精锐 E、ET199 通讯协议分析之模拟锁基础

看雪 ID: YangCoCol

前言：

众所周知，深思洛克和坚石诚信可算得上是加密锁行业龙头，原因是他们都使用了智能卡芯片做为加密锁主控，同时又内嵌了国际先进的 C51 锁内编程技术，使得加密锁在理论上达到不可复制。

本篇文章将对深思的精锐 E 和坚石的 ET199 做简单分析，总结并对比两款锁的通讯协议的异同，数据的加解密，给读者提供开发模拟锁基本思路。

本文并没有长篇幅详细的介绍，只是给出重要环节的数据和调试分析，这就需要读者要有一定的 USB 协议、软件调试、硬件开发的基础，如果读者想进一步了解制作模拟锁完整过程，包括加密数据获取解密、算法分析工具编写、USB 固件编写等等，请与作者联系，展开进一步的技术交流。

免责声明：

本文纯属技术交流之贴，并无任何商业目的，若读者利用此贴对任何第三方企业或个人造成任何形式的侵害都与作者无关，作者对其概不负责，亦不承担任何法律责任。

1. 精锐 E

外观：

枚举过程分析：

用协议分析工具抓取设备枚举过程，得到的 HID 报告描述符数据如下：

```
06 a0 ff 09 01 a1 01 09 02 a1 00 06 a1 ff
09 03 09 04 15 00 25 7f 35 00 45 ff 85 80 75 08 95 3f b1 02      ----- 63 Bytes
09 05 09 06 15 00 25 7f 35 00 45 ff 85 01 75 08 96 01 01 b1 02   ----- 257 Bytes
09 07 09 08 15 00 25 7f 35 00 45 ff 85 02 75 08 95 ef b1 02      ----- 239 Bytes
09 09 09 0a 15 00 25 7f 35 00 45 ff 85 03 75 08 95 df b1 02      ----- 223 Bytes
09 0b 09 0c 15 00 25 7f 35 00 45 ff 85 04 75 08 95 cf b1 02      ----- 207 Bytes
09 0d 09 0e 15 00 25 7f 35 00 45 ff 85 05 75 08 95 bf b1 02      ----- 191 Bytes
09 0f 09 10 15 00 25 7f 35 00 45 ff 85 06 75 08 95 af b1 02      ----- 175 Bytes
09 11 09 12 15 00 25 7f 35 00 45 ff 85 07 75 08 95 9f b1 02      ----- 159 Bytes
09 13 09 14 15 00 25 7f 35 00 45 ff 85 08 75 08 95 8f b1 02      ----- 143 Bytes
09 15 09 16 15 00 25 7f 35 00 45 ff 85 09 75 08 95 7f b1 02      ----- 127 Bytes
09 17 09 18 15 00 25 7f 35 00 45 ff 85 0a 75 08 95 6f b1 02      ----- 111 Bytes
```

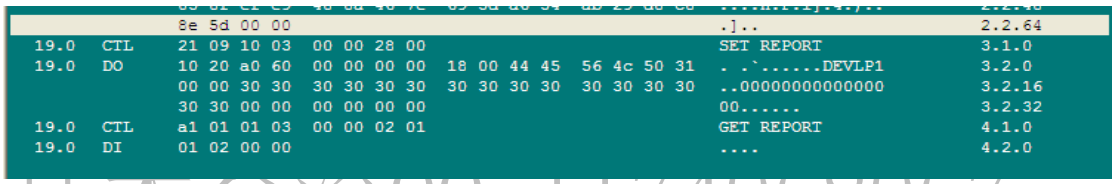
```
09 19 09 1a 15 00 25 7f 35 00 45 ff 85 0b 75 08 95 5f b1 02      ----- 95 Bytes
09 1b 09 1c 15 00 25 7f 35 00 45 ff 85 0c 75 08 95 4f b1 02      ----- 79 Bytes
09 1d 09 1e 15 00 25 7f 35 00 45 ff 85 0d 75 08 95 3f b1 02      ----- 63 Bytes
09 1f 09 20 15 00 25 7f 35 00 45 ff 85 0e 75 08 95 37 b1 02      ----- 55 Bytes
09 21 09 22 15 00 25 7f 35 00 45 ff 85 0f 75 08 95 2f b1 02      ----- 47 Bytes
09 23 09 24 15 00 25 7f 35 00 45 ff 85 10 75 08 95 27 b1 02      ----- 39 Bytes
09 25 09 26 15 00 25 7f 35 00 45 ff 85 11 75 08 95 1f b1 02      ----- 31 Bytes
09 27 09 28 15 00 25 7f 35 00 45 ff 85 12 75 08 95 17 b1 02      ----- 23 Bytes
09 29 09 2a 15 00 25 7f 35 00 45 ff 85 13 75 08 95 0f b1 02      ----- 15 Bytes
09 2b 09 2c 15 00 25 7f 35 00 45 ff 85 14 75 08 95 07 b1 02      ----- 7 Bytes
c0 c0
```

以上为其特性报告数据，报告数据长度在 7 - 257 字节之间。

通讯数据安全性分析：

用协议分析工具获取用 **VB** 编写的例子和锁的通讯数据，获取数据如下：

下图使用默认密码“**0000000000000000**”，**VB** 调试并用 **BusHound** 抓取数据，输入输出报告都为明文。



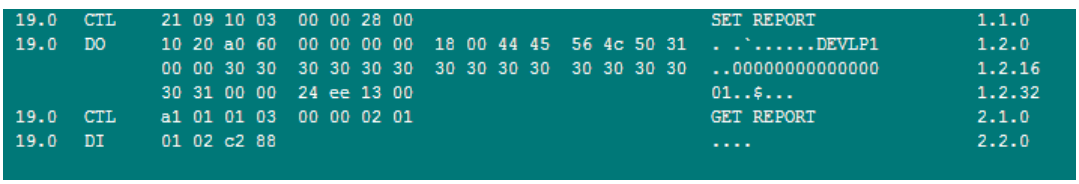
```
                8e 5d 00 00                                      .]..                2.2.64
19.0   CTL      21 09 10 03  00 00 28 00                         SET REPORT          3.1.0
19.0   DO       10 20 a0 60  00 00 00 00  18 00 44 45  56 4c 50 31  . .`......DEVLP1   3.2.0
                00 00 30 30  30 30 30 30  30 30 30 30  30 30 30 30  ..00000000000000    3.2.16
                30 30 00 00  00 00 00 00                         00......            3.2.32
19.0   CTL      a1 01 01 03  00 00 02 01                         GET REPORT          4.1.0
19.0   DI       01 02 00 00                                      ....                4.2.0
```



```
'verify pin
Dim pin(0 To 15) As Byte                ' device PIN
For i = 0 To UBound(pin)
    pin(i) = Asc(Mid("0000000000000000", i + 1, 1))
Next

bRet = EleVerifyPin(edc, pin(0))
If bRet Then
    info = "verify device PIN success"
Else
    dwErrRet = EleGetLastError()
    info = "verify device PIN failed! error code: " + Str(dwErrRet)
    List1.AddItem info
    Exit Sub
End If
List1.AddItem info
```

将密码修改，输出报告依然为明文，并且输入报告后两个字节数值发生变化，表示密码验证失败。



```
19.0   CTL      21 09 10 03  00 00 28 00                         SET REPORT          1.1.0
19.0   DO       10 20 a0 60  00 00 00 00  18 00 44 45  56 4c 50 31  . .`......DEVLP1   1.2.0
                00 00 30 30  30 30 30 30  30 30 30 30  30 30 30 30  ..00000000000000    1.2.16
                30 31 00 00  24 ee 13 00                         01..$...            1.2.32
19.0   CTL      a1 01 01 03  00 00 02 01                         GET REPORT          2.1.0
19.0   DI       01 02 c2 88                                      ....                2.2.0
```

```
'verify pin
Dim pin(0 To 15) As Byte                ' device PIN
For i = 0 To UBound(pin)
    pin(i) = Asc(Mid("0000000000000001", i + 1, 1))
Next

bRet = EleVerifyPin(edc, pin(0))
If bRet Then
    info = "verify device PIN success"
Else
    dwErrRet = EleGetLastError()
    info = "verify device PIN failed! error code: " + Str(dwErrRet)
    List1.AddItem info
    Exit Sub
End If
List1.AddItem info
```

小结：

通过以上两条数据的分析，可以基本确定不同命令码由报告描述符中的 **xx** 中的数决定，**01 —> 获取密码验证结果；10 —> 密码验证**。

有了这两条数据就可以为模拟锁提供最基本的登录模拟参考。

下面对精锐 **E** 的核心功能(代码移植运行)进行分析：

```
19.0   CTL    21 09 12 03  00 00 18 00                          SET REPORT                1.1.0
19.0   DO     12 0f 90 30  00 00 00 00  07 00 4d 4f  44 55 4c 45  ...0......MODULE         1.2.0
              31 ff ff ff  02 02 93 7c                          1.......                  1.2.16
19.0   CTL    a1 01 01 03  00 00 02 01                          GET REPORT                2.1.0
19.0   DI     01 02 00 00                                       ....                      2.2.0
19.0   CTL    21 09 11 03  00 00 20 00                          SET REPORT                3.1.0
19.0   DO     11 18 90 3a  00 00 00 00  10 00 30 31  32 33 34 35  ...:......012345         3.2.0
              36 37 38 39  61 62 63 64  65 66 4c 45  31 ff ff ff  6789abcdefLE1...        3.2.16
19.0   CTL    a1 01 01 03  00 00 02 01                          GET REPORT                4.1.0
19.0   DI     01 12 66 65  64 63 62 61  39 38 37 36  35 34 33 32  ..fedcba98765432          4.2.0
              31 30 00 00                                       10..                      4.2.16
```

```
sIn = "0123456789abcdef"

info = "bubblesort input:    " + sIn
List1.AddItem info

bRet = EleExecute(edc, "MODULE1", sIn, Len(sIn), Output(0), 1024, RealLen)
If bRet Then
    info = "execute bubblesort success"
    info = "bubblesort result:  "
    For index = 0 To Len(sIn) - 1
```

小结：

传入到加密锁的的字符串“**0123456789abcdef**”,经过所内代码运算，可以通过抓取的数据看到返回数据为“**fedcba9876543210**”,我们可以直接确定所内代码功能为“字符串逆序”。

我们可以看到，核心功能的数据基础通讯根本没有加密，也就是说，通讯协议上很脆弱，不用 **OD** 等调试工具就能做出核心功能的软模拟或硬模拟。

通讯数据的安全性就集中在了用户的移植代码上，数据的保护需用户自行去做，而且只有这一个安全屏障而已，极易被攻击。

而出于软件运行效率的考虑，一般移植代码的复杂度和代码量都不会太大，这又为数据分析带来更大的便利。

总结：

其实分析到这里，已经没有必要再分析下去，原因很简单，精锐 E 加密锁的模拟思路清晰可见，而且通讯协议也清晰明了，只要对 USB 协议清楚、加密锁工作原理明白、有一定的数学基础、略懂软件调试的人做出模拟锁还是不难的。

针对上面的测试我在这做个简单的总结，XX 的报告为获取返回值，XX 的报告为密码验证，XX 的报告为执行锁内可执行模块，XX 的报告为选取加密锁中指定可执行模块。

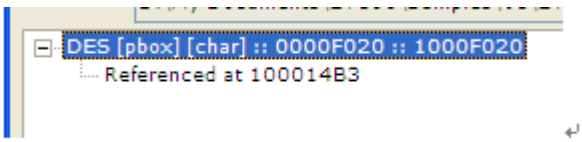
特点总结：1.基础通讯无加密。2.数据量较小。3.不同命令 SETUP 包区分。4.对用户代码的强度依赖大。

==========

2. ET199

外观：

通讯加密：DES



加密方式：单次随机密钥交换

Device	Phase	Data	Description	Cmd.Phase.Ofs(x
19.2	DO	00 06 00 00 00 06 00 47 47 4b 00 00 00 00 00 00	.......GGK......	1.1.0
		00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	1.1.16
		00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	1.1.32
		00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	1.1.48
19.1	DI	00 42 00 00 00 3a b7 b6 f3 86 c8 d4 fe 49 8c ea	.B...:.......I..	2.1.0
		94 fd 3f 4b 02 a6 81 ac cb 72 e7 dc ff a6 12 b9	..?K.....r......	2.1.16
		b7 fd 8a fc 68 f9 6f 00 f1 35 a5 6e df 8c b3 46	....h.o..5.n...F	2.1.32
		54 54 3b 8c 63 dc c9 80 3f 84 4b 25 c2 3d 66 5c	TT;.c...?.K%.=f\	2.1.48
19.1	DI	00 42 00 3a 00 08 8e 35 47 6a cf c6 90 00 31 6f	.B.:...5Gj....1o	3.1.0
		2d 0c 4e 90 54 05 31 c3 44 28 a2 bd 7e 57 04 f8	-.N.T.1.D(...W..	3.1.16
		9c d3 b6 10 cd a8 65 1d a0 53 d6 7a b7 ea da 6c	......e..S.z...l	3.1.32
		71 02 55 6b a4 09 26 5a d6 2c d1 01 3e dc 48 f4	q.Uk..&Z.,..>.H.	3.1.48

两包输入报告数据计算出锁生命周期所使用的 DES 密钥，OD 跟踪如下：

```
100016C4  .  E8 87300000     call ET199_32.10004750                  <--计算动态DES密钥
100016C9  .  0FB64424 17     movzx eax,byte ptr ss:[esp+0x17]
100016CE  .  8B5424 22       mov edx,dword ptr ss:[esp+0x22]
100016D2  .  69C0 38010000   imul eax,eax,0x138
100016D8  .  8B4C24 26       mov ecx,dword ptr ss:[esp+0x26]
100016DC  .  83C4 08         add esp,0x8
100016DF  .  5F              pop edi
100016E0  .  8990 9DFF0010   mov dword ptr ds:[eax+0x1000FF9D],edx
100016E6  .  8988 A1FF0010   mov dword ptr ds:[eax+0x1000FFA1],ecx
```

```
地址       HEX 数据                                        ASCII
1000FF9D  01 CE CB D0 5B 7F 98 82  00 00 00 00 00 00 00 00  ....[...........
1000FFAD  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
1000FFBD  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

OD 分析数据加解密：

```
10003CEA  .  83FE 01         cmp esi,0x1
10003CED  .v 75 14           jnz short ET199_32.10003D03             <--判断是否需要DES解密
10003CEF  .  8B45 0C         mov eax,[arg.2]
10003CF2  .  8D5424 31       lea edx,dword ptr ss:[esp+0x31]
10003CF6  .  52              push edx
10003CF7  .  8D4C24 7D       lea ecx,dword ptr ss:[esp+0x7D]
10003CFB  .  E8 80FDFFFF     call ET199_32.10003A80                  <--动态密钥DES解密
10003D00  .  83C4 04         add esp,0x4
10003D03  >  66:0FB64C24 34  movzx cx,byte ptr ss:[esp+0x34]
10003D09  .  33C0            xor eax,eax
10003D0B  .  8A6424 33       mov ah,byte ptr ss:[esp+0x33]
10003D0F  .  66:0BC1         or ax,cx
10003D12  .  0FB7C0          movzx eax,ax
10003D15  .  66:3D 0004      cmp ax,0x400
10003D19  .v 0F83 95000000   jnb ET199_32.10003DB4                   <--校验结果比较
10003D1F  .  8A5C24 36       mov bl,byte ptr ss:[esp+0x36]
10003D23  .  8B4D 08         mov ecx,[arg.1]
```

```
100014B0  >  0FB688 20F00010  movzx ecx,byte ptr ds:[eax+0x1000F020]  <--DES P矩阵取值
100014B7  .  8A90 18FA0010    mov dl,byte ptr ds:[eax+0x1000FA18]
100014BD  .  3A91 E4FA0010    cmp dl,byte ptr ds:[ecx+0x1000FAE4]
100014C3  .  0F95C1           setne cl
100014C6  .  8888 78FA0010    mov byte ptr ds:[eax+0x1000FA78],cl
100014CC  .  83C0 01          add eax,0x1
100014CF  .  83F8 20          cmp eax,0x20
100014D2  .^ 7C DC            jl short ET199_32.100014B0
```

总结：

基础通讯有 **DES** 加密，存在密钥交换过程，存在随机数干扰。

特点总结：1.基础通讯有加密。2.通讯数据量固定，3.不同命令包在 APDU 中。

作者后述：

目前，几大软件行业企业几乎都是用的以上两家的加密锁，模拟锁带来的暴力已经促使一条灰色产业链的诞生，而以上两款加密锁的某些缺陷，也是模拟锁能被开发出的理论基础。