NFC 门禁卡复制

作者：RolabHJ
原文链接：https://ld246.com/article/1572014815658
来源网站：链滴

<h2 id="0-前言">0.前言</h2>
由于租的小区房，只有一张门禁卡，女票每次过来进出小区很不方便，于是萌生了复制门禁卡的法，国庆期间实践成功
<h2 id="1-硬件准备">1.硬件准备</h2>

NFC 读写器：我选用的是 PN532，就一个 IC 控制的 PCB 板，它通过串口与 PC 连接
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https://b3ogfile.com/file/2019/10/image-5e63b125.png?imageView2/2/interlace/1/format/jpg">

UID 白卡：同 PN532 一样，某宝搜索 UID 卡即可搜索到
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https://b3ogfile.com/file/2019/10/image-d2d83dd8.png?imageView2/2/interlace/1/format/jpg">

<h2 id="2-软件准备">2.软件准备</h2>
所有有关 nfc 的软件（Ubuntu/Win 等）都是从 GitHub 上拉取的 libnfc 编译生成的，如果你时间很多，可以去 github 上拉取源码编译，然后通过令行进行 NFC 的读写（需要熟悉 libnfc 的命令行），如果没时间就使用别人编译好的上位机（一些神们总是为小白制作了各式各样的方便好用的 tool），例如我使用的是
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https: /b3logfile.com/file/2019/10/image-811ab47a.png?imageView2/2/interlace/1/format/jpg"></ >
<h2 id="3-知识储备">3.知识储备</h2>
NFC 卡复制需要了解 NFC 卡的数据结构
<img src="https://ld246.com/images/img-loading.svg" alt="20190124142629109.jpg" da a-src="https://b3logfile.com/file/2019/10/20190124142629109-83161643.jpg?imageView2/2/ nterlace/1/format/jpg">
通常 NFC 卡，一共有 16 个扇区，每个扇区 4 个块，每个块 16 个字节，因此一张 NFC 卡的容为 <code>16*4*16=1024</code> 字节，通常每个扇区的第 4 块，用于存放密码 A 和密码 B，即中的 KEY A 和 KEY B，密码 A 和密码 B 需要通过上位机进行破解，通常情况下，暴力破解都可破解但是一般的卡其密码都是默认密码，我住的小区亦是如此，因此很容易就破解了
<h2 id="4-操作">4.操作</h2>
点击上位机的密钥破解即可自动破解，一旦破解便会保存一个 <code>.mfd</code> 文件，直利用上位机将该文件写入空白 uid 卡即可，这里需要注意的是：
<blockquote>
当向空白 uid 卡写入 <code>.mdf</code> 文件时，一共 64 个块，只会写进去 63 个块，还一个块不会写入，这个块就是保存有 uid（世界唯一 ID）数据和厂商数据的数据块，它位于 0 扇区的 0 块，因此还需要手动写入 uid 数据（厂商数据貌似写不了，但我实测即使厂商数据不一致，门禁依是可用的，说明一般情况下门禁不会对比厂商数据，它对比的是 uid 以及 1~63 扇区的数据）
</blockquote>
<h2 id="5-参考">5.参考</h2>
NFC 的复制还可以结合到拥有 NFC 的手机上，更加便捷

Ubuntu NFC 环境
52 破解
