谈谈 Mifare Classic 破解

Date: November 17, 2013 | Category: RFID,极客

2008 年的时候，荷兰恩智浦（NXP）公司开发的 RFID 产品 Mifare Classic 就被破解了，黑历史在这里就不在具体说了，想详细了解可以自己 Google 百度。现在还是重点说说关于 Mifare Classic 破解的内容。

Mifare Classic 提供 1 Kb - 4Kb 的容量，现在国内采用的多数是 Mifare Classic 1k(S50)[后面简称 M1 卡]，而我以后的测试也大多是基于 M1 卡开展。

大家要先了解 M1 卡的结构，这能够为后期的破解做铺垫。

M1 卡有从 0 到 15 共 16 个扇区，每个扇区配备了从 0 到 3 共 4 个段，每个段可以保存 16 字节的内容，为什么这里要强调从 0 开始呢？这跟 C 语言里面数组下标默认从 0 开始是差不多的，好计算地址偏移，我们不必太过在意，只是要记住是从 0 开始，写入数据的时候不要写错地方就可以了。每个扇区的第 4 个段（也就是 3 段）是用来保存 KeyA，KeyB 和控制位的，因为 M1 卡允许每个扇区有一对独立的密码保护，这样能够更加灵活的控制数据的操作，控制位就是这个扇区各种详细权限计算出来的结果。

每张 M1 卡都有一个全球唯一的 UID 号，这个 UID 号保存在卡的第一个扇区（0 扇区）的第一段（0 段），也称为厂商段，其中前 4 个字节是卡的 UID，第 5 个字节是卡 UID 的校验位，剩下的是厂商数据。并且这个段在出厂之前就会被设置了写入保护，只能读取不能修改，当然也有例外，有种叫 UID 卡的特殊卡，UID 是没有设置保护的，其实就是厂家不按规范生产的卡，M1 卡出厂是要求要锁死 UID 的。下图很清晰的列出了 M1 卡的结构。

		一个段内的字节															
区号	段号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	说明
15	3 (63)	KEYA						Access Bits				KEYB						区尾15
	2 (62)																	数据段
	1 (61)																	数据段
	0 (60)																	数据段
14	3 (59)	KEYA						Access Bits				KEYB						区尾14
	2 (58)																	数据段
	1 (57)																	数据段
	0 (56)																	数据段
:	:																	:
:	:																	:
:	:																	:
1	7 (7)	KEYA						Access Bits				KEYB						区尾1
	6 (6)																	数据段
	5 (5)																	数据段
	4 (4)																	数据段
0	3 (3)	KEYA						Access Bits				KEYB						区尾0
	2 (2)																	数据段
	1 (1)																	数据段
	0 (0)																	厂商段

厂商段是存储器第一个区的第一个数据段（段 0 ）。它包含了 IC 厂商的数据。基于保密性和系统的安全性，这个段在 IC 卡厂商编程之后被置为写保护，如图 25 所示。

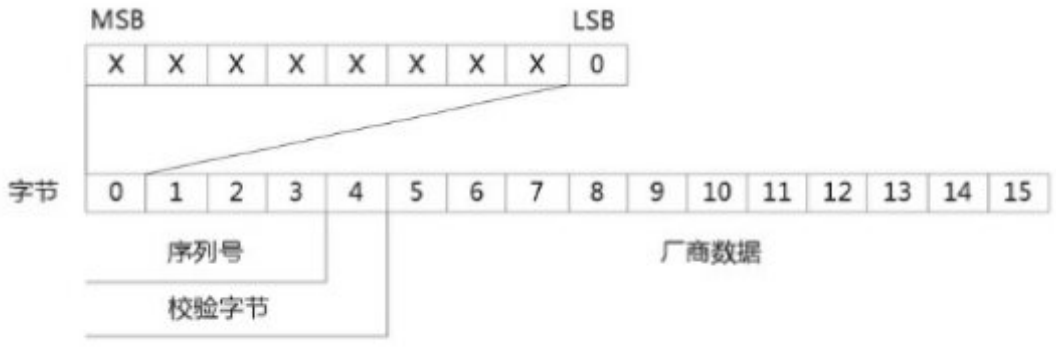

图 25 厂商段结构

更多的 M1 卡结构可以下载这两个 PDF 仔细阅读。

高频 IC 卡指南

飞利浦官方 M1 卡文档

看完上面的文档我相信你对 M1 卡也有了一定的了解，现在就来简单谈谈 M1 卡的各种破解方法，后面会陆续发布相对应的实际案例。

1. 暴力破解

暴力破解是破解工作永远的话题，只要你拥有庞大的计算资源，管你什么密码都能破解。而且，在 CRYPTO1 算法的细节没有被泄露之前，最有效的方法就是暴破了。还有一个很重要的原因就是，M1 卡是被动卡，需要读卡器为它提供能

量，一旦读卡器切断了电源，卡中的临时数据就会丢失，这样就没有办法记录下攻击者究竟输错了多少次密码，卡永远不会因为密码输入错误太多而被锁定，只要攻击者有时间慢慢跟它耗，密码肯定会出来的。

这里列举一些常见的 M1 卡密钥

```
FFFFFFFFFFFF
A0A1A2A3A4A5
D3F7D3F7D3F7
000000000000
A0B0C0D0E0F0
A1B1C1D1E1F1
B0B1B2B3B4B5
4D3A99C351DD
1A982C7E459A
AABBCCDDEEFF
B5FF67CBA951
714C5C886E97
587EE5F9350F
A0478CC39091
533CB6C723F6
24020000DBFD
000012ED12ED
8FD0A4F256E9
EE9BD361B01B
```

> 2. 重放攻击

重放攻击是基于 M1 卡的 PRNG 算法漏洞实现的，当卡接近读卡器获得能量的时候，就会开始生成随机数序列，但这有一个问题，因为卡是被动式卡，本身自己不带电源，所以断电后数据没办法保存，这时基于 LSRF 的 PRNG 算法缺陷就出来了，每次断电后再重新接入电，卡就会生成一摸一样的随机数序列，所以我们就有可能把这个序列计算出来，所以只有我们控制好时间，就能够知道在获得能量后的某一刻时间的随机数是多少，然后进行重放攻击，就有可能篡改正常的数据。如果卡的所有权在我们手上的时候，我们甚至不需要浪费太多的时间就可以实现。

> 3. 克隆卡片

这是一个很简单也很实用的方法，因为M1卡自带扇区可以保存数据，所以大部分的卡片会选择加密扇区后将数据保存在里面，所以我们完全可以克隆一张带有一样数据的克隆卡。这就会用到一种叫 UID 卡的特殊 M1 模拟卡，前面说到每张 M1 卡在 0 扇区第 1 段都会有一个全球唯一的 UID 编号，而且这个块在出厂之后是被厂商设定保护无法修改的，UID 卡就是没有设定 0 扇区保护的卡，所以你可以随意的修改你想要的 UID，这样我们就可以克隆出一张连 UID 都相同的卡片了。

> 4. 密钥流窃听

利用神器 Proxmark 3 可以嗅探到全部扇区都加密的 M1 卡，在卡和已经授权的读卡器交换数据的时候进行窃听，就能把 tag 数据读取出来，利用 XOR 算 Key 工具就可以把扇区的密钥计算出来，这也是 PRNG 算法的漏洞所导致的。

> 5. 验证漏洞

验证漏洞是目前使用最多的M1破解手段，在读卡器尝试去读取一个扇区时，卡会首先发一个随机数给读卡器，读卡器接到随机数之后利用自身的算法加密这个随机数再反馈回给卡，卡再用自己的算法计算一次，发现结果一致的话就认为读卡器是授权了的，然后就用开始自己的算法加密会话并跟读卡器进行传送数据。这时候问题就来了，当我们再次尝试去访问另一个扇区，卡片又会重复刚才那几个步骤，但此时卡跟读卡器之间的数据交换已经是被算法加密了的，而这个算法又是由扇区的密钥决定的，所以密钥就被泄露出来了。因此验证漏洞要求我们至少知道一个扇区的密钥，但目前大部分的扇区都没有全部加密，所以很容易就会被破解。

破解 M1 卡当然不仅仅只有这几种方法，但对于我们来说已经足够了，目前国内 80% 的 IC 卡都是 M1 卡，例如门禁卡，饭卡，智能电卡之类的。

这里再提供两篇 Radboud 大学关于破解 Mifare 的论文，大家可以研究下，的确是受益匪浅。（注意是英语的哦。）

The Mifare Hack

Dismantling MIFARE Classic

提供各类智能卡（IC 卡、ID 卡）解密，破解，复制等相关业务以及技术咨询

厂家淘宝网店地址：http://bobylive.taobao.com

Tags: 破解, 安全, RFID, 极客, Mifare, M1, S50, 密钥, 黑客

---

51 Comments

论如何优雅地蹭饭：克隆篡改公司饭卡（M1卡）| 湛江网站建设_湛江企业网站制作_湛江低价网站建设_湛江网站定做
November 12th, 2014 at 01:52 pm

[...] 首先了解M1卡的结构：请参考http://bobylive.com/static/1491 [...]

Reply

论如何优雅地蹭饭：克隆篡改公司饭卡（M1卡）| 中国 X 黑客小组
November 10th, 2014 at 04:12 pm

[...] 首先了解M1卡的结构：请参考http://bobylive.com/static/1491 [...]

Reply

Vincent
November 6th, 2014 at 10:04 pm

如果知道一个扇区的密码但不是你列举的常见的M1卡密钥
那该怎样用M1卡服务程序破解 好像M1卡服务程序没有书密钥的地方

Reply

Sirius
November 8th, 2014 at 12:18 am

可以添加默认密钥文件的，在其目录下以文件形式保存，文件名即key

Reply

Vincent
November 8th, 2014 at 12:21 am

文件后缀名写什么
文件内容写什么

Reply

Sirius
November 13th, 2014 at 11:40 am

这个还真的忘了，你用张别的卡试试，他会自动生成的，按照格式写就好

Reply

Sirius
November 15th, 2014 at 08:54 pm

temp文件夹里有

葛星辰
November 13th, 2014 at 10:13 pm

只会生成dump文件额

论如何优雅地蹭饭：克隆篡改公司饭卡 | PushEAX's Blog
November 6th, 2014 at 07:15 pm

[...] 首先了解M1卡的结构：请参考http://bobylive.com/static/1491 [...]

Reply

PM3实例:克隆篡改公司饭卡（M1卡）-安全之家
November 6th, 2014 at 05:34 pm

[...] 首先了解M1卡的结构：请参考http://bobylive.com/static/1491 [...]

Reply

论如何优雅地蹭饭：克隆篡改公司饭卡（M1卡） - FreeBuf.COM
November 6th, 2014 at 07:01 am

[...] 首先了解M1卡的结构：请参考http://bobylive.com/static/1491 [...]

Reply

路飞
November 3rd, 2014 at 09:03 pm

博主，出现不可以写入怎么解决?
写入问题
有些部分是不可以写！请检查。
扇区:14，块:0
key with write access (A) not know

扇区:14，块:1
key with write access (A) not know

扇区:14，块:2
key with write access (A) not know

Reply

Sirius
November 6th, 2014 at 09:09 am

KeyA未知

Reply

学校水卡破解技术 | 传奇博客
October 24th, 2014 at 06:07 pm

[...] 看到上图我用方框框着的数据了吗？这就是卡扇区的控制段，其中前6字节和后6字节的FFFFFFFFFFFF就是这个扇区的密码，中间的FF078069就是控制位，还不清楚M1卡的结构的可以去看看这篇介绍M1卡结构文章。[...]

Reply

Vincent
October 6th, 2014 at 11:21 am

高频IC卡指南的连接点击不了啊

Reply

Sirius
October 7th, 2014 at 01:16 pm

检测并没问题，请用迅雷试试

Reply

Vincent
October 7th, 2014 at 01:18 pm

嗯 对
右键点迅雷下载可以下
直接点击链接下载不了

Reply

苏州才子
September 25th, 2014 at 03:10 pm

那如果全加密的M1卡是不是就只能暴力破解了?

Reply

Sirius

September 25th, 2014 at 04:36 pm

嗅探，利用算法漏洞可以算出key

Reply

« Previous Page 1 2

Write a new comment

NickName *

Email *

Website

http://

Content *

Submit

Previous Text: 入手 RFID 工具 ACR122U

Next Text: 2013 - 11 - 13