浅谈RFID安全

By G7@91Ri_Team

基本概念

射频识别（英文：Radio Frequency IDentification，缩写：RFID）是一种无线通信技术，可以通过无线电讯号识别特定目标并读写相关数据，而无需识别系统与特定目标之间建立机械或者光学接触。

RFID的应用

RFID在生活中的应用非常广泛，各种门禁卡、公交卡、停车卡、银行卡、乃至身份证，都是RFID技术在现实世界的具体应用。

RFID卡的分类

简单地可以把RFID卡分为低频卡（ID卡）和高频卡（IC卡）两类。低频卡工作于125KHz到135KHz，高频卡工作于13.56MHz频率。我们通常说的NFC是RFID的一个子集，属于高频卡的标准。

如何简单的区分ID卡和IC卡？Tips：观察卡面、手机手电筒功能

ID卡

- 以下是ID卡常见的两种形态，ID卡卡面上通常标有一串数字，这串数字就是ID卡存储的数据。如果用灯光透射ID卡，能看到厚厚的铜线圈匝，这是ID卡的一个显著特征。
- 因为ID的数据是明文存储的，所以ID卡其实毫无安全性可言，只需用合适的读卡器将数据读出再写入ID白卡（可读可写），即可成功克隆出一张合法ID卡。
- 现在很多小区的门禁卡，就是左边这种蓝色的ID卡~卡片型的ID卡在食堂也很常见~

IC卡

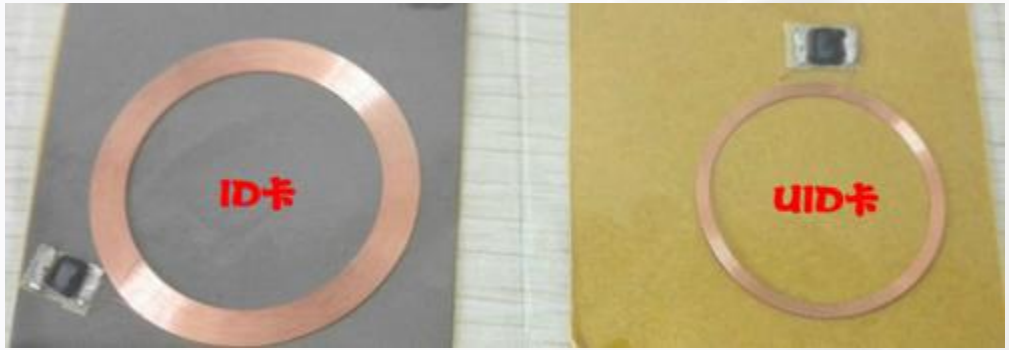
射频IC的种类繁多，卡面一般无标识。简单的判断方法：在灯光透射下可以看到一圈较细的线圈（一般是方形的）。IC卡存储数据，不仅仅是UID。

常见：Mifare卡、种类

破解方法

以常见的S50卡为例，探讨常见的攻击破解方法（0扇区、KeyA&&KeyB、UID白卡）

- 默认密钥攻击
- 认证嵌套漏洞
- DarkSide攻击
- 密钥流窃听



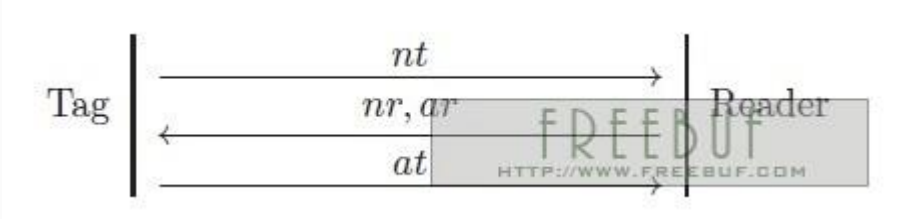
默认密钥攻击

很多IC卡都没有更改默认的key，导致可以直接用默认key进行读取数据

```
Try to authenticate to all sectors with default keys...
Symbols: '.' no key found, '/' A key found, '\' B key found, 'x' both keys found
[Key: ffffffffffff] -> [xxxxx....////xxx]
[Key: a0a1a2a3a4a5] -> [xxxxx....////xxx]
[Key: d3f7d3f7d3f7] -> [xxxxx....////xxx]
[Key: 000000000000] -> [xxxxx....////xxx]
[Key: b0b1b2b3b4b5] -> [xxxxx....////xxx]
[Key: 4d3a99c351dd] -> [xxxxx....////xxx]
[Key: 1a982c7e459a] -> [xxxxx....////xxx]
[Key: aabbccddeeff] -> [xxxxx....////xxx]
[Key: 714c5c886e97] -> [xxxxx....////xxx]
[Key: 587ee5f9350f] -> [xxxxx....////xxx]
[Key: a0478cc39091] -> [xxxxx....////xxx]
[Key: 533cb6c723f6] -> [xxxxx....////xxx]
[Key: 8fd0a4f256e9] -> [xxxxx....////xxx]
```

认证嵌套漏洞

IC卡读写卡原理：三轮确认



DarkSide攻击

基于IC卡类别当中NXP公司所发布的MIFARE算法漏洞

当读卡器发送的加密数据中的某8bit全部正确的时候卡会给读卡器发送一个加密的4bit的NACK回复，其他任何情况下卡都会直接停止交互。（PRNG漏洞）

结合认证嵌套漏洞

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（PRNG漏洞）


Thanks
Q&A