## Tesla NFC数据应答流程分析

我们应该使用两个pm3,一个抓去手机与车端的数据,一个抓去卡与手机端的数据,看一下是不是有丢包现象。

## pm3抓到正常开门数据

```
Rdr | 26
I REQA #REQA数据,类似于广播,不停的发送,等待卡片回应
Tag | 48 00
I ATQA #卡片回答
Rdr | 93 | 20
I ANTICOLL #防止多张卡冲突的一条命令, 用来锁定一张卡
Tag | 88 04 36 10 aa
Rdr | 93 70 88 04 36 10 aa b3 b4
                                                          l ok
| SELECT_UID #获取卡的UID
Tag | 24 d8 36
Rdr | 95 20
I ANTICOLL-2 #防止冲突
Tag I 72 Of 60 80 9d
Rdr | 95 70 72 0f 60 80 9d 3e f6
                                                          l ok
I ANTICOLL-2 #防止冲突
Tag | 20 fc 70
Rdr | e0 60 3f 94
                                                          I ok
I RATS #数据交换速率,等待时间协商
Tag I 05 78 77 91 02 d5 b6
Rdr | 26
l REQA
Rdr | 0a 00 00 a4 04 00 0a f4 65 73 6c 61 4c 6f 67 69 |
   I 63 f8 09
                                                          I ok
I? #applet选择, tesla先选择了一个applet id
Tag | 0a 00 6d 00 83 5f
                                                          I ok
I # 6d00表示没有这个applet id
```

```
Rdr | 26
I REQA
Rdr | 0b 00 00 a4 04 00 0a 74 65 73 6c 61 4c 6f 67 69 |
 I 63 01 bb
I ? #选择新applet uid
Tag | 0b 00 90 00 48 8f
                                                     l ok
I # 9000返回存在
Rdr | 26
l REQA
Rdr | 26
I REQA
Rdr | 26
I REQA
Rdr | 26
I REQA
Rdr | 0a 00 80 11 00 00 51 04 c2 7f cf 7b 92 5c ba 99 |
   l be a3 f3 77 c3 f3 fb 90 e0 a7 b6 76 51 ab 58 c9 l
   | Of 44 7c 7c ef a8 3f 99 db 27 93 de e1 81
                                              71 97 I
   I c7 9d d9 5c aa 58 79 fd a9 d4 98 17 d0 02 f8 20 I
  l 16 a5 8f 27 da 78 83 0f 4a 92
                                                     l ok
l? # 发送加密数据等待卡计算
Tag I fa 00 01 d3 4b
l #卡返回swtx等待
Rdr | fa 00 01 d3 4b
                                                     l ok
I ? #车返回确认等待
Tag I fa 00 01 d3 4b
Rdr | fa 00 01 d3 4b
                                                     l ok
Tag I fa 00 01 d3 4b
Rdr | fa 00 01 d3 4b
                                                     l ok
Tag | fa 00 01 d3 4b
Rdr | fa 00 01 d3 4b
                                                     I ok
```

从流程可以看到tesla会先选择一个applet id=>f4,如果没有就选择第二个applet id=>74,实际测试中发现,74是用来开关车门的,f4目前还不确定。

## nfcgate开门数据

```
Rdr | e0 60 3f 94
I RATS
Tag I 05 78 80 71 00 6f 7c
Rdr | 26
I REQA
Rdr | 02 00 a4 04 00 0a f4 65 73 6c 61 4c 6f 67 69 63 |
                                                           l ok
 l ed b1
I ? #选择f4 applet超时
Tag I f2 01 91 40
Rdr | f2 01 91 40
Tag | f2 01 91 40
Rdr | f2 01 91 40
Tag | f2 01 91 40
Rdr | f2 01 91 40
Tag | f2 01 91 40
Rdr | f2 01 91 40
Tag | f2 01 91 40
Rdr | f2 01 91 40
Tag | f2 01 91 40
Rdr | f2 01 91 40
Tag | f2 01 91 40
Rdr | f2 01 91 40
Tag | f2 01 91 40
Rdr | f2 01 91 40
Tag | f2 01 91 40
```

168723604   168728340	Tag   f2		91	40													! . !	
168779712   168784480	Rdr   f2		91	40													ok	?
169229428 7 169234164	Tag		91	40														
169285776   169290544	Rdr   f2		91	40													ok	?
169735492   169740228	Tag		91	40														
169792256   169797024	Rdr   f2		91	40													ok	?
170241972   170246708	Tag   f2	2 01	91	40														
170298752   170303520	Rdr   f2	2 01	91	40													ok	?
170748484   170753220	Tag   f2	2 01	91	40														
170812016   170816784	Rdr   f2	01	91	40													ok	?
171261732   171266468	Tag   f2	01	91	40														
171318080   171322848	Rdr   f2	01	91	40													ok	?
171767796   171772532	Tag   f2	01	91	40														
171823152   171827920	Rdr   f2	2 01	91	40													ok	?
172272868   172277604	Tag   f2	2 01	91	40													į į	
172330368   172335136	Rdr   f2	2 01	91	40													ok	?
172780084   172784820	Tag   f2	2 01	91	40													į į	
172835888   172840656	Rdr   f2	2 01	91	40													ok	?
173285604   173290340	Tag   f	2 01	91	40													i i	
173347840   173352608	Rdr   f	2 01	91	40													ok	?
173797556   173802292	Tag   f2	2 01	91	40													i i	
173859264   173864032	Rdr   f	2 01	91	40													ok	?
174308980   174313716	Tag   f2	01	91	40													i i	
174357232   174358288	Rdr   26	j _															i l	REQA
174479024   174499856	Rdr   03	8 00	a4	04	00	0a	f4	65	73	6c	61	4c	6f	67	69	63	i	
	j jfo	l 3f															ok	?

时间单位为us,使用tag-rdr获取时间,不确定对不对。

因为tesla会第一次选择一个不存在的applet id, 所以在nfcgate中,我们可以在第一次tesla选择applet id = f4时,替换数据为74的applet id, 在11个s-block以内,返回6d00, tesla会发送applet id=74的请求,nfcgate直接抛弃这一条指令,那么我们可以为选择applet id争取最多22个s-block,通过查看抓包数据发现,nfcgate会在5s时返回数据,小于22个s-block,那么,便可以保证选择applet id正常通过。

下面这个是pm3抓包时,一个f4通过的例子,但是在选择74 applet id时,失败了

217140576	217141632	Rdr	26																	REQA
217142820	217145188	Tag	48	00																
217254128	217256592	Rdr	93	20																ANTICOLL
217257780	217263604	Tag	88	04	36	10	aa	40		L-2	6.4								-1-	CELECT HTD
217348192	217358656	Rdr	93	70 d8	88 36	04	36	10	aa	b3	b4								ok	SELECT_UID
217359908	217363428	Tag   Rdr	24   95	-	30															ANTTCOLL -2
217466256   217469908	217468720 217475796	Kur   Tag	95   72	20 0f	60	80	9d											ł		ANTICOLL-2
217560336	217570800	l Rdr	1 95	70	72	0f	60	80	9d	3e	f6							-	ok I	ANTICOLL-2
217572052	217575636	Tag	20	fc	70	01	00	00	Ju	30	10							ł	UK	AVIICOLL-2
217642176	217646944	l Rdr	l e0	60	3f	94												ł	ok	RATS
217651076	217659268	Tag	05	78	80	71	00	6f	7c										ok	
217724000	217725056	Rdr	26															i		REQA
217845776	217866608	Rdr	02	00	a4	04	00	0a	f4	65	73	6c	61	4c	6f	67	69	63		
			ed	b1															ok	?
218311620	218316356	Tag	f2	01	91	40												i		
218367312	218372080	Rdr	f2	01	91	40												ĺ	ok	?
218817028	218821764	Tag	f2	01	91	40														
218880736	218885504	Rdr	f2	01	91	40													ok	?
219330452	219335188	Tag	f2	01	91	40														
219393312	219398080	Rdr	f2	01	91	40													ok	?
219843028	219847764	Tag	f2	01	91	40														
219906736	219911504	Rdr	f2	01	91	40													ok	?
220356452	220361188	Tag	f2	01 01	91 91	40													ok	?
220419568   220869284	220424336 220874020	Rdr	f2   f2	01 01	91	40 40													ok	f
220009204	220937776	Tag   Rdr	12   f2	01	91	40													ok	?
221360708	221366532	Tag	02	6d	00	81	с5											ł	UK	
221418848	221419904	Rdr	26	ou	00	01	CJ											ŀ		REQA
221536816	221557712	Rdr	03	00·	•a4•	· 04 ·	- 00 -	•0a•	.74	65	73	6c	61	4c	6f	67	69	63		1.241
			0b	9d															ok	?
222002660	222007396	Tag	f2	01	91	40														
222058960	222063728	Rdr	f2	01	91	40												ĺ	ok	?
222508676	222513412	Tag	f2	01	91	40			17	44	7	<b>:</b> 牛:	·후f	1	<b>4</b> ⊨	旦	左-	7/10	tim	eout 了
222572400	222577168	Rdr	f2	01	91	40			儿	177		ענין	1	4,		Æ	1 ×	<b>4</b> H	Loki	eput J
223022116	223026852	Tag	f2	01	91	40														
223085200	223089968	Rdr	f2	01	91	40													ok	?
223534916	223539652	Tag	f2	01	91	40														
223598640   223650912	223603408   223651968	Rdr   Rdr	f2   26	01	91	40													ok	? REQA
223030912	223793600	l Rdr	20   03	00	a4	04	00	0a	74	65	73	6c	61	4c	6f	67	69	63 I		REŲA
223//2/04	223733000	i Kui I	l 0b	9d	a+	04	- 00	va	_/-	05	,,	UC	01	40	01	07	09	05	ok I	?
224048372	224053108	l   Tag	f2	01	91	40												ł		
224105376	224110144	Rdr	f2	01	91	40													ok	?
224555092	224559828	Tag	f2	01	91	40												i		
224618176	224622944	Rdr	f2	01	91	40													ok	?
225067892	225072628	Tag	f2	01	91	40												i		
225131616	225136384	Rdr	f2	01	91	40													ok	?
225581332	225586068	Tag	f2	01	91	40														
225645072	225649840	Rdr	f2	01	91	40													ok	?
226094788	226099524	Tag	f2	01	91	40														2
226158512	226163280	Rdr	f2	01	91	40													ok	?
226608228	226612964	Tag   Rdr	f2   f2	01 01	91 91	40 40													ok	?
226671344   227121060	226676112   227125796	Kur   Tag	12   f2	01 01	91	40													ok	,
227121000	227189552		l f2	01	91	40													ok I	?
	EE, 103332	-1101		-01		- '0													- 01	

## 现在有两个方向:

- 1. 本来以为tesla的数据发送会分包,那么可以通过在数据发送完成之后,不回复应答信息,迫使车端 重新发送一遍数据来争取时间,但是发现tesla的数据没有做分包发送。(不存在可以利用的场景)
- 2. 修改RATS中等待时间,改成telsa接受的最大值(可能需要自己修改的白卡中实现部分测试,才能在实际场景中测试);
- 3. 选择速率更快的转发方案,保证在5个s-block内返回数据,大概是0.44s\*5(卡片计算需要6个s-block),或者在数据计算时,tesla可以允许更多的s-block(需要测试才能知道)。