平安安全应急响应中心
PINGAN Security Response Center

看雪

新视角下的安全攻防对抗

平安SRC线上沙龙系列主题活动 第二期

物理安全与近源渗透威胁分析

杨文韬

安全研究员

近源渗透的5个trick

1、投递恶意的USB设备

2、社会工程学

3、传统锁具的撬锁

4、RFID锁具攻防

5、无线电锁具安全

6、绕过Windows锁屏和Bitlocker

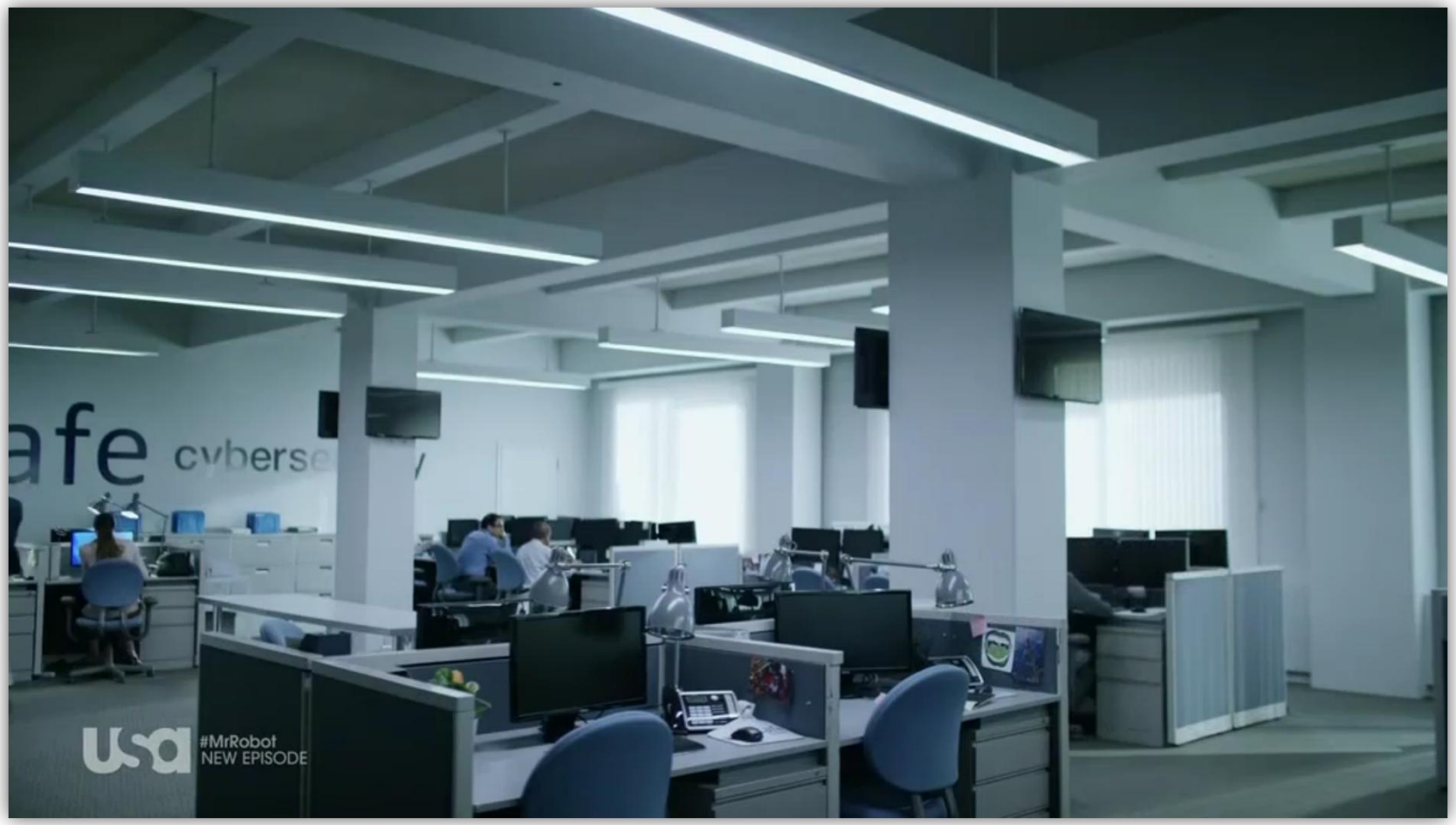
7、植入硬件后门

Trick1: 投递恶意的USB设备

Trick 1：投递恶意的USB设备

可能是最为知名近源渗透手段。

在目标建筑物附件散播恶意的USB设备，在企业员工拾取并插入计算机时植入木马。



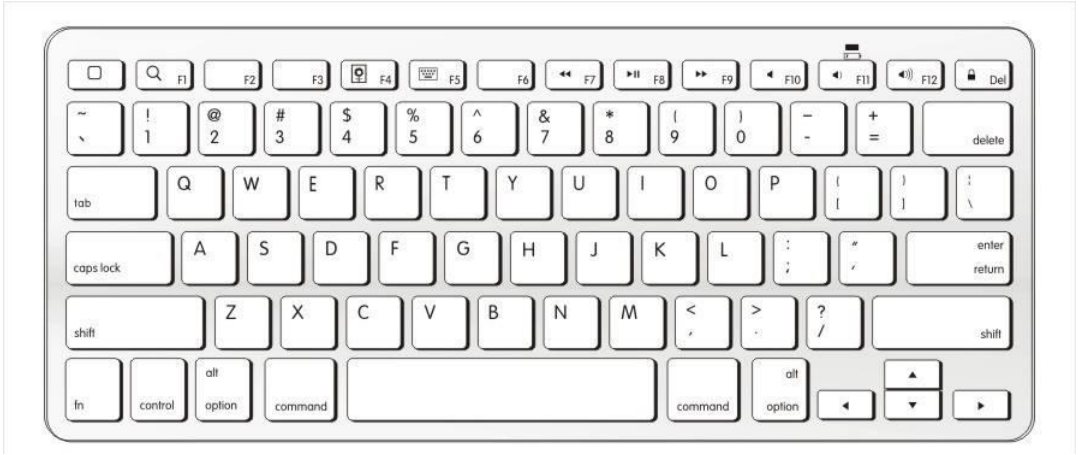
MR.Robot S01E06

Trick 1：HID注入攻击

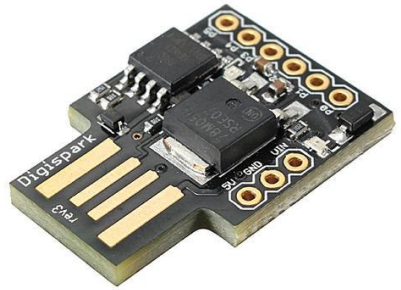
USB相关的攻击手段之一：

HID注入攻击，有时称为BADUSB攻击。

即通过模拟键盘输入，执行恶意的指令，以此进行攻击。



缩小



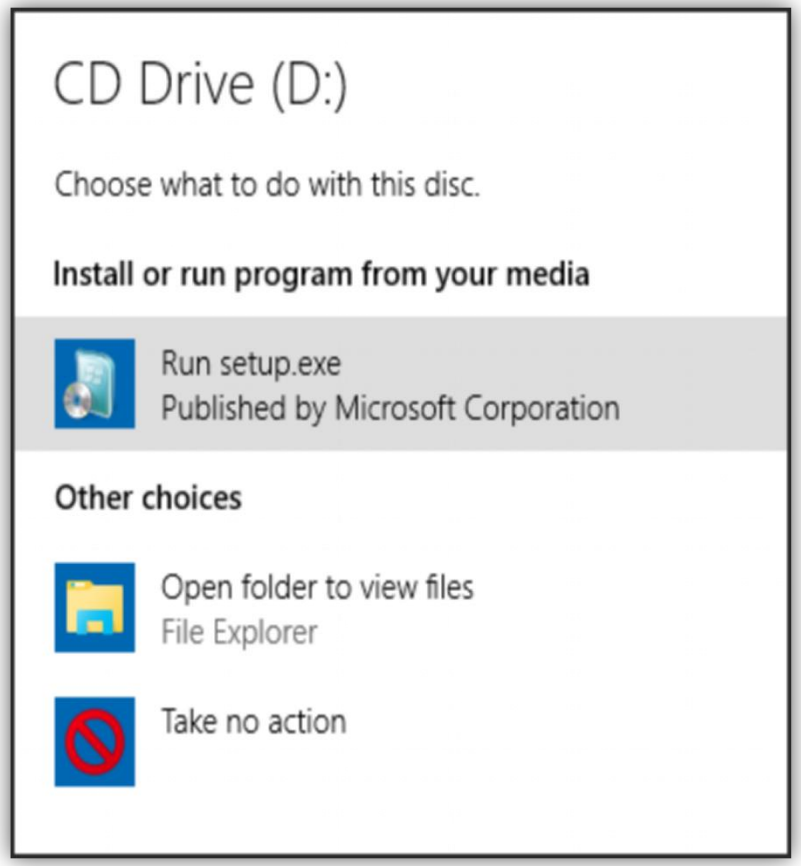
Trick 1：死去的Autorun突然开始攻击我

HID攻击的缺陷：

1. 屏幕会有命令行窗口，可以看到短暂的输入过程
2. 容易受到系统不同，或用户操作的影响

USB相关的攻击手段之二：Autorun

Autorun是Windows的一项机制，最早在Windows95被引入。被用于新设备接入后，自动执行一系列操作。例如插入驱动程序光盘时自动运行安装程序。



Trick 1：死去的Autorun突然开始攻击我

历史悠久。曾经造成了严重的安全问题。

现代Windows系统对其添加了安全审核。使其的执行受多个限制：

- 限制1：只允许DRIVE_FIXED（固定设备）的CD-ROM驱动器开启Autorun
- 限制2：用Autoplay替代Autorun（即不会在没有任何操作的情况下执行命令）

NoDriveTypeAutoRun [edit]

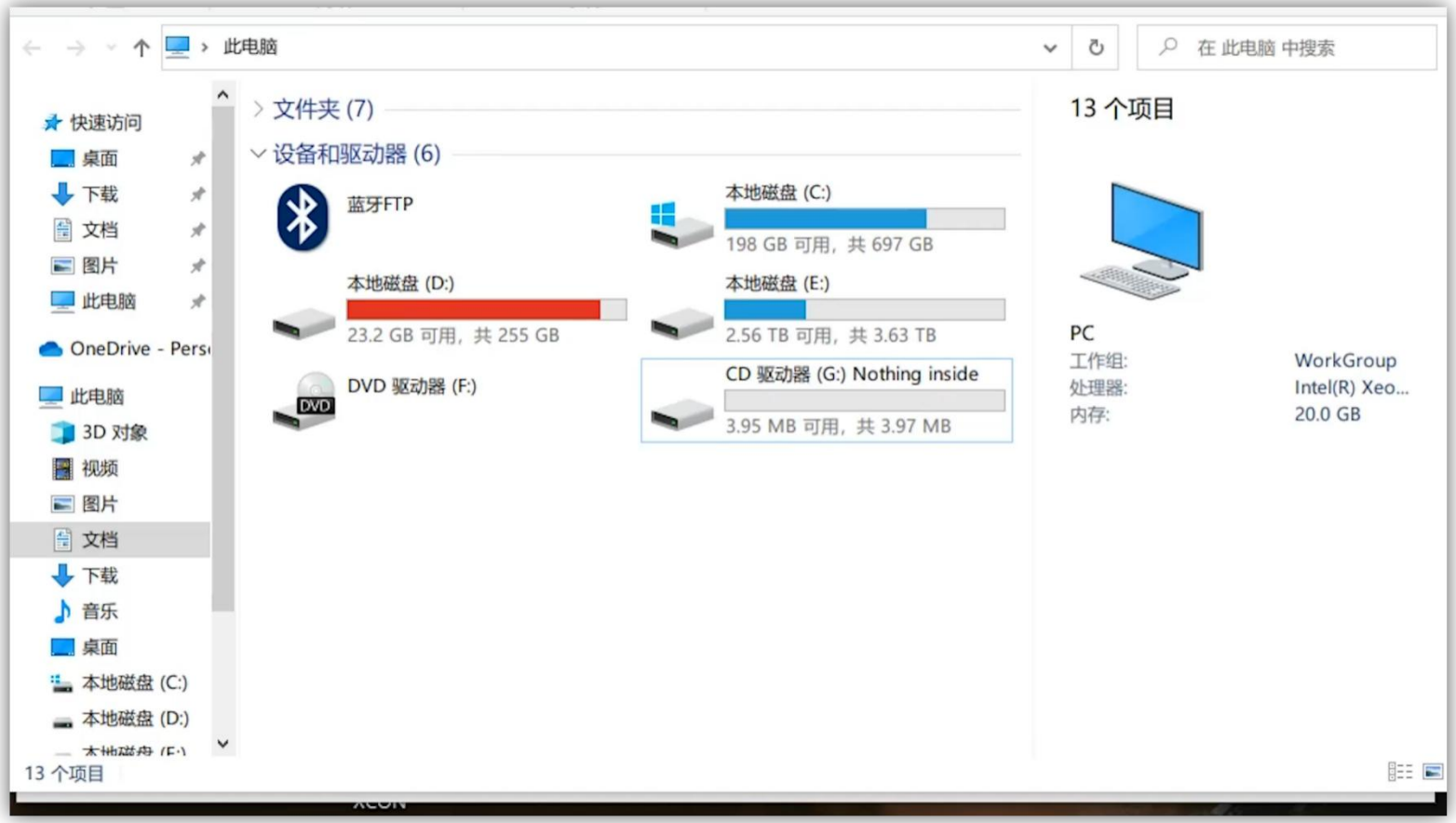
`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`

Entry name	Data type	Range	Default
`NoDriveTypeAutoRun`	REG_DWORD	0x00 to 0xFF	0x95 or 0x91

Trick 1：死去的Autorun突然开始攻击我

Autoplay使得攻击者不能在完全无交互的情况下执行命令。

但需要的交互也非常少：通过任意方法打开驱动器，即可执行命令。



Trick 1：死去的Autorun突然开始攻击我

通过在存储设备的根目录下放置一个autorun.inf，可以配置自动运行

Trick 1：死去的Autorun突然开始攻击我

难点：存储设备需要为DRIVE_FIXED（固定设备）的CD-ROM驱动器。但USB设备的类型完全由USB设备本身的参数决定，通过修改DBINQUITY，可以伪造任意设备。

方法1：

有些U盘的量产工具提供了相关功能。

可以在U盘上划分一个单独的空间，伪装成CD-ROM驱动器。

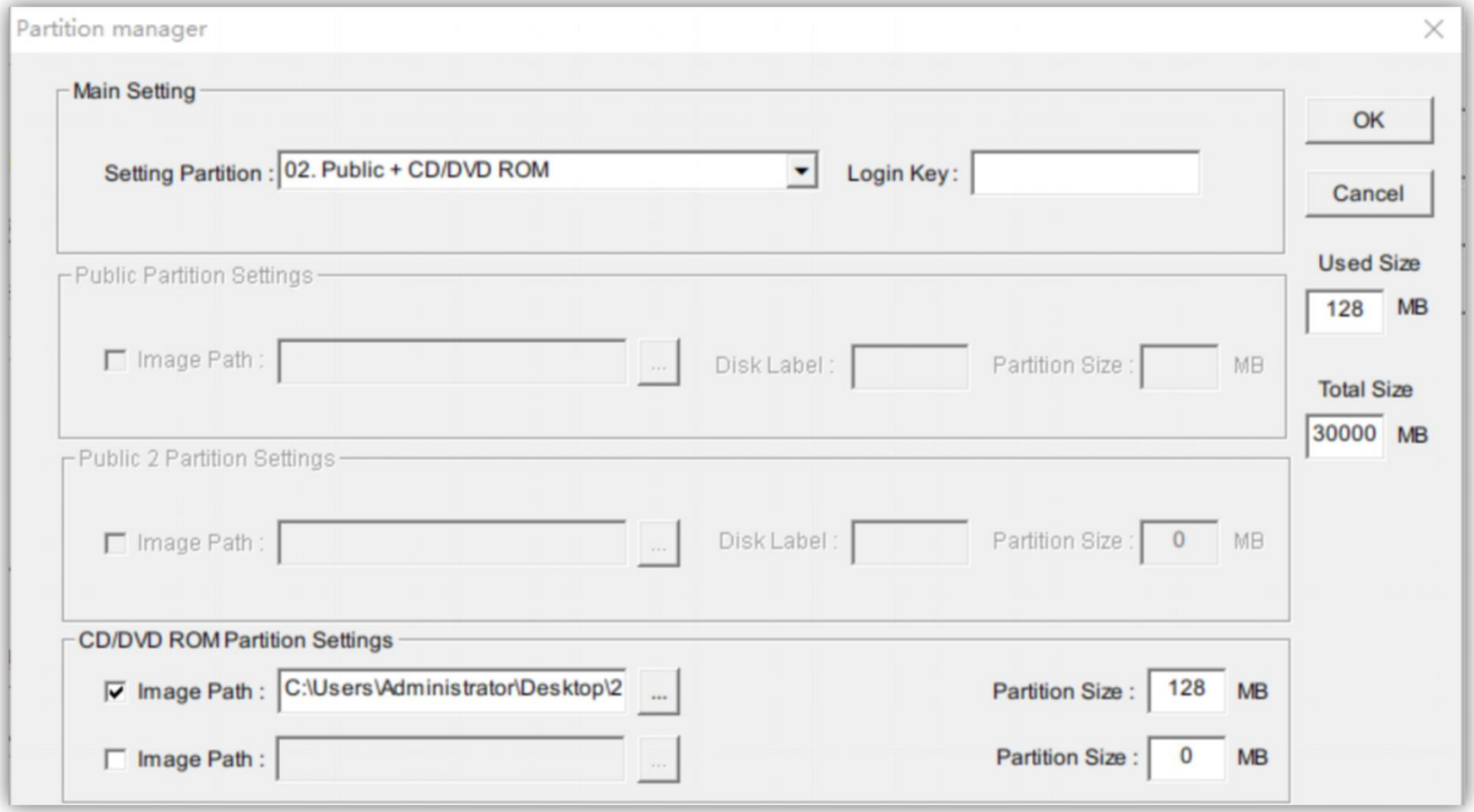
以Innostor（银灿）917MP主控芯片的U盘为例：

Trick 1：死去的Autorun突然开始攻击我

U盘量产工具可以创建一个支持Autorun的特殊分区

在量产工具的Partition Manager功能中，可以设置U盘为

Public+CD/DVD ROM模式



Trick 1：死去的Autorun突然开始攻击我

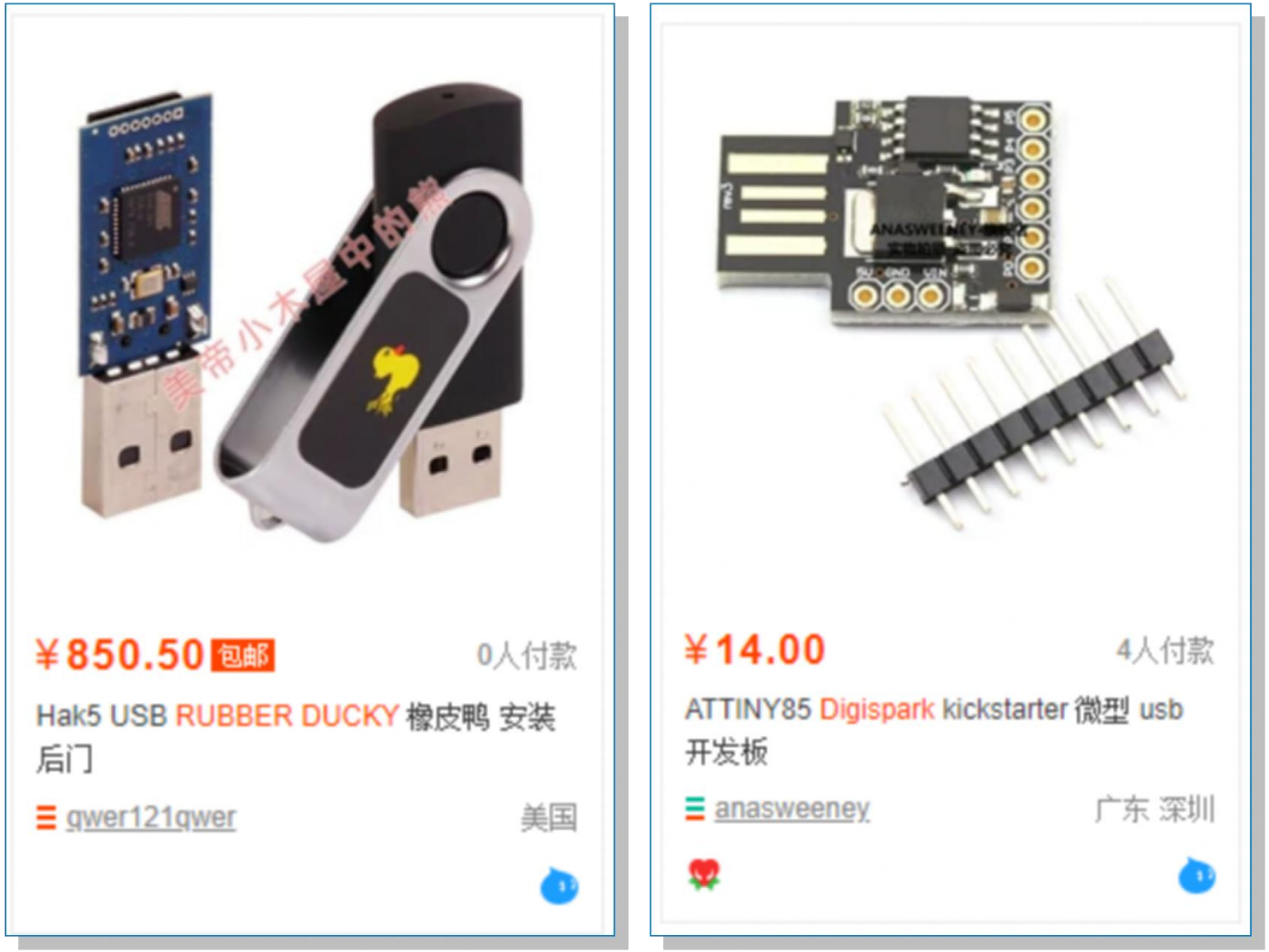
常见的HID攻击设备

1、橡皮鸭：

最早产品化的攻击设备，可以插入MicroSD卡

2、Digispark：

最廉价的攻击设备，但只有键盘功能。而且无法装入U盘外壳

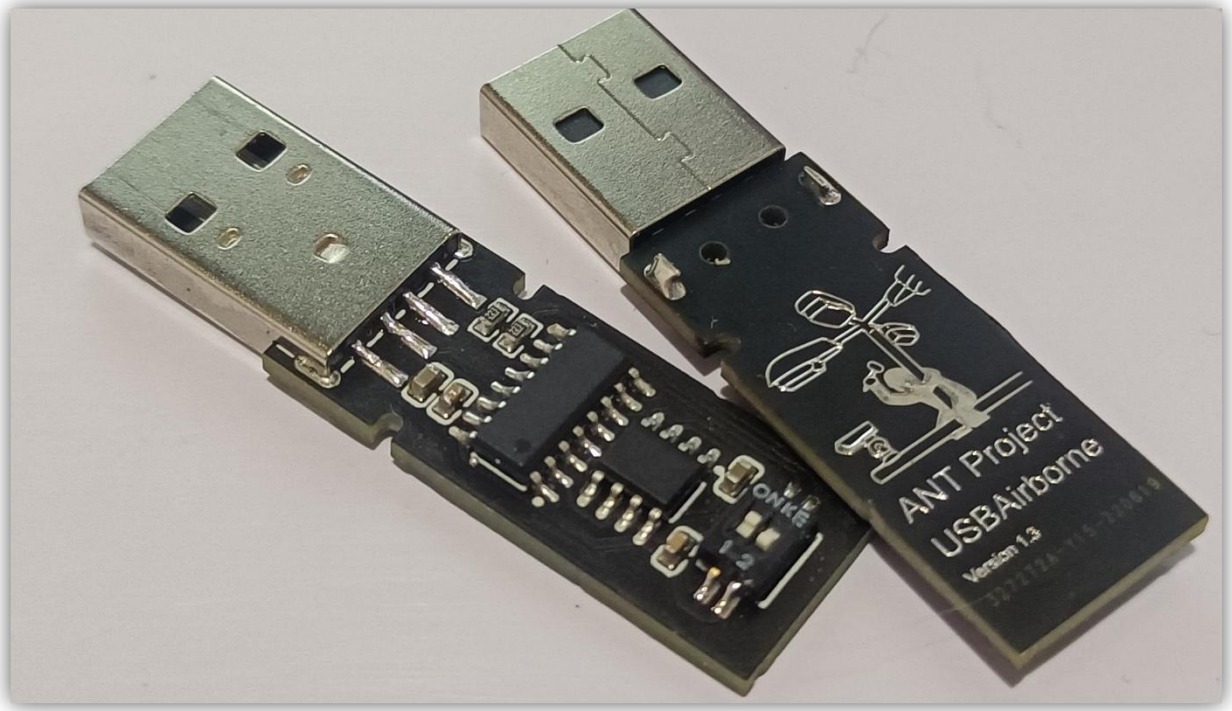


Trick 1：死去的Autorun突然开始攻击我

方法2：

USBAirborne是专用于近源渗透的攻击设备。有着以下优势：

- 单个成本低于10元（以塑料外壳计算）
- 标准G2板型，适配通用U盘外壳
- 自带4MB的存储空间，用于存储Payload
- 支持BadUSB和Autorun攻击



- 软硬件皆开源，可二次开发

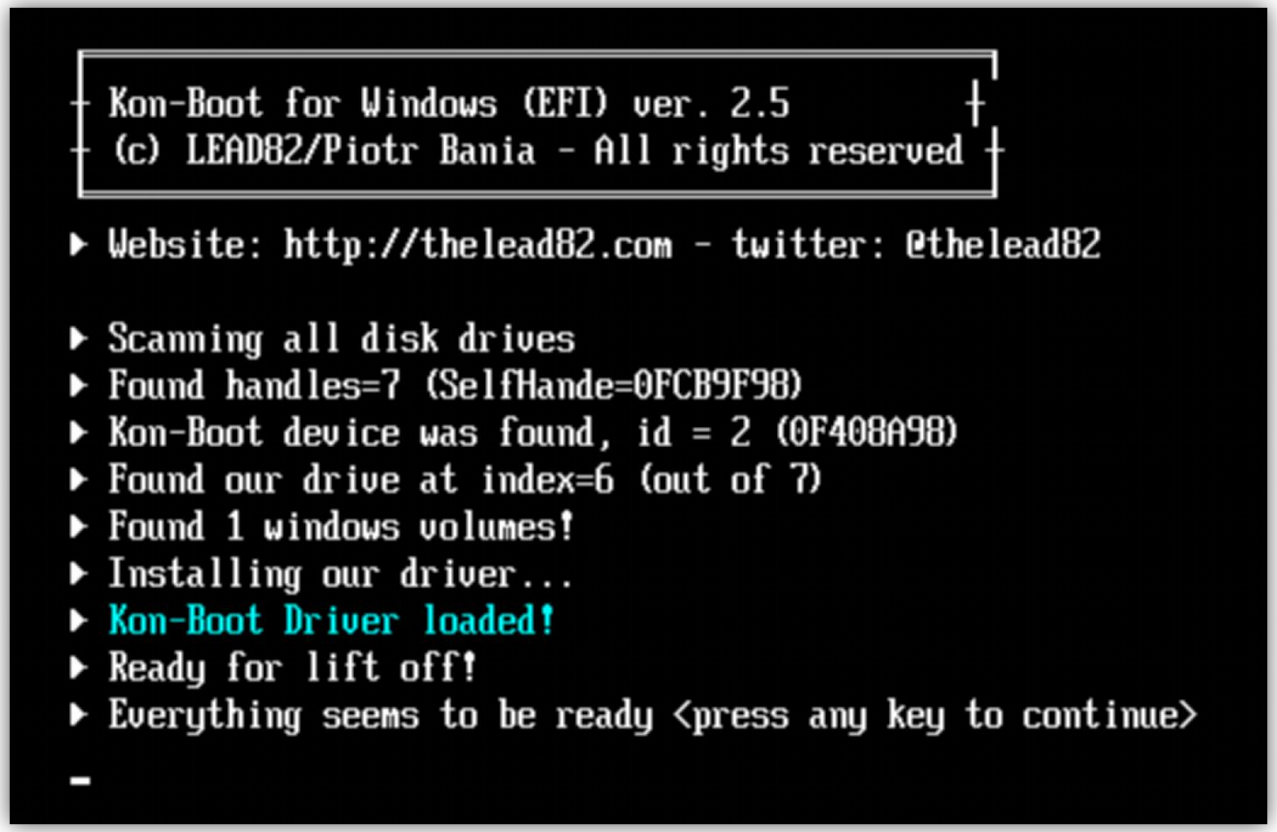
Trick2: 绕过Windows锁屏和Bitlocker

Trick2：绕过Windows锁屏和Bitlocker

方法1：Kon-boot

Kon-Boot可以绕过绝大多数Windows版本的开机密码。

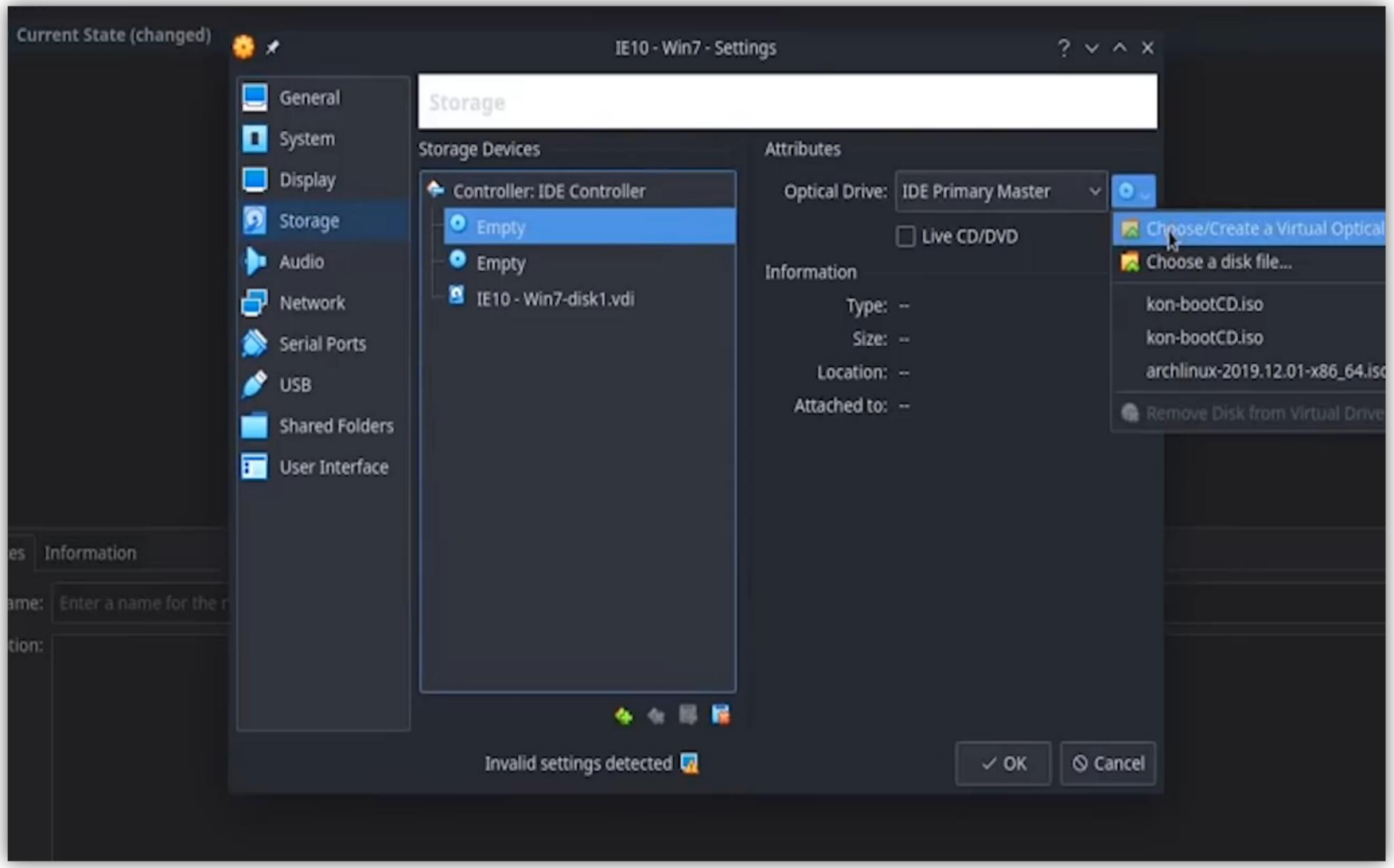
针对使用网络验证的Windows 10，无法绕过开机密码。但可以选择添加新账户，会安装Shift键后门。



Trick2：Kon-Boot

将KON-Boot安装到U盘后，在开机时选择从U盘引导。

KON-Boot将会运行，并使得Windows密码失效



Trick2：Kon-Boot的缺陷

Kon-Boot可以满足大多数渗透场景的需求，但它有着几个缺点：

1、 Kon-Boot绕过密码的成功率差强人意，经常需要重试

2、是付费软件，全功能版价格为140美元

3、无法绕过Bitlocker磁盘加密

Trick2：GrabAccess

和Kon-Boot类似，GrabAccess也是密码绕过工具。其优点有：

1. 免费，并基于GPL协议开源
2. 可以绕过Bitlocker植入后门
3. 只要引导环境符合要求，成功率接近百分百
4. 自动化植入木马。只需要一步操作，耗时短，适合近源渗透场景

Trick3: 社会工程学

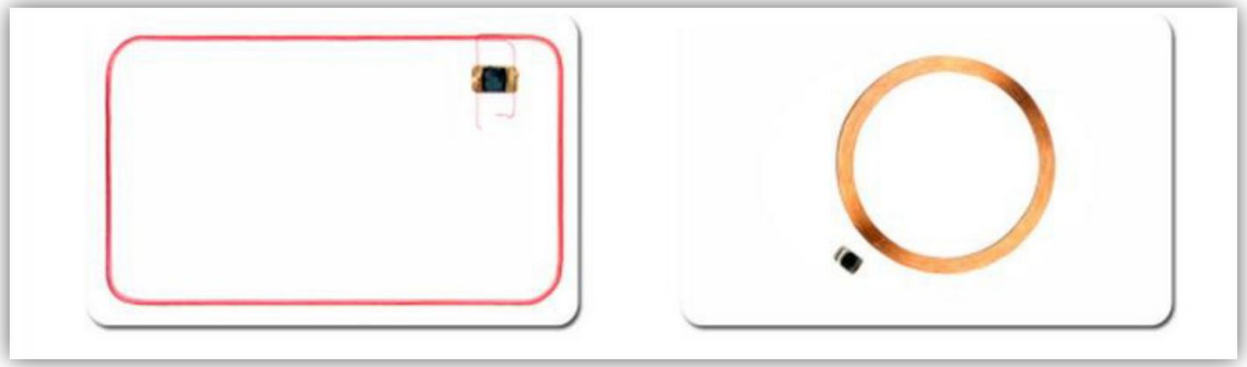
Trick3：社会工程学

1. **伪装访客**
    a. 伪装为外卖员、快递员
    b. 伪装为面试者、维修工
2. **与设备相关的水坑攻击/窃密**
    a. BadUSB、内置后门的外设（如键盘）
    b. 废弃设备中的信息泄露
3. **盗取访问凭证**
    a. 工牌、门禁卡的卡面仿照
    b. 针对NFC卡的UID盗取

MR.Robot S01E05

Trick4: RFID锁具攻防

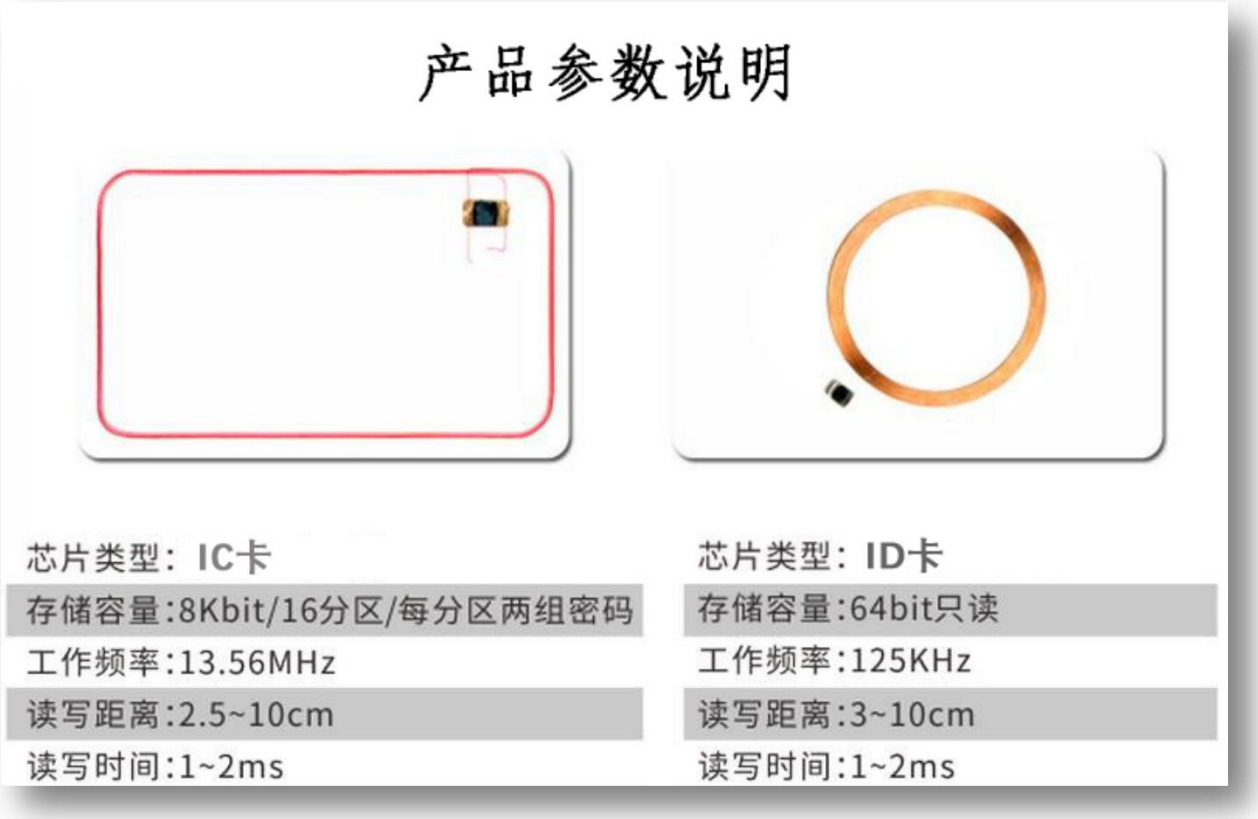
Trick4：RFID锁具攻防



Trick4：RFID锁具攻防

ID卡与IC卡：

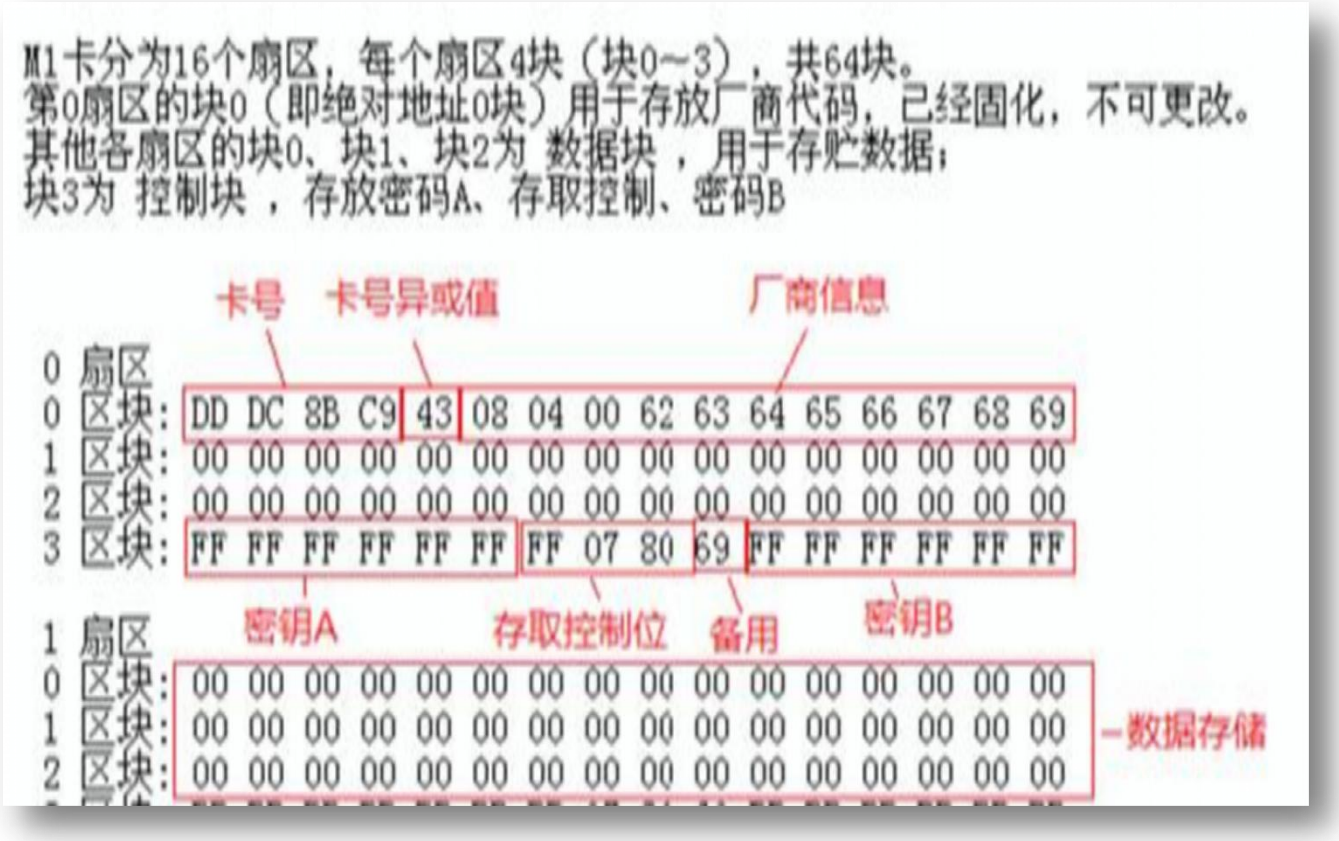
- ID卡较为古老，但廉价
- ID卡只有一个ID号，无法存储数据
- IC卡内部有存储器，并且可以加密数据
- IC卡以NXP公司的Mifare为主
- Mifare卡的存储空间分为1K版和4K版
- CPU卡在正常设计的情况下极难破解



Trick4：RFID锁具攻防——Mifare卡破解

Mifare S50卡的结构：

1. 共有16个扇区，每个扇区4个区块
2. 扇区0的区块0为厂商信息，只读
3. 扇区0的区块0-3为卡片UID
4. 扇区0区块0的第5位为卡片类型（SAK）
5. SAK 08代表S50，18代表S70，20和28代表CPU卡
6. 每扇区的第三区块为密钥和存取控制



Trick4：RFID锁具攻防——Mifare卡破解

M1卡实战中常见的安全问题：

1. 弱密钥或默认密钥
2. 只校验UID，造成加密失效
3. 使用了CPU卡，却只模拟M1卡使用

攻击手段：

1. 安卓手机的NFC读写
2. PN532破解一般加密
3. Proxmark3或变色龙破解全加密卡

Trick4：RFID锁具攻防——Mifare卡破解

M1卡破解实战——基于带有NFC的手机

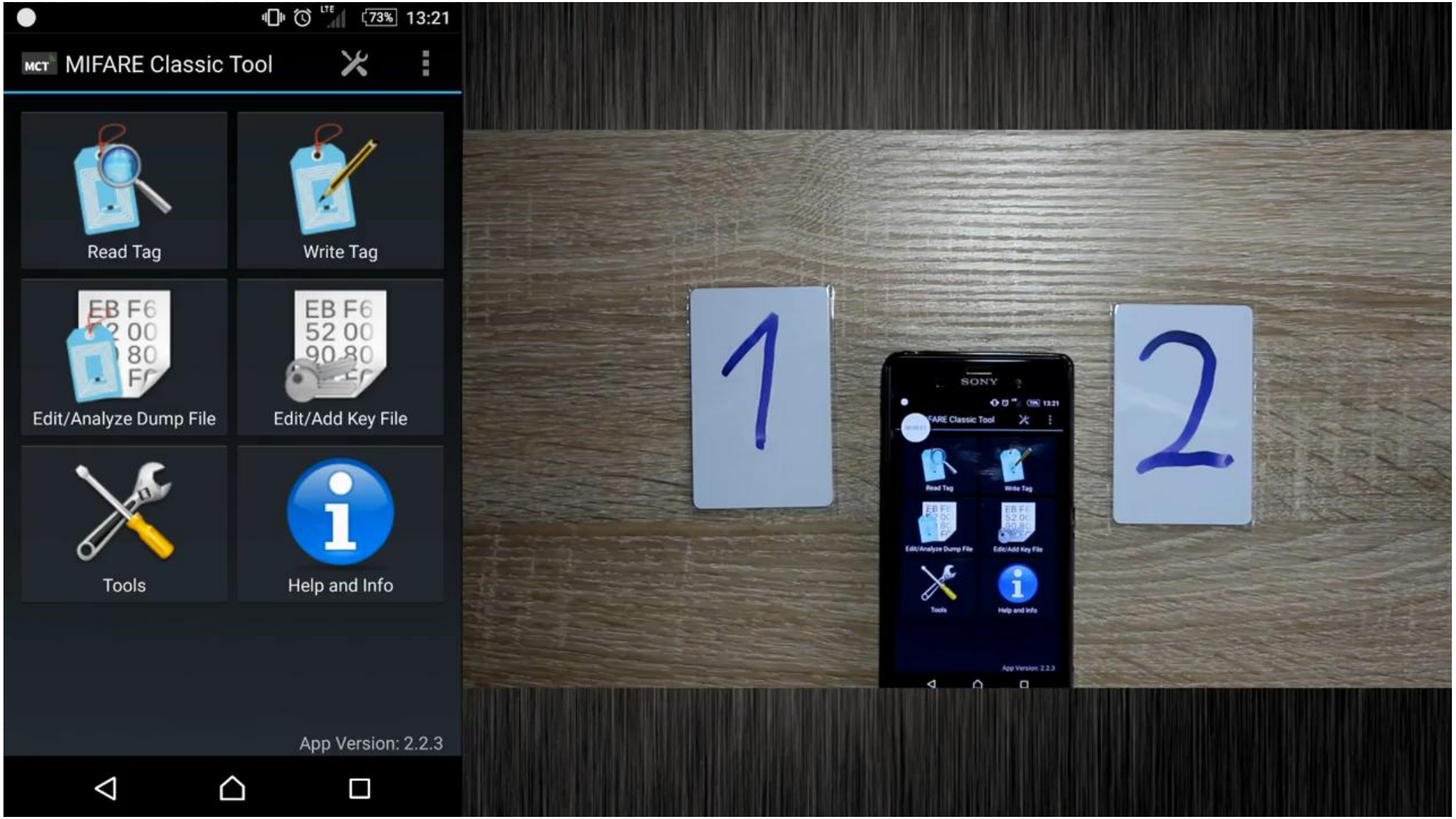
1、准备白卡：

- UID可擦写的卡

2、相关工具（手机需支持NFC功能）：

- MIFARE Classic Tool：读写卡与爆破
- M Tools:快速读取UID
- NFC卡模拟：读和伪装UID（需Root）

Trick4：RFID锁具攻防——Mifare卡破解

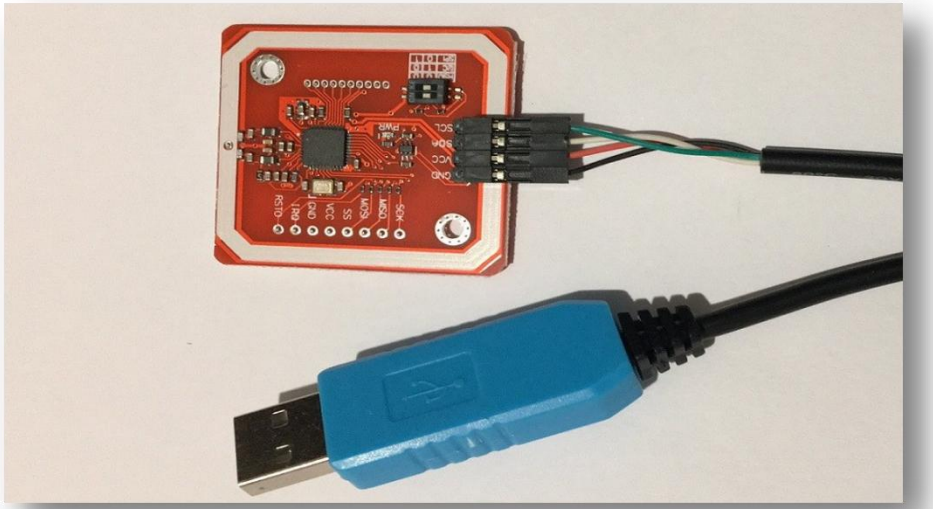


Trick4：RFID锁具攻防——Mifare卡破解

M1卡破解实战——基于PN532

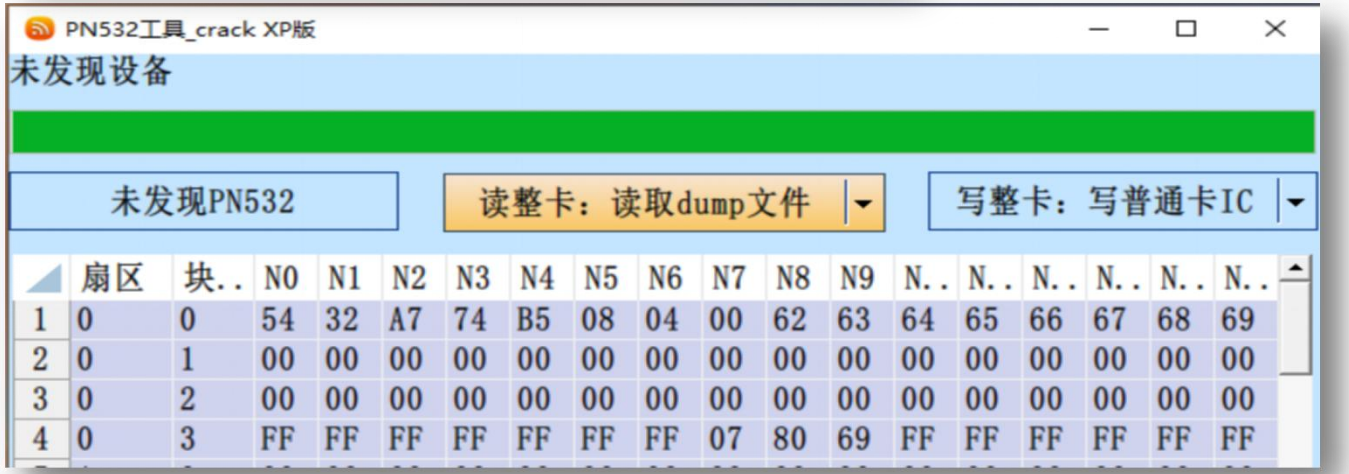
1. 准备设备（PN532）：

- PN532模块一个
- UART转USB模块一个



2. 安装串口驱动

3. 使用工具破解密钥、读写卡



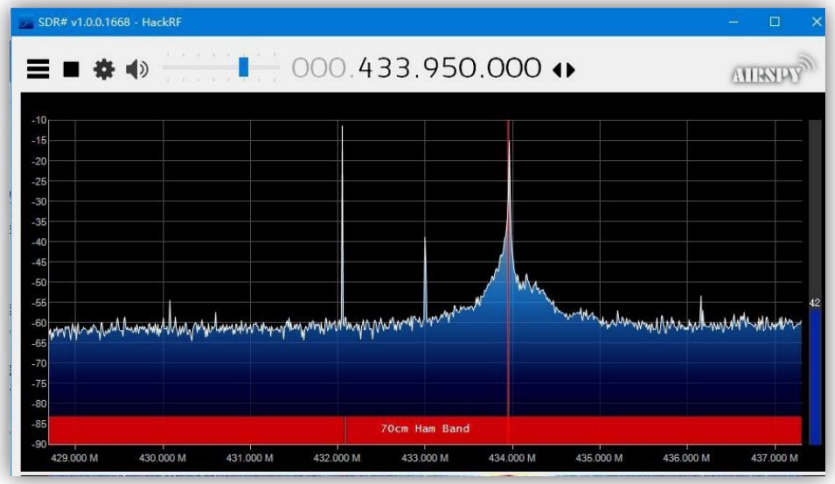
	扇区	块..	N0	N1	N2	N3	N4	N5	N6	N7	N8	N9	N..	N..	N..	N..	N..	N..
1	0	0	54	32	A7	74	B5	08	04	00	62	63	64	65	66	67	68	69
2	0	1	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
3	0	2	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
4	0	3	FF	FF	FF	FF	FF	FF	FF	07	80	69	FF	FF	FF	FF	FF	FF

Trick5: 无线电锁具安全

Trick5：无线电锁具安全

无线遥控模块：

- 常见于门禁、停车场栏杆等
- 也可用于偷电瓶
- 一般使用315Mhz、443Mhz频段
- 如使用固定码，则可被重放攻击
- 部分滚动码的生成算法已被分析，可能造成滚动码失效
- 在不知道密码的情况下可进行爆破



Trick5：无线电锁具安全——无线信号的重放

高级、全面，当昂贵的方法：

使用HackRF重放：

- 可支持几乎所有频段
- 可抓取频谱图进行分析

廉价但有效的方法：

使用可拷贝的遥控器重放

- 只支持315/443MHz
- 只支持固定码
- 可能因为噪音等原因失效

Trick5：无线电锁具安全——无线信号的重放

About Me

杨文韬 / PushEAX

研究方向为硬件安全/近源渗透

目前致力于近源渗透的理论研究和工具开发。