



# 一起来试验 保险箱的脆弱面

by: 姚威 (黑客叔叔p0tt1)

# About Me

姚威

ID：黑客叔叔p0tt1

凌晨网络科技有限公司

RainRaid Crew 信息安全团队

3.A.M Lab 凌晨三点网络攻防实验室

一个精神分裂非典型双子座的信息安全从业者&创业者



凌晨网络科技

# content

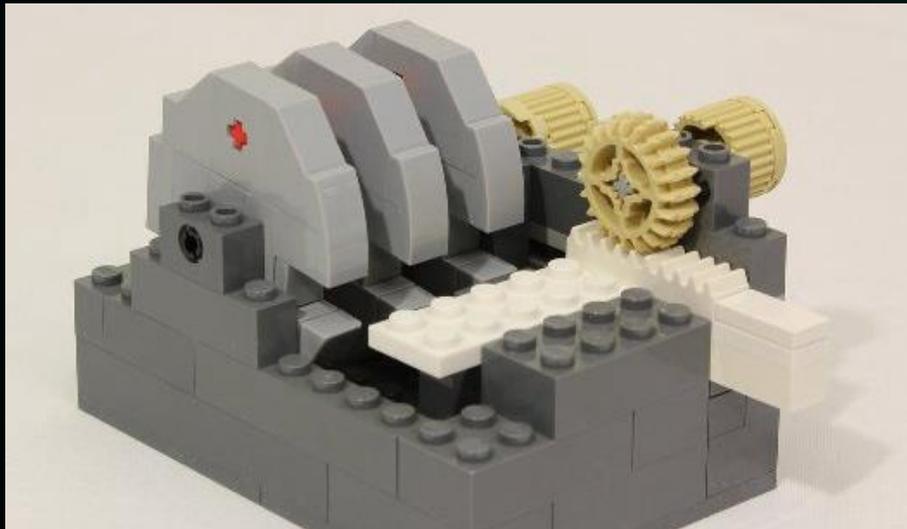
- Part 01 / 保险箱的分类
- Part 01 / 那些脆弱的攻击面
- Part 01 / 一些小实验
- Part 01 / 问题与探讨

01

保险箱的分类



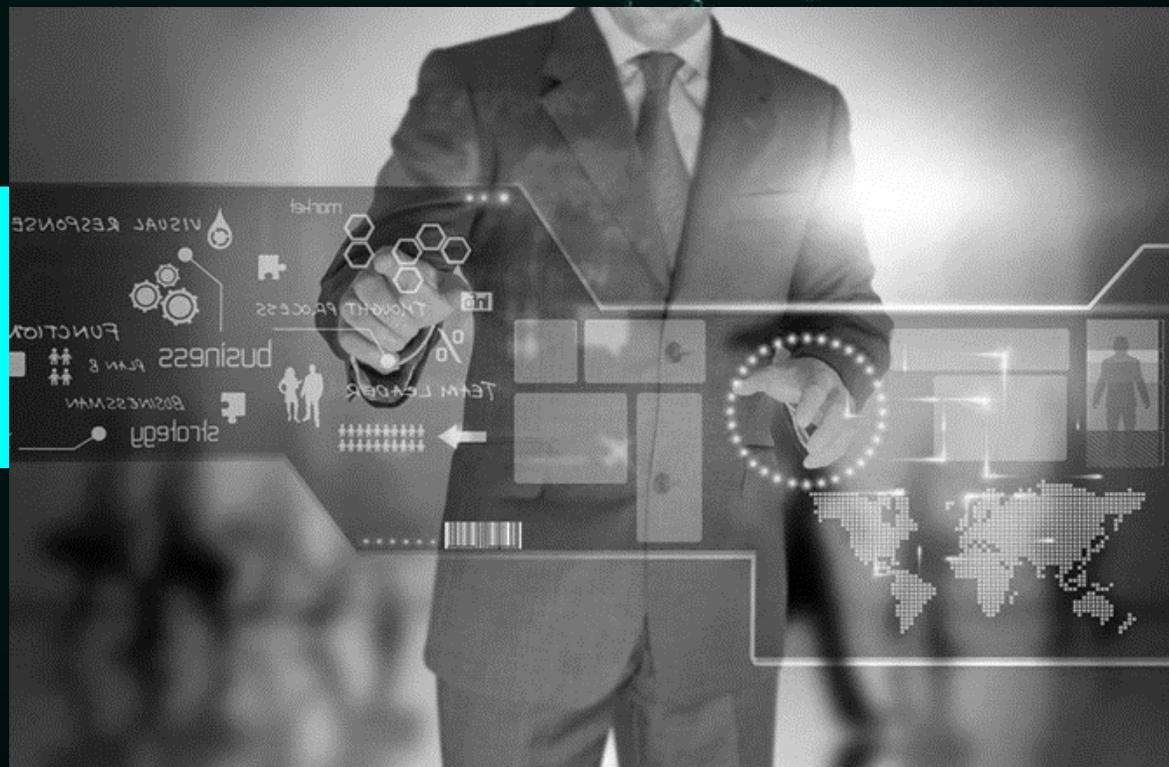
● 轮盘锁与电子锁



## ● 智能保险箱

# 万物互联你敢没有啊啾啾？

诚实的说，现在想做个硬件不智能你好意思？  
讲真，现在智能设备没有APP你好意思？  
所以，APP没有wifi和蓝牙等接口你好意思？  
然，为什么不重要，炫酷才是王道！



# ● 就那么随便的选择了两个智能保险箱



# 搭载互联网云技术

让智能锁系统与智能设备实时连接



# 你需要的一种无忧生活

一种跨越距离的安全体验

## MINGDE SAFE

一种说走就走的生活



不再被累赘的  
金属钥匙困扰



没有繁琐，没有忧虑

不再因为钥匙丢失  
干着急

1:49

3月3日 星期四

保险箱管家 现在  
2016-03-03 13:49:04: 我的保险箱,手动开  
锁  
滑动来查看

无论身在哪里  
安全一手掌握

不要保险箱被盗了  
我在外面却一无所知



# 利用电子面板 进行技术破解?

**NO!**

我无电子面板  
您无处下手!

SAFEOK



# 利用网络黑客暴力破解？



APP

+



蓝牙

+



NFC芯片

=

**NO!** 没有可能



3次错码报警

+



50次错码锁住

+



点对点注册





02

那些脆弱的攻击面

**\*123456#**

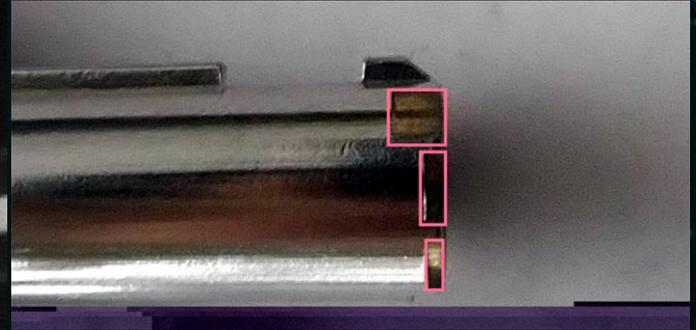
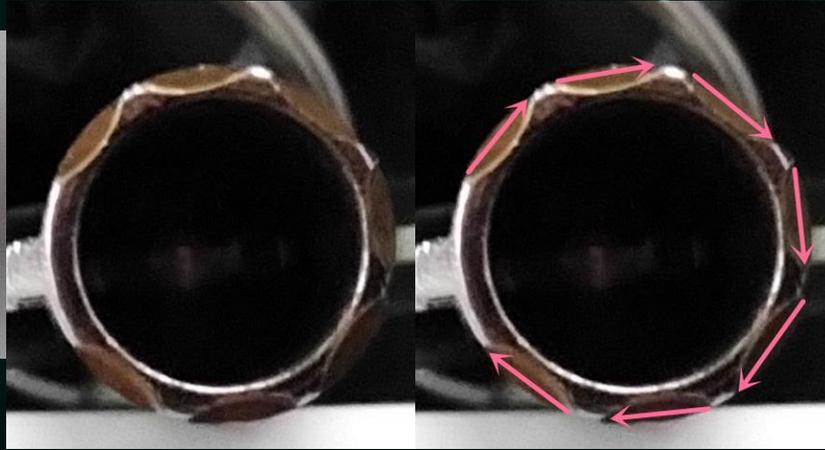
**\*888888#**

**\*000000#**

**\*666666#**

**然后按功能键进入MENU**

**超管 ? GOD ? 后门 ?**



● 智能保险箱的攻击面是窄了还是宽了呢？



**交互的问题**  
操作的逻辑，交互的判断



**接口的问题**  
各种蓝牙,wifi,nfc，指纹都安全吗？



**数据的问题**  
从机械到智能，数据懂得人少？



**云端的问题**  
云端安全吗？传输安全吗？

- 细化下攻击面和攻击方案

# SUCCESS



## WiFi

WiFi密码是可以破解的，还有弱密码，还有万能钥匙，所以wifi密码不能当做其他硬件的加密，再说，还可以劫持和ARP

## 蓝牙

蓝牙这玩意，和NFC一样，虽然都是近距离，但是功率这东西可以上功放，最重要的是，蓝牙是可以监听的，你不做加密，就别怪听风耳

## 云端&APP

云端通信的过程的单双向，APP的逆向分析，通信的算法和APP的代码实现可以变得交互高效，也会搞笑



03

一些小实验

The background features a dark teal gradient with glowing blue circuit traces and numerous small, bright blue particles scattered throughout, creating a high-tech, digital atmosphere.

视频播放时间



04

问题与探讨

## ● 问题与探讨

### 为什么要智能

究竟是为了便捷加模块  
还是为了噱头加模块

### 什么叫智能

是使用更智能了  
还是模块更智能了



### 智能与安全的平衡怎么找

安全不是去掉所有智能设计  
智能设计当然也不能没有安全

### 解决方案

既然智能设备就是堆接口和模块，我们认了，但是针对接口和模块的安全解决方案这个锅什么时候有人来背？

- 最后举个小栗子



## 硬编码和协议

我们在这次破解的过程中发现了一个问题，就是我们所组合的几个漏洞与设计缺陷，在写修补方案的时候，发现远程完全没办法修补，但是奇怪的是，漏洞提交后，版本更新了，却依然没有办法解决根本的问题，虽说大家都联网了，然而智能设备在解决安全问题的时候却没有像智能手机或APP那样智能了。

The background features a dark blue gradient with glowing cyan circuit traces and numerous small, bright cyan particles scattered throughout, creating a futuristic, digital atmosphere.

谢谢

THANKS