手机手环复制教程

模拟实现的条件:::

1.复制器一台

2.手机或者手环一部 (必须具备 NFC 功能)

3.可反复擦写的卡一张 (UID 或 CUID 都可)

4.需要模拟的 IC 卡 (称之为原卡, 13.56Mhz 的 M1 卡)

前言:小米从 MIUI12 开始支持模拟加密 IC 卡/华为手机 CPU980 以上支持模拟,但只能模拟加密 IC 卡卡号信息 (0 扇区 0 块)

本教程以 NSR108 软件版本为 2020060302, 复制加密卡数据到小米 4NFC 手环为例。

第一步:原卡解密

机器连接电脑后打开软件,把需要模拟的卡(原卡)放在机器的感应区域,点击"开始 解码"按钮。解码过程中不要移动卡片或者机器,耐心等待解码成功(解码时间根据不 同卡加密程度而定,几秒钟至一小时的情况都有)。

第二步: 另存数据

解码成功以后,右侧数据栏会出现 16 进制的原始数据,点击"另存数据"按钮,对数据进行保存选好输出路径,保存后会得到一个 dump 文件,并且文件大小标准为 1K 文件,这里我们重命名为"123.dump"

接口 状态 USB ····································			> N1F0011	34050	✓
	读卡器目	已经连接			
LF Card H	IF Card 侦测嗅	探数据比较	参数酉	置	
卡片 : Mifare Cla 解码成功	ssic 1K, uid: b52dce	1e Atqa:0400 S	ak: 08	-	➡ 提示解码成功
解码参数 □ 卡片类型强制)为 MF1-S50		Key A:		
	FFFFFFFFFFF		Key B:		
●标准解码 练	别: 4	· · · · · · ·	扇区	块	数据
○直接爆破 扇	区: 3 ~ 深度	ŧ: 6 —	0	0	B5 2D CE 1E 48 08 04 00 00 08 61 33 16 42 28 80
	林_止上上	土工品研究石	0	1	00 00 00 50 00 09 00 00 00 00 00 70 00 00 00 00
場作区 🌽	第 少标	(山)「火口州年11月	0	2	00 00 00 00 00 00 00 00 00 00 00 00 00
	1		0	З	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
开始解码	只读卡号	写UID卡	1	0	00 00 00 00 00 00 00 00 00 00 00 00 00
	1		1	1	00 00 90 00 00 65 00 00 00 00 09 00 00 78 00 00
安莱港M1 上	ECHID/EUID-E		1	2	00 00 00 00 00 00 00 00 00 00 00 00 00
与首通阿下	SCOID/FOIDF	坝UFUID卡	1	З	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
			2	0	00 00 00 00 00 00 00 00 00 00 00 00 00
格式化卡片	写GTU卡	写单块数据	2	1	00 00 12 00 00 43 00 80 00 00 00 00 00 30 00 00
			2	2	00 00 00 00 00 00 00 00 00 00 00 00 00
分析数据	특λ dump	日存数据	2	3	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
75 DTXADH	11/ 1P	/ JIJ XADH	3	0	00 00 00 00 00 00 00 00 00 00 00 00 00
			0	3 4 6	

]		状态	0010010001	另存为			
SB	~	wCopy N 读卡器已纪	SR 108-H V601 经连接		此电脑 > 文档	✔ 0 2 搜索"文档"	8
F Card	HF Card	侦测嗅探	· 数据比较	组织 新建文件关	· 夕安 ^	修改日期	ы • ж. л и
:片:Mifare 码成功	Classic 1K, ui	d: b52dce1e	e Atqa:0400 Sa	 ✓ ★ 快速访问 ■ 桌面 ▲ 下封 	Adobe	2020/5/12 13:51 2020/3/19 12:21	文件夹 文件夹
附的梦烈 门上已来那	吊制为 MF1-S	50		● 文档 ★	Corel	2020/3/24 11:21	文件夹
」 トク天空: 一 伸田 家田		FEE			WeChat Files	2020/3/24 15:55	文件夹
		TTT	12	1月份贴片明细	WpsPrint Files	2020/3/20 19:53	文件夹
⊃直接爆破 操作区	扇区: 3	─ 深度:	6	Share 单文件标签 卡工坊出货记录		LoLofof+ 1030	Domi
开始解码	ı 只读	未号	写UID卡	> Network Construction	自定	义文件名,默认文件类型为du	qmr
写普通M1·	卡 写CUID	/FUID-ŧ	锁UFUID卡				
格式化卡)	+ 写G	TUŧ	写单块数据	文件名(N): 123 保存类型(T): Dur	.dump np Files (*.dump)		
分析数据	导入	dump	另存数据	▲ 隐藏文件夹	夏后占土 (2)	保存(S)	取消

第三步: 写入空卡

换上复制空白卡,点击写 UID 卡或者 CUID 卡按钮,写卡成功后点击格式化卡片,格式 化成功后得到一份不带加密数据的卡。

	状态					
USB wCopy NSR108-H V601>			> N1F00113	4050	と	
	✓ 读卡器E	已经连接				
LF Card Hi	- Card 侦测嗅	探数据比较	参数配	置		
卡片:Mifare Clas	sic 1K, uid: b52dce	1e Atqa: 0400 S	ak: 08		➡ 提示写UID卡成功	
状态:写 UID 卡瓦	成功					
解码参数			Key A:	-		
	为 MF1-S50					
日 伸田 家田 日	FEFFFFFFFF		Key B:			
						L
●标准解码 级	1	扇区	t ‡	紫 灯 非民		
○ 直接爆破 扇	▽: 3 〜 深閉	ŧ: 6 — • —	0	0	B5 2D CE 1E 48 08 04 00 00 08 61 33 16 42 28 80	
			ŏ	1	00 00 00 50 00 09 00 00 00 00 00 70 00 00 00 00	
ポニジト	は田山の下		0	2	00 00 00 00 00 00 00 00 00 00 00 00 00	Ì
探IF区			0	3	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	
开始解码	只读卡号	写UID卡	1	0	00 00 00 00 00 00 00 00 00 00 00 00 00	
			1	1	00 00 90 00 00 65 00 00 00 00 09 00 00 78 00 00	
宇花港M1ト	ECHIDICHIDE		1	2	00 00 00 00 00 00 00 00 00 00 00 00 00	
与首通MI下	SCOID/FOIDF	坝 OFOID 下	1	3	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF FF	
		1	2	0	00 00 00 00 00 00 00 00 00 00 00 00 00	
格式化卡片	写GTU卡	写单块数据	2	1	00 00 12 00 00 43 00 80 00 00 00 00 00 30 00 00	
			2	2	00 00 00 00 00 00 00 00 00 00 00 00 00	
分析数据	导入 dump	另存数据	2	3	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	
75 FIRADA		2 TO XXDH	3	0	00 00 00 00 00 00 00 00 00 00 00 00 00	
			3	1	00.00.67.00.00.00.54.00.00.32.00.50.00.00.00	

Į□ USB	状态 wCopy 读卡器E	NSR108-H V601 P经连接…	> N1F00113	34050	✓ 连接 蜂鸣 检查更新	
LF Card H	F Card 侦测嗅	探数据比较	参数配	置		
卡片:Mifare Clas 状态:格式化卡片	ssic 1K, uid: b52dce 针成功	1e Atqa:0400 S	iak: 08		→ 提示格式化卡片成功	
解码参数 □ 卡片类型强制	为 MF1-S50		Key A:			
□ 使用密钥 F	FFFFFFFFF		Key B:			
●标准解码 级○直接爆破 扇	ŧ: 6	扇区 0	块 0 1	数据 B5 2D CE 1E 48 08 04 00 00 08 61 33 16 42 28 80 00 00 00 50 00 09 00 00 00 00 07 00 00 00 00		
操作区			0	2	00 00 00 00 00 00 00 00 00 00 00 00 00	
TT #442770	口法上马	FUDE	0	3	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	
71781784149	六块下方		1	1	00 00 90 00 00 65 00 00 00 00 00 00 00 78 00 00	
写普通M1卡	写CUID/FUID卡	锁 UFUID 卡	1	2	00 00 00 00 00 00 00 00 00 00 00 00 00	
格式化卡片	写GTU卡	写单块数据	2	0	00 00 00 00 00 00 00 00 00 00 00 00 00	
分析数据	导入 dump	另存数据	2	3	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	
		0	4			

第四步:模拟原卡卡号

手机打开蓝牙点开小米运动 (app),连接手环后,找到"门卡模拟",打开门卡模拟, 再次注意此时只是模拟了原卡的卡号而已,加密数据并不会写入,按照提示进行下一步。 (手机各有不同请自行操作一下)

9:34		# ≈ ■	10:12	att 🗢 (•• 10:18	배 중 🛤	10:18	:::: 중 100
	小米手环 4 NFC版	ß	<		<	门卡模拟	<	门卡模拟
	93. \$\$\$	C				手环门卡功能 经想提权后将门卡模拟到手环中 出行更方便	请料	8门卡紧贴手环以进行检测 ^{贴近后请点击开始检测}
	π	>						
		х						11
① 门卡模:	eu	>	门卡模拟 手环模拟门卡,将实	本 门卡模拟弱手环上使用	2			
● 来电提 未开出	52	>	小米空白卡 手环并通空白卡,开	8 后去物业投权或激活即可使用	>			
事件提用 无符度器	離せ	>						
● 手环间 未开自	钟	>						
	知提醒	х						
	B2	3				宣看门卡支持范围		
	更多>					T-#		臺費门卡支持范围
小爱同学		>						开始检测

检测卡片成功后,点击开始模拟,耐心等待模拟成功,成功后自行添加卡片名称,点击完成。

第五步: 写入数据

手机或者手环模拟成功后,把手机或者手环放置复制器的感应区域,导入之前保存好的 原始卡数据 dump 文件,点击"写普通 M1 卡",软件提示写卡成功即模拟成功。



	状态					
USB wCopy NSR108-H V601>				34050	50 🗸 连接 蜂鸣 检查更新	
~	读卡器日	已经连接				
LF Card HF Card	侦测嗅	探数据比较	参数酉	置		
⊧片 : Mifare Classic 1K. ui 状态 : 写 MF1 卡成功	d: b52dce	1e Atqa:0400 S	ak: 08		→→→ 提示写卡成功即模拟成功	
解码参数 □卡片类型强制为 MF1-S	50		Key A:			
) 使用密钥 FFFFFFFF	FFF		Key B:			
		1.				U
●标准解码 级别: 4		a ta a a a	扇区	块	块数据	
○直接爆破 扇区: 3	≹:6 —	0	0	0 B5 2D CE 1E 48 08 04 00 00 08 61 33 16 42 28 8	30	
			0	1	1 00 00 00 50 00 09 00 00 00 00 00 70 00 00 00 0	0
操作区			0	2	2 00 00 00 00 00 00 00 00 00 00 00 00 00	0
			0	3	3 FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	F
开始解码 只读	法号	写UID卡	1	0		0
						0
写普通M1卡 写CUID)/FUID卡	锁UFUID卡		2		E
A			2	0		0
格式化卡片 军 G	TUŧ	写单块数据	2	1		ň
		-J T WXXDH	2	2		0
			2	3	3 FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	F
分析数据 导入	dump	为仔颈猎	3	0	0 00 00 00 00 00 00 00 00 00 00 00 00 0	0
				11 222	ex	

如果写手机时软件提示写卡失败或者验证卡片某扇区密码错误,我们就需要重来了。 把模拟进去的空卡删掉,按照步骤重新模拟,模拟成功后点击开始解码,解码成功后, 再进行格式化(特别注意:空卡模拟成功后解码手机再格式化,)格式化成功后再按照 步骤导入原卡数据 dump 文件,点击'写普通 M1 卡'按钮,写卡成功即模拟成功。 小米的卡模拟功能只能模拟 0 扇区 0 块的前 8 个字节,且绝大部分梯控只验证 0 扇区 0 块前 8 个字节数据,后 8 字节的厂商编码无法更改。

关于复制加密 IC 卡信息到手机成功后,无法读取到写入手机 NFC 完整信息的解决办法 思路:因为手机手环 NFC 芯片安全等级较高,已经修复了嵌套攻击漏洞,所以 NFC 解 码软件不能靠后门破解。虽然后门堵死了,正门有钥匙还是可以进,钥匙就是原卡 dump 文件中的密钥 A 或者密钥 B,有了密钥,安全等级再高也可以读取 NFC 信息。

注意把软件更新到最新版本(检查更新)

解码原卡后,点击"另存数据",保存原卡数据 dump 文件。再回到软件,点击"导入 dump" 按钮,把保存好的原卡 dump 文件导入进去后,软件会自动填写密钥,需手动勾选"使用密钥",把手机放置机器读卡区域,点击"开始解码",就可以解码写入手机的数据。 如写入手机或者手环后刷卡不成功,此时可另存数据,保存手机解码出来的 dump 文件。 切换到软件的"数据比较"界面,分别导入原卡数据 dump 文件与写入手机的数据 dump 文件,比较数据是否一致(此操作可参考复制器使用说明)。