Android 7 以上版本，绕过CA限制，抓取https

WangLane 关注
0.697 2019.05.13 13:50:16 字数 558 阅读 3,028

环境

手机：小米5A
系统：MIUI 10
电脑：win10
抓包：mitmdump （可替换成其他抓包软件）
电脑需要安装：

- mitmdump（可替换成任意抓包软件）
- adb
- openssl

背景

我需要抓取https请求，苹果手机可以毫无问题的抓取，而安卓就不可以。原因是安卓7之后对证书的策略进行变更，应用不再使用用户证书。

有两种方式绕过：

- **在手机上安装系统证书**
- **修改app的manifest文件重新打包**

这里我们只讲第一种方法， 所以我们需要把证书添加到系统证书中。

为此，我们需要一台已经root的小米手机。root教程在miui论坛中已经非常详细了。官方给出了详细的步骤和工具。

开始

假设到这里你已经有一台root成功的小米手机。

安卓受信任的CA证书以特定的格式存储在 /system/etc/security/cacerts 目录下。我们可以在adb shell中查看到：

```
ls
00673b5b.0 31188b5e.0 5a250ea7.0 87753b0d.0 aeb67534.0 d4c339cb.0
02756ea4.0 343eb6cb.0 5a3f0ff8.0 882de061.0 b0ed035a.0 d59297b8.0
04f60c28.0 35105088.0 5cf9d536.0 89c02a45.0 b0f3e76e.0 d66b55d9.0
0d5a4e1c.0 3929ec9f.0 5e4e69e7.0 8d6437c3.0 b3fb433b.0 d6e6eab9.0
0d69c7e1.0 399e7759.0 5f47b495.0 91739615.0 b7db1890.0 d7746a63.0
10531352.0 3a3b02ce.0 60afe812.0 9282e51c.0 b872f2b4.0 d8317ada.0
111e6273.0 3ad48a91.0 6187b673.0 9339512a.0 b936d1c6.0 dbc54cab.0
12d55845.0 3c58f906.0 63a2c897.0 9479c8c3.0 bc3f2570.0 dc99f41e.0
17b51fe6.0 3c6676aa.0 67495436.0 9576d26b.0 bdacca6f.0 dfc0fe80.0
1dac3003.0 3c860d51.0 69105f4f.0 95aff9e3.0 bf64f35b.0 e442e424.0
1dcd6f4c.0 3c9a4d3b.0 6e8bf996.0 9685a493.0 c491639e.0 e48193cf.0
1df5a75f.0 3d441de8.0 6fcc125d.0 9772ca32.0 c51c224c.0 e775ed2d.0
1e1eab7c.0 3e7271e8.0 75680d2e.0 9c3323d4.0 c7e2a638.0 e8651083.0
1e8e7201.0 40dc992e.0 76579174.0 9d6523ce.0 c907e29b.0 ea169617.0
1eb37bdf.0 418595b9.0 7672ac4b.0 9dbefe7b.0 c90bc37d.0 ed39abd0.0
1f58a078.0 455f1b52.0 7999be0d.0 9f533518.0 cb156124.0 ee7cd6fb.0
21855f49.0 48a195d8.0 7a7c655d.0 a0bc6fbb.0 cb1c3204.0 facacbc6.0
```

WangLane 关注
总资产5 (约0.49元)

Python笔记 | python 合并字典
阅读 6

scrapy | scrapy 和 requests分别对response进行解码
阅读 26

推荐阅读

这是一份面向Android开发者的复习指南
阅读 9,299

Python模块-Requests学习与CTF和AWD实战
阅读 455

如何加载100M的图片却不撑爆内存，一张 100M 的大图，如何预防...
阅读 8,812

公考言语框架
阅读 102

【渗透实例】Fuzz大法好啊
阅读 308

这里我们用到的是mitmproxy，它的证书存放在user/Administrator/.mitmproxy/ 目录下。pem为后缀的文件。

查看openssl版本

```
openssl version
```

如果是1.0以上的版本：

```
openssl x509 -inform DER -in cacert.der -out cacert.pem
openssl x509 -inform PEM -subject_hash_old -in cacert.pem
```

如果是1.0以下的版本：

```
openssl x509 -inform DER -in cacert.der -out cacert.pem
openssl x509 -inform PEM -subject_hash -in cacert.pem
```

上面的两条语句，如果已经是pem后缀的文件，可以直接执行第二条， cacert.pem就是你的证书文件。

第一行会输出一个类似这样的hash串：

```
7672ac4b
```

然后重命名证书

```
cp cacert.pem 7672ac4b.0
```

复制证书到设备上

可以直接粘贴到手机中，也可以用adb复制过去，这里的7672ac4b换成前面你得到的那个hash串

```
adb root
adb remount
adb push 7672ac4b.0 /sdcard/
```

复制到系统目录并修改权限

```
adb shell
su
mount -o rw,remount /system
mv /sdcard/<cert>.0 /system/etc/security/cacerts/
chmod 644 /system/etc/security/cacerts/7672ac4b.0
reboot
```

验证

然后我们在手机中依次进入：设置→安全→信任证书→系统证书

证书安装成功就没什么问题了：

image.png

可能遇到的问题

可问题：

```
remount of /system failed: Read-only file system
remount failed
```

解决方法：

```
adb root
adb disable-verity
adb reboot
adb remount
adb shell
mount -o rw,remount /system
```

参考文章：

Configuring Burp Suite with Android Nougat
Android 7 Nougat and certificate authorities