump ter Out This Si	D16273193088562 1970526515dfc4 50509bc64170c424 5054fb0cc76842d 0 C Arrays	Close C
No. Time 33 114.5 40 114.5 44 115.6 45 115.1 48 117.7 31 114.8 34 117.7 31 114.8 34 115.6 43 115.6 46 115.1	4e10185a35a26841fb 964084479804697ai bc17ae77a397ees60i 905996c4a4773b33 d281d1c35312c32HT Daff: wda Find Save As Help 905990 19.9.2.15	9ed833111a19cbc344 24990194f074b8f82 7232025f11f19ef637 723025f11f19ef637 72114 B6:51:25 GMT (1364 bytes) Print ASCII	de792794169533 f1a70f4619ee22 6628b96690db 34ff69adc5745(O EBCDIC Fill	Hex Dump Hex Dump Hex Dump CP	0162731930885c2 13974528215dfc41 3d569bc64170c422 3b34fb0cc76842d4 p C Arrays tream 04 30859 > htt	Close Close Close
No. Time 33 114.9 40 114.9 44 115.6 45 115.1 48 117.7 31 114.8 34 114.9 39 114.16 39 114.5 43 115.6 46 115.1.1 47 117.7 50 117.7	4-018333332084150 964064459804617ai bc17ae77a397ee660 905996c4a4773b33 d281d1c33512c32HT Dafe: wed. 18 Jun Entire conversation Find Save As Help 90990 18, 8, 2, 15 34718 10, 6, 2, 15	9ed831114160c344 249019416744b8f82 22302511119ef637 2027283befcc96bbf FP/1.1 209 0K 2014 Bio:1:25 (MT (1364 bytes) Print ASCII	de 792 794 f09533 11 a70 f461 9ec22 e628bb9e690db 34f f09adc 5745f EBCDIC	Hex Dum; Hex Dum; Hex Dum; CP TCP	12/13/93/885/23 13/745/25154f-(4) 13/745/25154f-(4) 13/945/25154f-(4) 15/94/24 15/94/24 15/94/24 15/94/24 15/94/24 15/94/24 15/94/24 15/94/24 15/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24 16/94/24	Close
No. Time 33 114.5 40 114.5 44 115.6 45 115.1 48 117.7 39 117.7 31 114.8 34 114.9 39 114.5 43 115.6 46 115.1 47 117.7 50 117.7 Frame 47: 64	4-019785.a35.a288410 06406445984697.a bc17.ae77.a397eee60 095996-64.4773b33 d281d1c33512c32HT Dafe: wed. 18 Jim Entire conversation Find Save As Help 19990 18.6.2.15 19478 10.6.2.15 bytes on wire (512	9ed83111616c6344 24960194f044b8f82 27232025111190f637 2723025111190f637 27014 86:5125 CMI (1364 bytes) Print ASCII	de'92/94/19533 11/a7014619ee22 e628bb9e690db7 44ff09adc57450 EBCDIC Fill	Hex Dum; Hex Du	016213193085625 1397d526153dfc4 d599bc64176c42 bb34fb8cc76842dd bb34fb8cc76842dd c C Arrays tream b4:50059 > ht 64:50059 > ht	() () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () () ()

2.3.3 Create new Investigation Folder

 Place original (Mobile_threats_IH/mysuperAV.apk) and cloned/signed (Tools/SignAPK/mysuperAV_signed.apk) apks into a new folder "Mobile_threats_IH /Investigation"

Note: Alternatively you can also find both apks in path (/var/www/html/). Copy and paste them into the investigations folder.

		N	lobile_threat	ts_IH			- + ×
Во	okmarks Go	Tools Help					
\sim	/home/enis	a/Desktop/1	raining-Materi	ial/Mobile_thre	ats_IH		3
ľ	Investigation	Mods	Apk.zip	mysuperAV.a			
						Free space: 10	.1 GIB (Total: 22.7 GIB)
			SignAP	<			- +
Bo	okmarks Go	Tools Help					
\sim	/home/enis	a/Desktop/	Training-Materi	ial/Tools/SignA	РК		
Ť		key ak					ionaak bb
	em	кеу.рко	pk	signed.apk	signapk	signapk.jai	signapk-bb
						Free space:	10.1 GiB (Total: 22.7 Gi
	1		Investigati	ion			- +
Во	okmarks Go	Tools Help					
\sim	home/enis	a/Desktop/1	raining-Materi	ial/Mobile_thre	ats_IH/InvesI	tigation	
	mysuperAV.a	mysuperAV_ signed.apk	┝				
						Fron concor	111 1 1 10 110 10 10 10 7 7 7 10

Figure 26: Investigation Folder



2.3.4 Decode both apk files

In terminal run command:

- cd Desktop/Training-Material/Mobile_threats_IH/Investigation
- apktool d mysuperAV.apk
- apktool d mysuperAV_signed.apk
 - enisa@10: ~/Desktop/Training-Material/Mobile_threats_IH/Investigation

File Edit Tabs Help
enisa@10:~/Desktop/Training-Material/Mobile_threats_IH/Investigation\$ apktool d mysuperAV.
apk
I: Using Apktool 2.0.0-RC1 on mysuperAV.apk
I: Loading resource table
I: Loading resource table
I: Decoding AndroidManifest.xml with resources
I: Loading resource table from file: /home/enisa/apktool/framework/1.apk
I: Regular manifest package
I: Decoding file-resources
I: Decoding values */* XMLs
I: Baksmaling
I: Copying assets and libs
I: Copying unknown files
I: Copying original files
enisa@10:~/Desktop/Training-Material/Mobile_threats_IH/Investigation\$ apktool d mysuperAV_
signed.apk
ו: using apктооו ב.ש.ש-אכו on mysuperav_signed.apk
I: Loading resource table
I: Loading resource table
I: Decoding AndroidManifest.xml with resources

- + ×

Figure 27: Decode apk files

2.3.5 Compare the content of both Manifests

In terminal run command:

- cd Desktop/Training-Material/Mobile_threats_IH/Investigation
- diff mysuperAV/AndroidManifest.cml mysuperAV_signed/AndroidManifest.xml

	emsagero: "/Desktop/maining-material/Mobile_chreats_in/investigation = +
File Ed	fit Tabs Help
enisa idMan	@10:~/Desktop/Training-Material/Mobile_threats_IH/Investigation\$ diff mysuperAV/Andro ifest.xml mysuperAV_signed/AndroidManifest.xml
4 85 ,1	<u>ح</u> ــــــــــــــــــــــــــــــــــــ
>	<pre><uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"></uses-permission></pre>
>	<pre><uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"></uses-permission></pre>
>	<pre><uses-permission android:name="android.permission.INTERNET"></uses-permission></pre>
>	<pre><uses-permission android:name="android.permission.RECEIVE SMS"></uses-permission></pre>
>	<pre><uses-permission android:name="android.permission.READ_PHONE_STATE"></uses-permission></pre>
>	<pre><uses-permission android:name="android.permission.READ_SMS"></uses-permission></pre>
>	<pre><uses-permission android:name="android.permission.READ_CONTACTS"></uses-permission></pre>
>	<pre><uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"></uses-permission></pre>
>	<pre><uses-permission android:name="android.permission.ACCESS COARSE LOCATION"></uses-permission></pre>
11a21	, 26
>	<pre><receiver android:name="com.code.SMSBroadcastReceiver"></receiver></pre>
>	<intent-filter android:priority="1"></intent-filter>
>	<action android:name="android.provider.Telephony.SMS_DELIVER"></action>
>	<action android:name="android.provider.Telephony.SMS_RECEIVED"></action>
٨	
λ	
enisa	@10:-/Desktop/Training-Material/Mobile threats IH/Investigation\$

Figure 28: Modified Manifest

2.3.6 Convert apks into jar files

- cd Desktop/Training-Material/Tools/dex2jar/
- ./dex2jar.sh ../../Mobile_threats_IH/mysuperAV.apk
- ./dex2jar.sh ../../Mobile_threats_IH/mysuperAV_signed.apk



apisa@10: ~/Decktop/Training_Material/Tools/dev2lar_0.0.9.15				
Clie Edit Tahr Help				
ne_con_nos_neo enisa@10:~/Desktop/Training-Material/Tools/dex2jar-0.0.9.15\$./dex2jar.sh//Mobile_thr sats IH/Investigation/mysuperAV.apk				
his cmd is deprecated, use the d2j-dex2jar if possible lex2jar version: translator-0.0.9.15 lex2jar//Mobile_threats_IH/Investigation/mysuperAV.apk ->//Mobile_threats_IH/Inv estigation/mysuperAV_dex2jar.jar jone.				
enisa@10:~/Desktop/Training-Material/Tools/dex2jar-0.0.9.15\$./dex2jar.sh//Mobile_thr eats_IH/Investigation/mysuperAV_signed.apk				
this cmd is deprecated, use the d2j-dex2jar if possible dex2jar version: translator-0.0.9.15 dex2jar//Mobile_threats_IH/Investigation/mysuperAV_signed.apk ->//Mobile_threats _IH/Investigation/mysuperAV_signed_dex2jar.jar Done. enisa@10:~/Desktop/Training-Material/Tools/dex2jar-0.0.9.15\$ []				
Investigation - + ×				
e Edit View Bookmarks Go Tools Help				
< ▼ > ∧ 📓 /home/enisa/Desktop/Training-Material/Mobile_threats_IH/Investigation ♦				
aces Home Folder Desktop Trash Can Applications				

Figure 29: Dex2jar

2.3.7 Analyse classes

- Open JD-GUI (Programming > JD-GUI)
- Open both apks in JD-GUI

2.4 Task 4: Analysing Simplelocker

2.4.1 Task: Install Simplelocker

- Disable Network connection on VM!!!
- cd Desktop/Training-Material/Mobile_threats_IH/
- 7z e Simplelocker.apk.zip
- <ask for password in class>
- Install using adb install or adb push

2.4.2 Task: Analyse Simplelocker

- Use apktool, analyse manifest
- Use dex2jar to create jar file
- Open jar file with jd-gui
 - Challenge 1: What encryption algorithm is being used?
 - Challenge 2: What is the encryption key
 - \circ $\,$ Challenge 3: What files types are being encrypted $\,$

2.4.3 Task: Remove Simplelocker

• Uninstall simplelocker using adb uninstall

2.5 Task 5 (Optional): Analysing Other Artifacts

Under /home/enisa/Mobile_threats_IH you will find samples of apks (Apk.zip), some of them are malicious while others are not. Some samples are still dangerous; Command and Control servers still active. You may wish to hand them to your students for additional practice.

Since some of the artefacts are still active, in order to analyse the network connections you may wish to use sandbox tools such as Anubis.

If you wish to run the applications locally, you should:



- use a segregated unprotected network, and clean/dummy devices without personal data (accounts, credentials, etc); or
- use a dns and http server on the host, simulating the C&C servers (a possible approach could be to run the tool in a sandboxed malware analysis tool, check for network connections, and configure dns and http servers accordingly); or

disable network connection (note that this may not always produce results, as the code may check for network connection prior to running its code)

2.5.1 Task: Flappy Bird

Analyse the code of both Flappy bird APKs. One of them is malware. Which one?

- Go to Mobile Folder:
 - o cd /home/enisa/Desktop/Training-Material/Mobile_threats_IH/
- Unzip Simple locker file:
 - o unzip Apk.zip
 - <ask for password in class>
- 2.5.2 Upload apk files to automated tools
 - Anubis;
 - Mobile Sandbox;
 - Joe sandbox mobile;
 - Others.
 - •

2.6 Questions

No.	Question	Answer
1	List any suspicious permissions that are being acquired	
2	Can you identify any background app components (Services/Broadcast Receivers)?	
3	Can you identify the initial/starting activity?	



4	Do you notice any suspicious network connections initiated by the application?	
5	From the code, can you see any suspicious Functions?	
6	If so, can you link these functions to the permissions and/or suspicious network connections?	
7	List any other useful information (eg: encryption keys, data being saved to database, etc.)	
8	What is the main purpose of this artefact?	

3 Conclusion

Depending on the student's previous experience with Mobile Technologies, he/she should be able to answer most of the questions listed in section 2.1.5.1.



ENISA

European Union Agency for Network and Information Security Science and Technology Park of Crete (ITE) Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou Marousi 151 24, Athens, Greece



PO Box 1309, 710 01 Heraklion, Greece Tel: +30 28 14 40 9710 info@enisa.europa.eu www.enisa.europa.eu