移动端安全测试工具介绍

(PDF测试岗位课程)







移动端的安全测试工具也非常多,归纳起来可以分为下图列表的几个方面,同 时也包含其比较有代表性的工具和适用系统:

类型	名称	适用系统		
网络分析工具	burpsuite	Android, IOS		
	Fiddler			
	wireshark			
反编译工具	apktool	Android		
	dex2jar	Android		
	IDA	IOS		
	otool	IOS		
签名工具	keytool/jarsigner	Android		
	signapk	Android		
权限分析工具	manitree	Android		
动态分析工具	DroidBox	Android		
	DDMS	Android		
静态分析工具	APKInspector	Android		
	otertool	Android		
	ApkAnalyser	Android		
安全审计集成工具	drozer	Android		
	mercury	Android		
	iAuditor	IOS		
其他工具	SDB	Android 2		



基于移动端的在安全测试领域的现状,我们主要关注点是放在Android系统上,从安全测试的角度,选取了部分工具作为介绍,其中反编译工具Dex2jar、jd-gui、安全审计工具Drozer,网络抓包工具Wireshark (BurpSuite等通用,不做介绍),以及其他工具DDMS、SDB等。





Android apk反编译即通过apk文件进行逆向工程,获取原始的数据资源。

工具主要有:

apktool:资源文件获取,可以提取出图片文件和布局文件进行使用查看 Dex2jar:将apk反编译成Java源码(classes.dex转化成jar文件) jd-gui:查看APK中classes.dex转化成出的jar文件,即源码文件

安全测试主要是查看源码,故我们重点讲解下Dex2jar、jd-gui对apk文件的反编译过程。



将要反编译的APK后缀名改为.rar,并解压,得到其中的classes.dex文件 (它就是java文件编译再通过dx工具打包而成的),将获取到的classes.dex 放到工具dex2jar目录下,在命令行下执行命令d2j-dex2jar.bat classes.dex --force,效果如下:

F:\Tools>cd decompilation\app tools\dex2jar-0.0.9.15

F:\Tools\decompilation\app tools\dex2jar-0.0.9.15>d2j-dex2jar.bat classes.dex -force dex2jar classes.dex -> classes-dex2jar.jar

F:\Tools\decompilation\app tools\dex2jar-0.0.9.15>

表示已反编译成功。



直接通过jd-gui打开反编译后的文件,即可查看到源代码:

classes-dex2jar.jar ×	
🖅 🖶 android.support	IPersistentStore\$PersistentStoreException.class ×
ian <mark>⊕</mark> com	package com.suning.mobile.http;
🕂 🖶 a.a	
🕀 🖶 anzewei.commonlibs	import java.io.IOException;
🗄 🖶 baidu.location	wublic class IPersistentStoreStoreExcention
🗄 🖶 dk.view.drop	extends IOException
🗄 🖶 fasterxml.jackson.core	{
iter google	private static final long
🗄 🖶 hp.hpl.sparta	private final int
🖶 🖶 mobeta.android.dslv	public int
🕀 🖶 nineoldandroids	
🗄 🖷 🖶 sina	return and a second sec
🖨 🖶 suning	
⊞ ⊞ a.a.a.a.a	
🗄 ··· 🖶 maa	
🖻 🖶 mobile	
i a	
😟 🖶 ablumloader	
i⊒…⊕ blh	
i⊞… 🖶 ehttp	
⊨	
in IPersistentStore	





Drozer是Android下的开源app安全审计框架。Drozer可以通过与 Dalivik VM,其它应用程序的IPC端点以及底层操作系统的交互,避免正处于开 发阶段,或者部署于你的组织的android应用程序和设备暴露出不可接受的安 全风险。drozer提供了很多Android平台下的渗透测试exploit供测试和修复。

下载地址: <u>https://labs.mwrinfosecurity.com/tools/drozer/</u>

需同时下载drozer攻击端和drozer服务端 (即Agent .apk only) 一般drozer攻击端安装在电脑上

Drozer服务端安装在被测的app所在的安卓手机或模拟器上



1. 测试准备

①首先在被测移动端上打开 Drozer Server,并将其置于 开启状态,如图所示:





②配置adb工具并加入环境变量,执行命令adb forward tcp:31415 tcp:31415,打开端口监听

③进入adb安装目录,执行命令drozer.bat console connect,当出现以下信息时代表drozer启动成功:





2. 查看可攻击的风险点

```
①查看Attack surfaces:
格式:run app.package.attacksurface app名
例:run app.package.attacksurface com.suning.mobile.ebuy
```

```
dz> run app.package.attacksurface com.suning.mobile.ebuy
Attack Surface:
    6 activities exported
    6 broadcast receivers exported
    Ø content providers exported
    6 services exported
    dz>
```

6 activities exported表示可能存在6个activities相关的安全风险; 6 broadcast receivers exported表示可能存在6个receivers相关的安全风险; 0 content providers exported表示不存在content相关的安全风险; 6 services exported表示可能存在6个services相关的安全风险。



②获取app的信息:

格式: run app.package.info -a app名

例: run app.package.info -a com.suning.mobile.ebuy





3. Intent组件测试

①查看暴露的广播组件信息: 格式: run app.broadcast.info -a app名 例: run app.broadcast.info -a com.suning.mobile.ebuy





②拒绝服务攻击测试

a,发送空action

格式: run app.broadcast.send --action app名 receiver名

例:run app.broadcast.send --action com.suning.mobile.ebuy com.suning.mobile.ebuy.base.host.pushmessage.PushReceiver b, 发送空extras

格式:run app.broadcast.send --component app名 receiver名 例:run app.broadcast.send --component com.suning.mobile.ebuy com.suning.mobile.ebuy.base.host.pushmessage.PushReceiver

③提升权限

例: run app.service.start --action com.test.vulnerability.SEND_SMS -extra string dest 11111 --extra string text 1111 --extra string OP SEND_SMS



4. Provider测试

①查看provider信息: 格式: run app.provider.info –a app名 例: run app.provider.info –a com.suning.mobile.ebuy

②利用drozer查看可能的sqlite注入的uri: 格式: run scanner.provider.injection –a app名 例: run scanner.provider.injection –a com.suning.mobile.ebuy

③尝试简单的注入:

格式: run app.provider.query content:脆弱uri --projection "' 例: run app.provider.query content:

//com.suning.mobile.ebuy/favorites?notify=false --projection ""





wireshark是非常流行的网络封包分析软件,功能十分强大。可以截取各种网络封包,显示网络封包的详细信息。使用wireshark时需了解网络协议, 否则看不懂wireshark。为了安全考虑,wireshark只能查看封包,而不能修改 封包的内容,或者发送封包。

wireshark也能获取HTTP和HTTPS,但不能解密HTTPS,如果是代理或 处置HTTP,HTTPS协议的数据包建议还是用Burpsuite、Fiddler等工具,而 TCP,UDP协议的可用wireshark。移动端的APP很多情况与服务器进行交互 时采用的是TCP/IP协议进行传输,此时wireshark就能派上用场了!



1. 抓包操作

The Wireshark Network Analyzer [Wireshark 1.8.2	2 (SVN Rev 44520 from /trunk-1.8)]		_ _ X	
File Edit View Go Capture Analyze Statistics	Telephony Tools Internals Help			
	Wireshark: Capture Interfaces			_ 🗆 🗙
Filter:	Description	ID	Dackota Dack	vota (a
占击Caputre-	Description	18 fo80::o7:bo47:7233:o166	n n	Details
WIR >Interfaces 出现 ^{L8.2}		1600.167.0477.7233.6100	0	
右边的对话框,	🔲 📂 JMicron	fe80::c9c2:edb5:1838:52ba	0	Details
选择正确的网卡	📄 🚰 VMware Virtual Ethernet Adapter	fe80::bdda:6a78:2d3c:594f	12	Details
	📝 🛃 Microsoft	fe80::6994:ac1c:1d8d:8a5c	22	Details
Live list of the capture interfaces (counts incoming packets)	E Microsoft	fe80::3de3:ff78:fd8:bd12	0	Details
🗃 Start				
Chorse one or more interfaces to capture from, then	Help	<u>S</u> tart S <u>t</u> op	<u>O</u> ptions	<u>C</u> lose
PE /1 CAE5E8B. AAB 0.425E		WOOR WRIT WIRESHark as	securely as possible	
点击start ernet Adapter: \Device\NP	•			
┃ 开始抓包				
Capture Options				
Start a capture with detailed options				
Capture Help				
- How to Capture	_			
Sten hv: etan to a successful canture setun			-	19
Ready to load or capture No Packe	iii iii iii iii iii iii iii iii iii ii	Profile: Default	•	



2. 抓包窗口

Capturing from Microsoft: \Device\NPF_(A9559F22-1504-4F4D-8067-DC61681A9F9C) [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]					
Ele Edit View Go Capture Analyze St.	atistics Telephony Iools Internals Help				
	, Q, 🗢 🔿 🖗 🗐 📑 🕀 O, Q, 🗹 👪 🗹 🥵 % 🙀				
Filter: ip.src == 192.168.1.102 or ip.dst== 192.168.1.102 过滤器 Apply Save					
No. Time Source	Destination Pro ro				
953 97.2501200 192.168.1.102	106.187.54.210 TCP 54 imgames > http [ACK] Seg=1277 Ack=5954 win=4:				
954 97.2503690 106.187.54.210	192.168.1.102 HTTP 247 HTTP/1.1 200 OK (application/json)				
955 97.4460230 192.168.1.102	106.187.54.210 TCP 54 imgames > http [ACK] seq=1277 Ack=6147 win=4:				
956 108.860594 192.168.1.102	199.47.217.148 TCP 66 abbaccuray > http [SYN] Seq=0 win=8192 Len=0				
957 109.011307 199.47.217.148	192.168.1.102 TCP 66 http > abbaccuray [SYI]=0 Ack=1 Win				
958 109.011448 192.168.1.102	199.47.217.148 TCP 54 abbaccuray > http AC 封包 tk=1 Win=1728				
959 109.013060 192.168.1.102	199.47.217.148 HTTP 250 GET /subscribe?ho、 万I 表 59&ns_map=126.				
960 109.026703 199.47.217.148	192.168.1.102 TCP 54 http > abbaccuray [RS1 2945]=1 Ack=197 W				
961 109.02/505 199.4/.21/.148	192.168.1.102 TCP 34 http > abbaccuray [RST, Acry Sed=1461 ACK=19				
902 109.02/704 199.47.217.148	102.100.1.102 ICP 34 https://double.com/form/form/form/form/form/form/form/fo				
965 109.028524 199.47.217.148	192.106.1.102 ICP 34 http://dobaccuray_ksij_seq=1 whet000000 Le				
904 109.030333 192.100.1.102	199.47.217.140 TCP OD Tapitik > http [Stw] Sed=0 withed192 Letter MS.				
< [II. F				
⊕ Frame 963: 54 bytes on wire (43	2 bits), 54 bytes captured (432 bits) on interface 0				
Ethernet II, Src: Tp-LinkT_74:b	f:3a (b) 8:7a:74:bf:3a), Dst: Prodrive_26:12:bf (00:0f:11:26:12:bf)				
Internet Protocol Version 4, Sr	c: 192 7.148 (199.47.217.148), Dst: 192.168.1.102 (192.168.1.102)				
Transmission Control Protocol,	Sec Bod http (90), Dst Port: abbaccuray (1546), Seq: 1, Len: 0				
	封包详细 信息				
0000 00 0f 11 26 12 bf b0 48 7a 0010 00 28 62 6b 00 00 55 06 a0 0020 01 66 00 50 06 0a 47 a2 b7 0030 0c b5 3b 5a 00 00	74 bf 3a 08 00 45 00&H zt.:E. 92 c7 2f d9 94 c0 a8(bkU/P. 十六 02 00 00 00 00 50 04 .f.PGP. 进制				
Microsoft: \Device\NPF_{A9559F22-1504	Packets: 4598 Displayed: 4163 Marked: 0 Profile: Default				



3. Wireshark与OSI七层网络模型关系:

	Micro	soft: \Device\N	PF_{A9559F22-1504-4	IF4D-8067-DC61681A9F9C} [Wireshark 💻 💷 🗙
	<u>Eile E</u> d	t <u>V</u> iew <u>G</u> o	<u>Capture Analyze S</u> t	atistics Telephony <u>T</u> ools <u>I</u>	nternals <u>H</u> elp
			🕒 🖥 🗶 😂 占) 🔍 🗢 🛸 🎝 ዥ 🕹	
	Filter:	http			Expression »
	No.	Time	Source	Destination	Protocol Length Info 🔺
	e	0.71955800	192.168.1.102	239.255.255.250	SSDP 175 M-SE
	16	3.72025000	192.168.1.102	239.255.255.250	SSDP 175 M-SE
	29	6.05659500	192.168.1.102	199.47.217.148	HTTP 250 GET ,
	30	6.08003700 6.72027400	192.108.1.102	220 255 255 250	HTTP 200 GET ,
	49	10.72037400	192.108.1.102	61 155 160 116	550P 175 M-567
	87	11 3457020	61 155 169 116	197 168 1 107	
应用层 下	131	11.6735230	192.168.1.102	114.80.142.90	HTTP 1029 GET .
本 示尼	132	11.6839850	192.168.1.102	114.80.142.90	HTTP 1044 GET
衣 小层	133	11.6847080	192.168.1.102	114.80.142.90	HTTP 1043 GET ,
会话层		11 0057020	102 100 1 102		NTTO 1050 CET
传输展	🗩 Fram	e 29: 250 b	ytes on wire (20	00 bits), 250 bytes c	aptured (2000 bits) or
1 K TIBUTA	🚺 🕀 Ethe	rnet II, Sr	c: Prodrive_26:1	.2:bf (00:0f:11:26:12:	bf), Dst: Tp-LinkT_74:
网络层 ————————————————————————————————————	🕂 🕀 Inte	rnet Protoc	ol Version 4, Sr	·c: 192.168.1.102 (192	.168.1.102), Dst: 199.
	Tran	smission Co	ntrol Protocol,	Src Port: ssslog-mgr	(1204), Dst Port: http
数据链路层	🕀 нуре	rtext Trans	ter Protocol		
14 77 12					
初理层					



4. 封包中的每个字段结构:







除了上诉工具外,其他比较实用的工具有:DDMS、SDB

DDMS的全称是Dalvik Debug Monitor Service,是Android开发环境中的Dalvik虚拟机调试监控服务。在ADT集成开发环境中自带的工具箱里,一般启动批处理文件monitor.bat可以打开DDMS。

SDB的全称是SQLite Database Browser,是一个手机存储数据库格式的 文件查看器,可以直接下载后使用,无需安装。



1. DDMS界面简介





2. SDB界面简介

SQLite Database Browser - E:/box/ttt/app_webview/Cookies

Edit View Help File Ĩ H Ŋ T. LOG |∖? Database Structure Browse Data 选择 New Record Delete Record Table: cookies 表名 creation_utc_host_key value path encrypted_va * expires <u>utc</u> secure httponly last_access_u has_expires persistent priority 1 3139303893665476 passportpre.cnsu ids_r_me NiExNDU3MDU40V9B / 0 3139304208570977 οl 0 1 字段内容 2 3139303893665847 passportpre. cnsu TGC TGTCA6113F7A149B /ids/ 0 3139304208570977 ol 0 1 3 3139303893666020 . cnsuning. com custno 6114570589 0 3139304163817257 ol 0 1 0 3139303893668223 passportpre. cnsu device session "242678515020149 /ids 0 4 0 3139304208570977 1 5 3139303894732767 . cnsuning. com authId si6BDAAE6570D17B / 0 ol 1 3139304163817257 ol 0 1 6 3139303894732870 . cnsuning. com secureToken 591D96E376A60AE5 / n 1 3139304165720762 ol n 1 1 7 3139303900113724 shoppingpre.cnsu_device_session_"242678515020149 /app/cart1/gatew O. n. 0 3139303900113724 ol Ω n 0 3139304163817257 0 8 3139303901283312 . cnsuning. com mtisAbTest B ol nl 3139303901397208 . cnsuning. com 0/ 0 3139304163817257 0 9 mtisCartQty 0 0 0 1 10 3139303996851364 vfastpre. cnsunin JSESSIONID QbHF1In94MGFvvP2 /vfast-web n. ol 0 3139303996851364 o 0 1 3139304002842444 . suning. com 1/ 3139305802000000 0 0 3139304096120520 1 1 11 snme 0 3139304096120520 12 3139304002844604 . suning. com snsr direct%7Cdirect% / 3139390402000000 ol 1 1 1 1%7C149483040283 / o 03139304096120520 13 3139304002845736 . suning. com 3202376002000000 1 1 _snma 1 14 3139304002856048 . suning. com 9483040283168245 / 0 3139304096120520 ol ol ol 0 snmp 1 15 3139304002856859 . suning. com 1494830402846187 n. 0 0 3139304096120520 ٥ 0 snmb 1 16 3139304002891039 . suning. com ssar direct%7Cdirect% / 3139390402000000 0 0 3139304096120520 1 0 3139304096120520 17 3139304002893393 . suning. com 1494830402839636 / 3202376002000000 ol 1 ssav 1 1 0 3139304096120520 18 3139304002906378 . suning. com 1494830402896314 / 3139305802000000 nl 1 1 _ssas 1 nl 19 3139304007488718 orderpre. cnsunin JSESSIONID QhmpP7dRmGrr50AJ /mobile/v1/onlin 0 ol 0 3139304203412100 Ω 1 20 3139304007711010 mypre. cnsuning. c JSESSIONID cmIqgCHTmKal9bZc /msi-web 0 0 0 3139304007711010 0 0 1 21 3139304008053912 hqpre. cnsuning. c JSESSIONID 1QfC7cpJaxMSY9Yr /bof 0 0 0 3139304208992746 0 0 1 22 3139304014410759 rxfpre. cnsuning. JSESSIONID WFeXek9k8BabkjCr /epps-cpf n ol 0 3139304014410759 ol 0 1 0 3139304163817257 23 3139304015333427 . ensuning. com direct%7Cdirect% / 3139390415000000 n 1 SDST 1 1 24 3139304068781695 . cnsuning. com direct%7Cdirect% / 3139390468000000 ol 0 3139304163817257 ssar • Þ. 111

< 1 - 43 of 43 >

Go to:

0

_ 0

23



