

# 如何利用Nexus 5伪造一张门禁卡

seudingo

2015-10-05

文中提及的部分技术可能带有一定攻击性，仅供安全学习和教学用途，禁止非法使用！

## 0×00 前言

我租住的杭州一个老小区一年前出现了所谓的“出租房杀人事件”，事件过后民警叔叔们给小区的每个单元都装上了门禁，所有住户都需要在物业处登记，物  
的工作人员会让你提供身份证或者公交卡用来注册，注册之后就可以刷卡进门了。

但由于某些原因，我并不想去登记注册一张门禁卡，正好手头有一部nexus5，众所周知nexus5是有nfc功能的，我便想能不能用nexus5的nfc功能伪造一张门  
卡呢？一番尝试之后，就有了下文的方法。（从来没接触过无线安全，对Proxmark3，acr122u 等设备也是一窍不通，各位大牛见笑了）

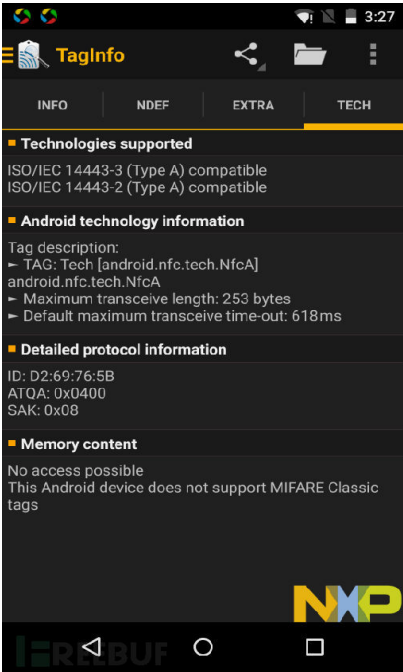
## 0×01 分析

由于身份证，公交卡等很多卡都可以用来当门禁卡，那基本上有九成把握这个门禁只是简单读取卡的id，并不会去解密里面的内容，只要简单模拟一个相同id  
卡就可以刷开门禁。

## 0×02 “采样”

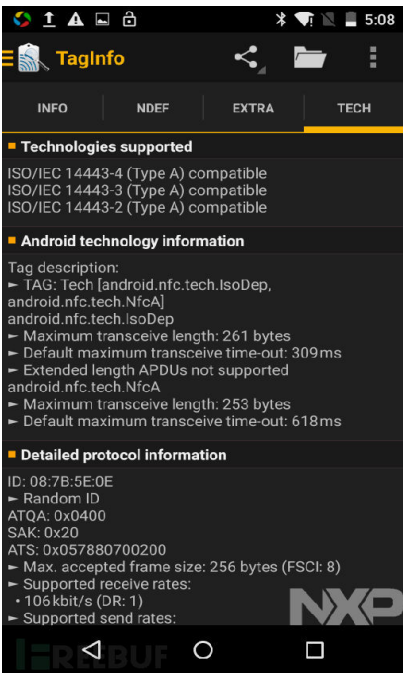
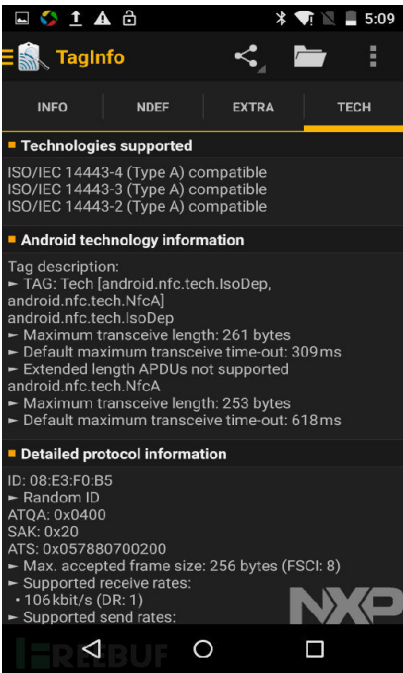
我们下载一款名为“TagInfo”的android应用，用它来读取一下现在可以刷开门禁的卡信息。（跟同楼的妹子借的）

如下图：



卡的id为：D2:69:76:5B

接着我们找另一台nexus5看一下手机原来的id，扫描出来这台nexus5的id是在不停变化的，如下图：



原来出于安全考虑，android手机的id是一个4个字节长度的随机id，每次连接都会变化，并且都以 “0x80” 开头。

android官方并没有提供任何的api可以指定修改nfc的id，但是我们可以用直接修改配置文件的方式来实现,前提当然是手机必须root过了。

0x03Just Do IT

1、到手机的 /etc/ 目录找一个文件名为libnfc-brcm-20791b05.conf，默认情况下，文件中NFA\_DM\_START\_UP\_CFG 的配置项是这样的值：

```
{45:CB:01:01:A5:01:01:CA:17:00:00:00:00:06:00:00:00:00:0F:00:00:00:00:E0:67:35:00:14:01:00:00:10:B5:03:01:02:FF:80:01:01:C9:03:03:0F:AB:5B:01:00:B2:04:E8:03:00:00:CF:02:02:08:B1:06:00:20:00:00:00:12:C2:02:00:C8}
```

2、通过修改这个值就可以改变id。把该文件下载到电脑上，先在最后面增加一个0x33作为标志位，接着接上要指定的id长度，在当前的情况下就是0x04,最后后面接上要制定的id：“0xD2,0x69,0x76,0x5B”，接着改变最首的数字，加上我们总共增加的字符串长度，这里我们需要加上6，所以最后配置项变成：

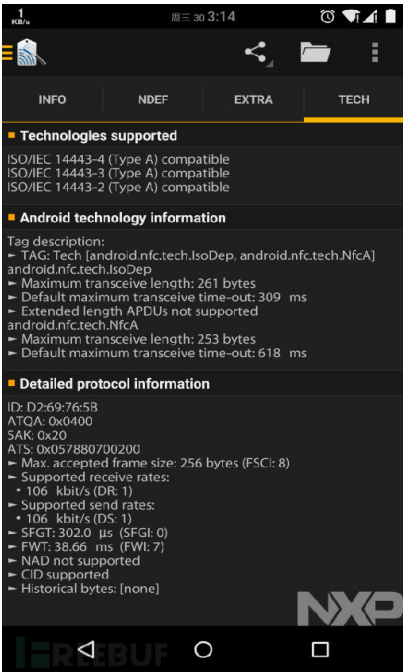
```
{4B:CB:01:01:A5:01:01:CA:17:00:00:00:00:06:00:00:00:00:0F:00:00:00:00:E0:67:35:00:14:01:00:00:10:B5:03:01:02:FF:80:01:01:C9:03:03:0F:AB:5B:01:00:B2:04:E8:03:00:00:CF:02:02:08:B1:06:00:20:00:00:00:12:C2:02:00:C8:33:04:D2:69:76:5B}
```

3、采用adb的方式覆盖系统中原来的文件，然后重启

```
adb root
```

```
adb remount
adb push libnfc-brcm-20791b05.conf /etc/
adb reboot
```

重启之后我们发现，这台nexus5的id已经被改成了我们想要的。



拿着修改好的nexus5去试试看？记得必须在唤醒屏幕的情况下nfc才有效。

0×04 演示视频

Toggle navigation

成功!

关注黑客与极客

首页

分类阅读

黑客

- 漏洞
- 安全工具
- WEB安全
- 系统安全
- 网络安全
- 无线安全
- 设备/客户端安全
- 数据库安全
- 安全管理

极客

- 极客有意思
- 周边

特色

- 专题
- 人物志
- 活动
- 视频
- 观点
- 招聘

活动

- FREE TALK•成都站
  - 2015-10-31
  - 进行中
- 作者问答送书
  - 2015-08-19
  - 进行中

讨论。

om)

!

回到

晒工作台，免费送书

2015-08-04

查看全部

小酒馆

公开课

商城

漏洞盒子

能够模拟任意 UID 只能对付使用 M1 卡的门禁，而不能模拟 M1 卡内容，更没法消费

登录

ZMOM1031

其实在手机和读卡器中间放一张NFC卡，在特定情况下会起到穷举的效果

已有 69 条评论

不脱也火

2015-10-05

我有Nexus 5，我想刷卡不要钱，我回去就做

dawner

2015-10-05

楼主的方法适用于 Broadcom BCM20793 NFC 芯片，但是这款芯片不支持 Mifare Classic  
能够模拟任意 UID 只能对付使用 M1 卡的门禁，而不能模拟 M1 卡内容，更没法消费

FLY (1级)

2015-10-06

@ dawner 您好，我想请教一下，小米3能实现上面的功能吗？小米3也带NFC 也有libnfc-brcm-20791b05.conf这个文件

FLY (1级)

2015-10-06

@ dawner 我测试了，小米3能用，并且不用唤醒屏幕就能用。

csxy

2015-10-06

@ FLY 你的文件怎么修改按楼主的一模一样吗？

FLY (1级)

2015-10-07

@ csxy 恩，就是按照楼主上面说的修改的

good\_kid (1级)

2015-10-10

@ FLY 对的，因为他是抄的所以说必须点亮屏幕，其实NFC重要的特点就是静默条件下的使用。

叶良辰

2015-10-05

我家的门能打开吗？👉

Glaucus

2015-10-05

非奶5的NFC手机表示没找到etc下的那个文件

FLY (1级)

2015-10-06

@ Glaucus 小米3 有这个文件

Oxroot (4级)

奔跑的蚂蚁

2015-10-06

@ Glaucus 找libnfc-brcm.conf

cc\_脉航 2015-10-05

这个可以啊

亮了 (

ZMOM1031 2015-10-05

其实在手机和读卡器中间放一张NFC卡，在特定情况下会起到穷举的效果

亮了 (

FLY (1级) 2015-10-11

@ ZMOM1031 能详细说一下吗？

亮了

Yuuki\_Lai 2015-10-05

试试 看看可以不

亮了 (

micki 2015-10-05

理论上是不是支持nfc的手机都可以？

亮了 (

dawner 2015-10-05

请注明出处：http://stackoverflow.com/a/28720342/1016460

亮了 (

清风987 (1级) 2015-10-05

@ dawner 层主大神哈，你是怎么发现的？？？

亮了

dawner 2015-10-05

以及出处的出处：http://stackoverflow.com/a/28360190/1016460

楼主只有故事是原创

亮了 (

Oxroot (4级) 奔跑的蚂蚁 2015-10-05

@ dawner 也不能说是翻译 作者参考了国外的一些内容吧 毕竟人家也有自己的一些思路 然后亲手实践了一下

亮了

a 2015-10-07

@ dawner nxp的nfc芯片能模拟m1吗

亮了

good\_kid (1级) 2015-10-10

@ a M1是NXP的专利，所以应该只有他家或者他授权的厂家才能模拟的。

亮

守望II奥姆卡 2015-10-05

你好，请教一下，先在信息最后面增加一个0x33作为标志位 这是为什么？

亮了 (

清风987 (1级) 2015-10-05

好吧。。。。看完五楼大神的回复之后，感觉英文版的更详细一些果断英文版本了

亮了 (

eumenides\_5272 2015-10-05

看到我啊啊啊

亮了 (

aaa 2015-10-05
















也就是必须先找一个可以通过的卡，然后读取他的卡ID才可以复制一个一样的  
如果换一个门，那就要换一个单眼的住户的卡才行了？

亮了 (




























HenryWang624 2015-10-05

[作揖]

亮了 (

2015/10/12		如何利用Nexus 5伪造一张门禁卡 - FreeBuf.COM   关注黑客与极客	
grafu		2015-10-05	15楼 <a href="#">回</a>
厉不厉害			 <a href="#">亮了</a> (
<hr/>			
_咋也不咋		2015-10-05	16楼 <a href="#">回</a>
并没有看懂			 <a href="#">亮了</a> (
<hr/>			
MR_0010		2015-10-06	17楼 <a href="#">回</a>
验证的密匙应该是默认密匙			 <a href="#">亮了</a> (
<hr/>			
Peanut Killer		2015-10-06	18楼 <a href="#">回</a>
文中：“原来出于安全考虑，android手机的id是一个4个字节长度的随机id，每次连接都会变化，并且都以“0×80”开头。”的'0×80'有错，应当是0×08.			 <a href="#">亮了</a> (
<hr/>			
<a href="#">syusa</a>	(1级)	2015-10-06	19楼 <a href="#">回</a>
NFA_DM_START_UP_CFG= {1F:CB:01:01:A5:01:01:CA:14:00:00:00:00:06:E8 :03:00:00:00:00:00:00:00:00:00:00:00:00:80 :01:01}			
这个是0X04 第一位怎么改啊 高手指点 怎么算的			 <a href="#">亮了</a> (
<hr/>			
<a href="#">n0w4ve5</a>	(1级)	2015-10-08	<a href="#">1</a>
@ syusa 1F换十进制16+15 十进制15+16+6=37 换十六进制=25  25:CB:01...			 <a href="#">亮了</a>
<hr/>			
哎哟妹妹的不错哦		2015-10-06	20楼 <a href="#">回</a>
小区卡我倒试过。挺不错的			 <a href="#">亮了</a> (
<hr/>			
<a href="#">小郎君</a>	(1级)	2015-10-06	21楼 <a href="#">回</a>
TagInfo的时候，很抱歉TagInfo已停止运行 是怎么回事啊？请指教			 <a href="#">亮了</a> (
<hr/>			
撸迪		2015-10-06	22楼 <a href="#">回</a>
小区卡我倒试过。挺不错的			 <a href="#">亮了</a> (
<hr/>			
csxy		2015-10-06	23楼 <a href="#">回</a>
0×33标记位是什么作用，或者说可以把0×33换成别的			 <a href="#">亮了</a> (
<hr/>			



刘大虎  2015-10-08	30楼 <a href="#">回</a>
.	
Cool 刚发现三星系列手机也可以，其中NFA_DM_START_UP_CFG 存在libnfc-sec文件中。	 <a href="#">亮了</a> (
<a href="#">taylorwin</a> (4级) 2015-10-08	<a href="#">f</a>
@ 刘大虎 三星什么型号呢？	 <a href="#">亮了</a>
xiaoming 2015-10-08	31楼 <a href="#">回</a>
还是买个能模拟uid的卡片吧。淘宝5块钱。	 <a href="#">亮了</a> (
张_will  2015-10-08	32楼 <a href="#">回</a>
玩过mifare classic tool，家里的门卡居然是加密的	 <a href="#">亮了</a> (
<a href="#">亢宇飞的微波</a> (1级) 2015-10-08	33楼 <a href="#">回</a>
一加手机 cm12.1系统，读出来的id是01：02：03：04 求怎么改，按上述方法改会造成nfc无法打开	 <a href="#">亮了</a> (
<a href="#">Sophie啾啾</a> (1级) 2015-10-09	34楼 <a href="#">回</a>
不错 学习了	 <a href="#">亮了</a> (
<a href="#">bawangq</a> (1级) 2015-10-09	35楼 <a href="#">回</a>
怎么我的身份证没办法看到id？？	 <a href="#">亮了</a> (
子曾曰不耻不若人何若人有  2015-10-09	36楼 <a href="#">回</a>
其它型号的NFC手机可以参考 这篇文章进行修改	 <a href="#">亮了</a> (
M1sT4k3r  2015-10-09	37楼 <a href="#">回</a>
回头试试。	 <a href="#">亮了</a> (
玉殷痕  2015-10-09	38楼 <a href="#">回</a>
越狱！	 <a href="#">亮了</a> (
云起涟漪YUNQILIANYI  2015-10-09	39楼 <a href="#">回</a>
[doge][喵喵]	 <a href="#">亮了</a> (
田瑞国  2015-10-09	40楼 <a href="#">回</a>
好办法。 其它型号的NFC手机可以参考 这篇文章进行修改	 <a href="#">亮了</a> (
VYSEa  2015-10-09	41楼 <a href="#">回</a>
这个是NFC-A，也就是NFC TAG产品用的标准，一般就用于识别东西而已，储存不了啥加密的数据。国内有些安防设备用去年说的Mifare Classic也罢，直接用TAG当门禁。。。。	 <a href="#">亮了</a> (
悲观主义的码农  2015-10-10	42楼 <a href="#">回</a>
n6和n5一样吗？	 <a href="#">亮了</a> (
WPloveYU  2015-10-10	43楼 <a href="#">回</a>
马克一下	 <a href="#">亮了</a> (
-老光  2015-10-11	44楼 <a href="#">回</a>
[喵喵][doge]	 <a href="#">亮了</a> (



[kentq](#) (1级) 2015-10-12

开始以为是ID卡，原来是卡ID，……

亮了 (

選擇檔案 未選擇任何檔案



昵称

必须 您当前尚未登录。[登陆？](#)[注册](#)

请输入昵称

邮箱

必须（保密）

请输入邮箱地址

表情 插图

提交评论(Ctrl+Enter) [取消](#) ☒ 有人回复时邮件通知我

关键字查找

- [黑客在身体中植入NFC芯片，绕过军…](#)
- [NFC协议安全工具-NFCGUI 1.5 Pro版…](#)
- [NFC协议安全工具-NFCGUI发布](#)
- [大话Apple Pay（苹果支付）安全](#)
- [跟我学姿势：极客教你如何科学的刷卡](#)

特别推荐



- [当DNS泄漏让VPN不再安全，我们该怎么办？](#)
- [一周海外安全事件回顾（9.8-9.14）：谁动了中本聪的奶酪？](#)
- [2015，你该警惕家中的大品牌路由器了：扒一扒那些“开后门”的路由器厂商](#)

<a href="#">江湖小吓</a>	2015-05-19	<a href="#">blackscreen</a>	2014-09-17	<a href="#">Rechange</a>	2015-01-05
<a href="#">美国国安局 (NSA) 工具库大揭秘</a>					
<a href="#">cs24</a>	2013-12-31				

