边信道攻击实战

Kevin2600

. Kevin2600

. 专注无线电; 嵌入式设备安全研究

. NewSky 安全研究员 + 安全培训讲师

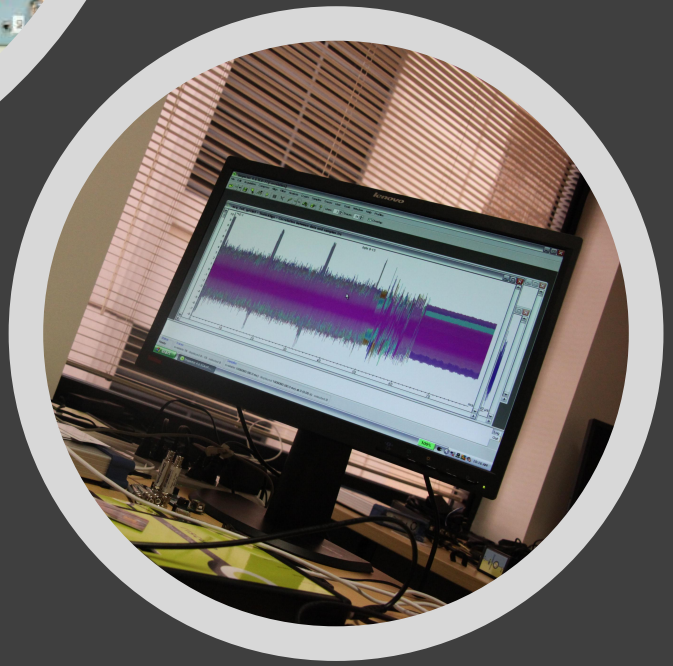
. 坚信黑客精神就是不断探索未知领域

青天科技 NewSky Security

Joinsec

边信道的传说?

$$
\begin{aligned}
r_{i,j} &= \frac{\sum_{d=1}^{D}\left[\left(h_{d,i}-\overline{h_i}\right)\left(t_{d,j}-\overline{t_j}\right)\right]}{\sqrt{\sum_{d=1}^{D}\left(h_{d,i}-\overline{h_i}\right)^2\sum_{d=1}^{D}\left(t_{d,j}-\overline{t_j}\right)^2}} \\
&= \frac{\sum_{d=1}^{D}\left[h_{d,i}t_{d,j}-t_{d,j}\overline{h_i}-h_{d,i}\overline{t_j}+\overline{t_j}\overline{h_i}\right]}{\sqrt{\sum_{d=1}^{D}\left({h_{d,i}}^2-2\overline{h_i}h_{d,i}+\overline{h_i}^2\right)\sum_{d=1}^{D}\left({t_{d,j}}^2-2\overline{t_j}t_{d,j}+\overline{t_j}^2\right)}} \\
&= \frac{\sum_{d=1}^{D}h_{d,i}t_{d,j}-\overline{h_i}\sum_{d=1}^{D}t_{d,j}-\overline{t_j}\sum_{d=1}^{D}h_{d,i}+D\overline{t_j}\overline{h_i}}{\sqrt{\left(\sum_{d=1}^{D}{h_{d,i}}^2-2\overline{h_i}\sum_{d=1}^{D}h_{d,i}+D\overline{h_i}^2\right)\left(\sum_{d=1}^{D}{t_{d,j}}^2-2\overline{t_j}\sum_{d=1}^{D}t_{d,j}+D\overline{t_j}^2\right)}} \\
&= \frac{\sum_{d=1}^{D}h_{d,i}t_{d,j}-\overline{h_i}\sum_{d=1}^{D}t_{d,j}-\frac{\sum_{d=1}^{D}t_{d,j}}{D}\sum_{d=1}^{D}h_{d,i}+D\frac{\sum_{d=1}^{D}t_{d,j}}{D}\frac{\sum_{d=1}^{D}h_{d,i}}{D}}{\sqrt{\left(\sum_{d=1}^{D}{h_{d,i}}^2-2\overline{h_i}\sum_{d=1}^{D}h_{d,i}+D\overline{h_ih_i}\right)\left(\sum_{d=1}^{D}{t_{d,j}}^2-2\overline{t_j}\sum_{d=1}^{D}t_{d,j}+D\overline{t_jt_j}\right)}} \\
&= \frac{\sum_{d=1}^{D}h_{d,i}t_{d,j}-\overline{h_i}\sum_{d=1}^{D}t_{d,j}}{\sqrt{\left(\sum_{d=1}^{D}{h_{d,i}}^2-2\overline{h_i}\sum_{d=1}^{D}h_{d,i}+D\overline{h_i}\frac{\sum_{d=1}^{D}h_{d,i}}{D}\right)\left(\sum_{d=1}^{D}{t_{d,j}}^2-2\overline{t_j}\sum_{d=1}^{D}t_{d,j}+D\overline{t_j}\frac{\sum_{d=1}^{D}t_{d,j}}{D}\right)}} \\
&= \frac{\sum_{d=1}^{D}h_{d,i}t_{d,j}-\overline{h_i}\sum_{d=1}^{D}t_{d,j}}{\sqrt{\left(\sum_{d=1}^{D}{h_{d,i}}^2-\overline{h_i}\sum_{d=1}^{D}h_{d,i}\right)\left(\sum_{d=1}^{D}{t_{d,j}}^2-\overline{t_j}\sum_{d=1}^{D}t_{d,j}\right)}} \\
&= \frac{\sum_{d=1}^{D}h_{d,i}t_{d,j}-\frac{\sum_{d=1}^{D}h_{d,i}}{D}\sum_{d=1}^{D}h_{d,i}}{\sqrt{\left(\sum_{d=1}^{D}{h_{d,i}}^2-\frac{\sum_{d=1}^{D}h_{d,i}}{D}\sum_{d=1}^{D}h_{d,i}\right)\left(\sum_{d=1}^{D}{t_{d,j}}^2-\frac{\sum_{d=1}^{D}t_{d,j}}{D}\sum_{d=1}^{D}t_{d,j}\right)}} \\
&= \frac{D\sum_{d=1}^{D}h_{d,i}t_{d,j}-\sum_{d=1}^{D}h_{d,i}\sum_{d=1}^{D}t_{d,j}}{D\sqrt{\frac{\left(\left(\sum_{d=1}^{D}h_{d,i}\right)^2-D\sum_{d=1}^{D}h_{d,i}^2\right)\left(\left(\sum_{d=1}^{D}t_{d,j}\right)^2-D\sum_{d=1}^{D}t_{d,j}^2\right)}{D^2}}} \\
&= \frac{D\sum_{d=1}^{D}h_{d,i}t_{d,j}-\sum_{d=1}^{D}h_{d,i}\sum_{d=1}^{D}t_{d,j}}{\sqrt{\left(\left(\sum_{d=1}^{D}h_{d,i}\right)^2-D\sum_{d=1}^{D}h_{d,i}^2\right)\left(\left(\sum_{d=1}^{D}t_{d,j}\right)^2-D\sum_{d=1}^{D}t_{d,j}^2\right)}}
\end{aligned}
$$



边信道的传说?

. Side-Channel 必须掌握很深的数学知识?

. Side-Channel 必须使用昂贵的硬件设备?

. Side-Channel 都有哪些实战中的运用?

. Side-Channel 作为小白该如何开始?

Contents:

边信道的那点事

故事起源:

二战期间盟军的一名研究人员发现他的示波器经常有莫名的噪音. 调查发现信号来源于隔壁房间的某台加密机. 在深入研究后, 这名研究员成功地将被加密前的明文信息从噪音中提取出来.

WHAT ?

边信道攻击是一种针对软件或硬件设计缺陷, 剑走偏锋的攻击方式

攻击途径通常采用被动式监听, 或通过特殊渠道发送隐蔽数据信号

攻击点不在暴力破解或算法分析, 而是通过功耗; 时序; 电磁泄漏等方式达到破解目的. 在很多物理隔绝的环境中, 往往也能出奇制胜

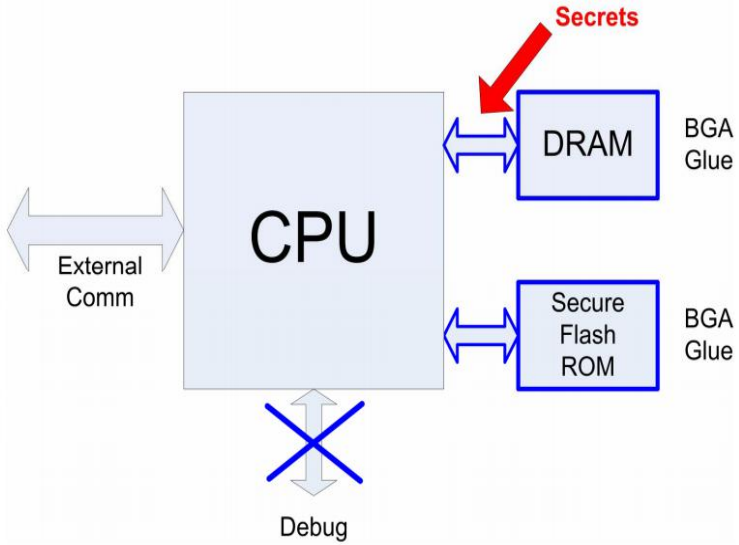
WHY ?

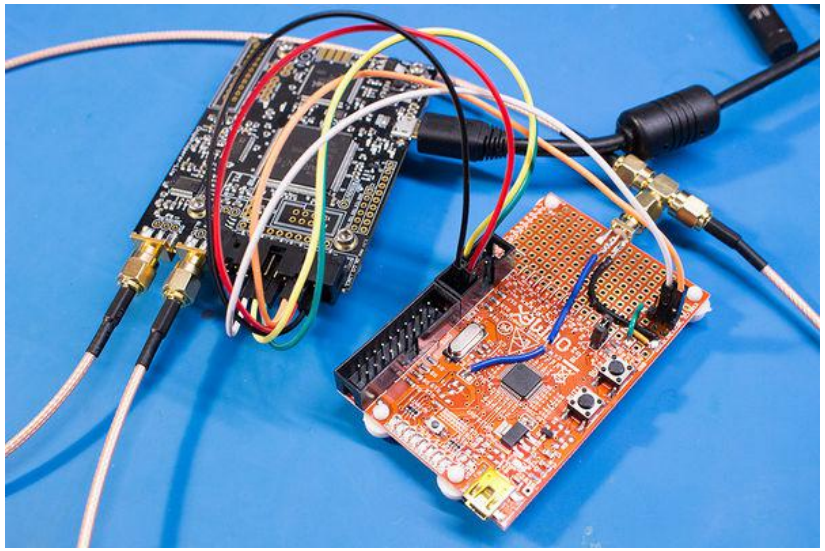
. Public key signature check

. Bootloader 加固 (bootdelay = 0)

. 屏蔽调试端口 UART; JTAG; SPI; I2C

. 电子设备全部物理隔离 (Air Gapping)





HOW ?

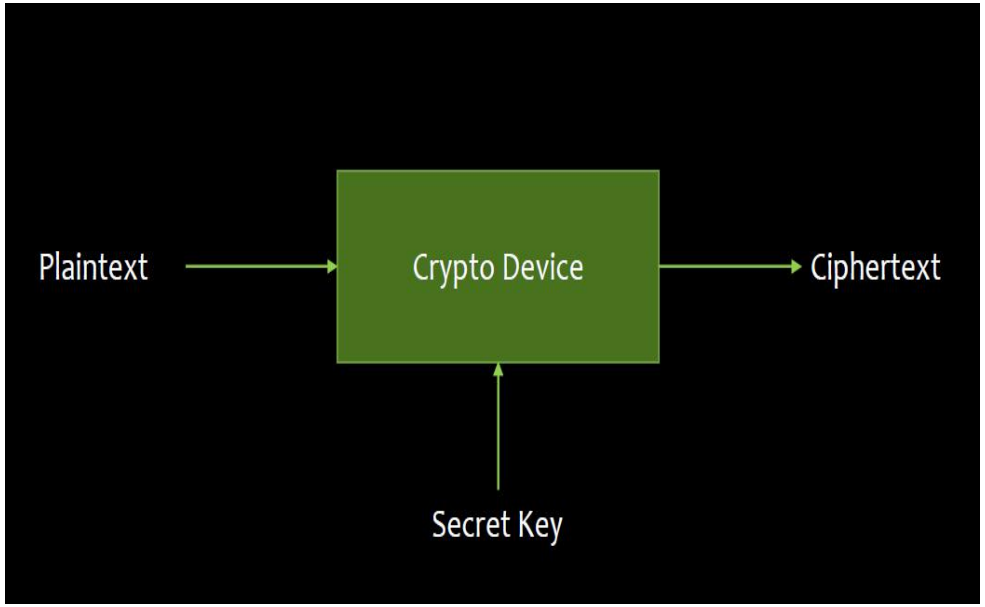
. 简单功耗分析 (Simple power analysis)

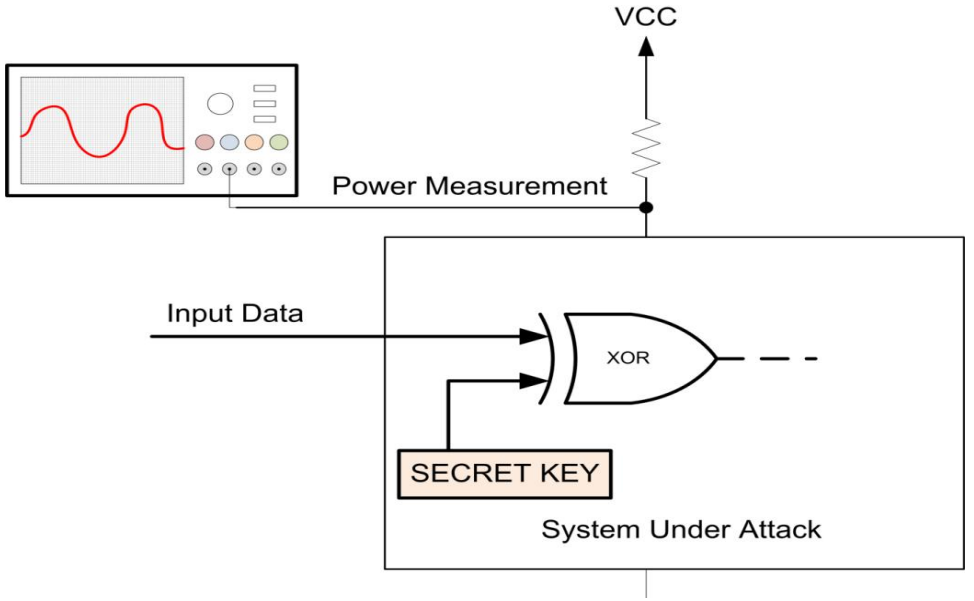
. 差分功耗分析 (Differential power analysis)

. 需要通过明文或密文触发加密机制运行

. 需要知道用何种加密方式 (AES128; RSA; 3DES)

. 功耗数据提取必须在目标加解密的过程中





被动式:

: 声波信号采集还原打印机原文

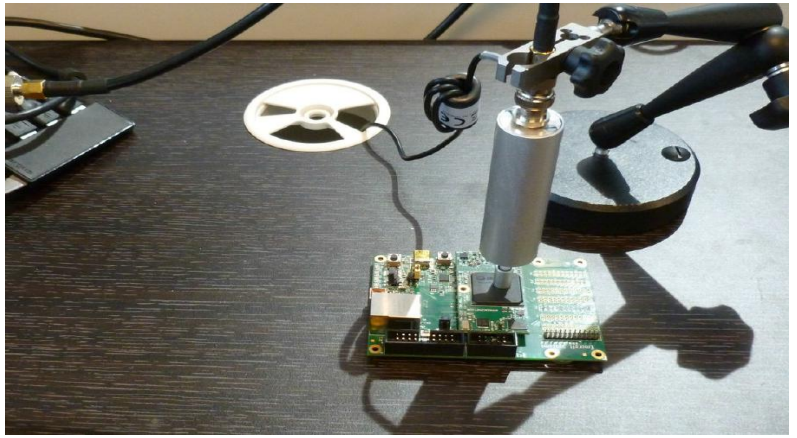
: 美国 NSA 电磁波监听 (TEMPEST)

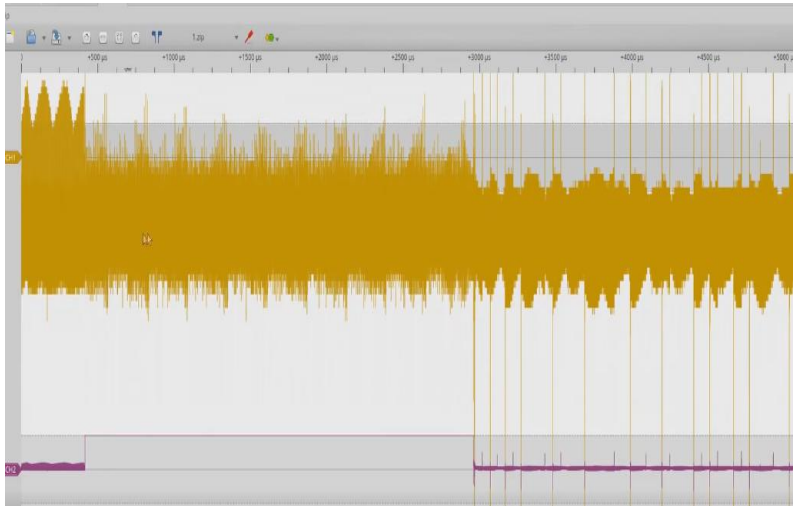
: 功耗分析破解南韩公交卡密钥系统 (3DES)

: 功耗分析获取 Philipe Hue 智能灯系统密钥 (AES)

: 通过测量分析电磁发射获取 GnuPG 密钥信息 (RSA)

: 通过声波远程获取物理隔离网络中的数据 (Funtenna)





主动式:

: Xbox360 Glitch 攻击 (运行 unsigned code)

: 智能网关 Hue NAND Glitch (得到 Root 权限)

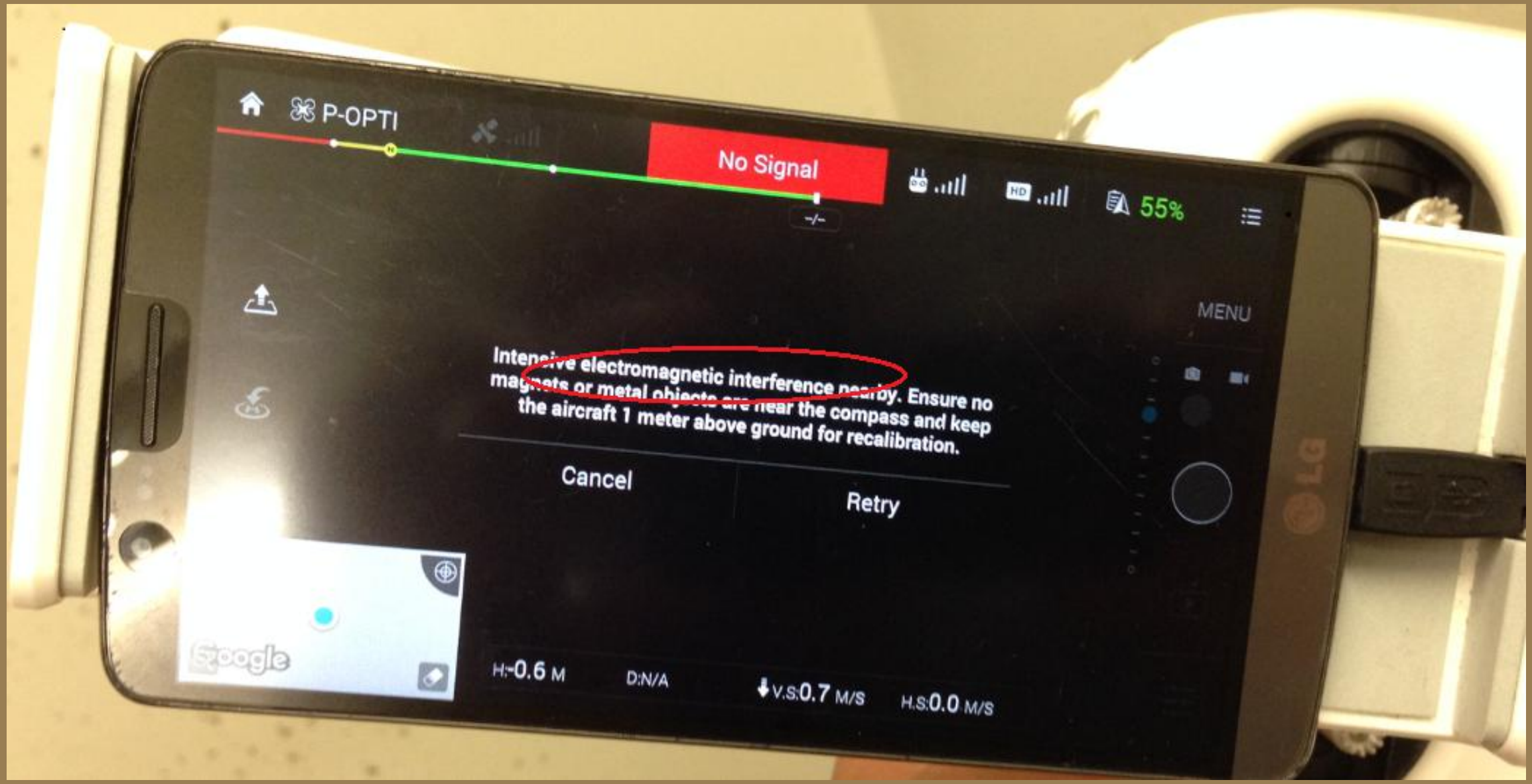
: 腾讯玄武激光发指令到二维码读取器 (Bad Barcode)

: 浙江 & Michigan 大学通过声波干扰视频监控硬盘存储

: 以色列 Ben-Gurion 大学通过 USB 发送电磁信号 (USBee)

: Osmo-fl2k 软件无线电发送 FM; GSM; UMTS 与 GPS 信号

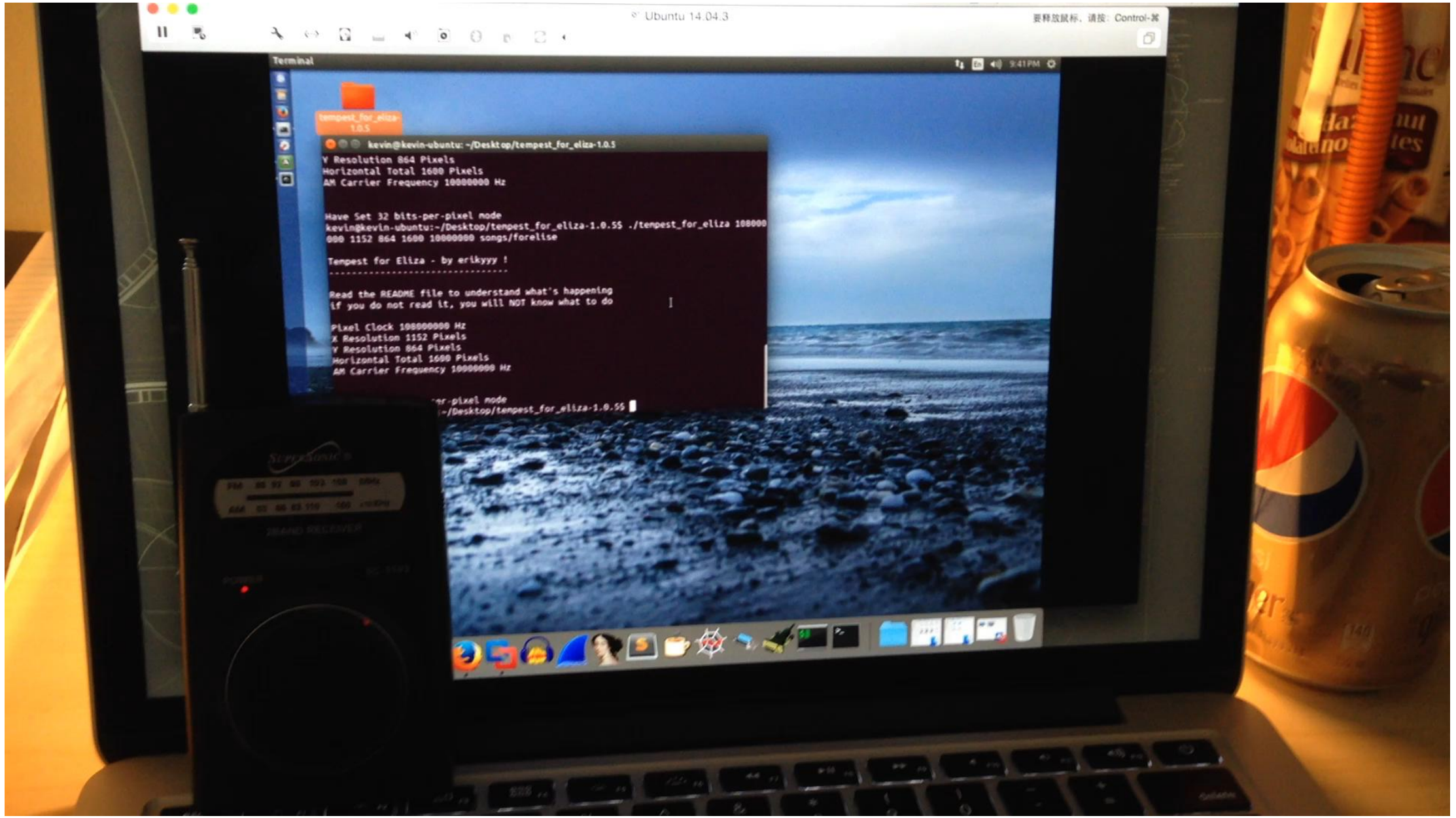
边信道案例 – EM leaking


P-OPTI
No Signal
55%
MENU
Intensive electromagnetic interference nearby. Ensure no
the compass and keep
the aircraft 1 meter above ground for recalibration.
Cancel
Retry
Google
H:0.6 M
D:N/A
V.S:0.7 M/S
H.S:0.0 M/S

电磁波 101

- 电磁波是电磁场的运动形态, 属于能量的一种
- 自身温度大于绝对零度物体, 都可以发射电磁波
- 电磁波应用广泛微波炉; 移动通信; 无线卫星通信
- 电子设备产生电磁波, 对无线电设备造成信号干扰

视频演示

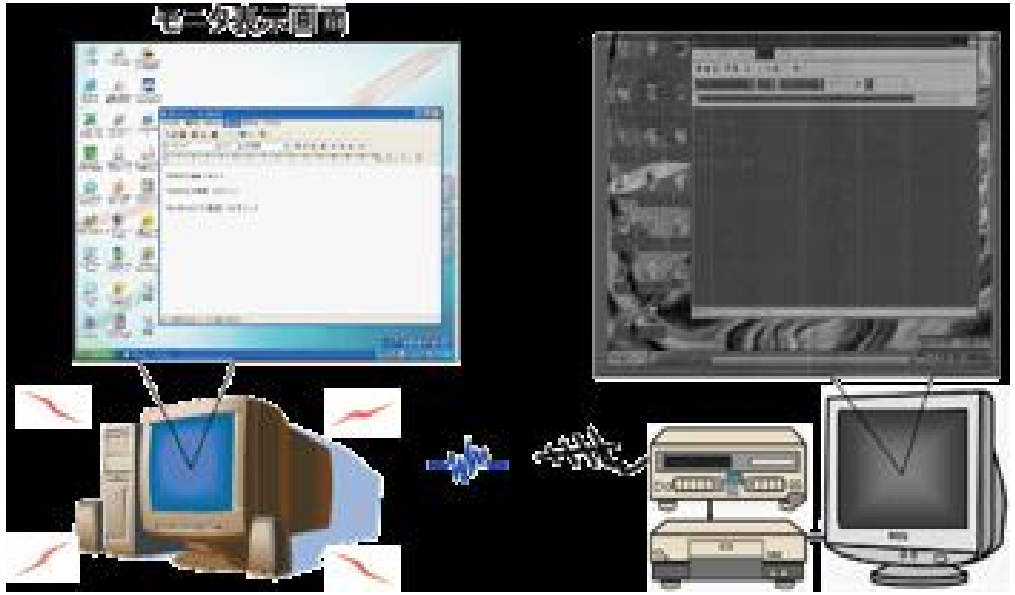

Ubuntu 14.04.3
Terminal
kevin@kevin-ubuntu: ~/Desktop/tempest_for_eliza-1.0.5
Y Resolution 864 Pixels
Horizontal Total 1600 Pixels
AM Carrier Frequency 10000000 Hz
Have Set 32 bits-per-pixel mode
kevin@kevin-ubuntu:~/Desktop/tempest_for_eliza-1.0.5$ ./tempest_for_eliza 108000
000 1152 864 1600 10000000 songs/forelise
Tempest for Eliza - by erikyyy !
Read the README file to understand what's happening
if you do not read it, you will NOT know what to do
Pixel Clock 108000000 Hz
X Resolution 1152 Pixels
Y Resolution 864 Pixels
Horizontal Total 1600 Pixels
AM Carrier Frequency 10000000 Hz

电磁泄漏隐患

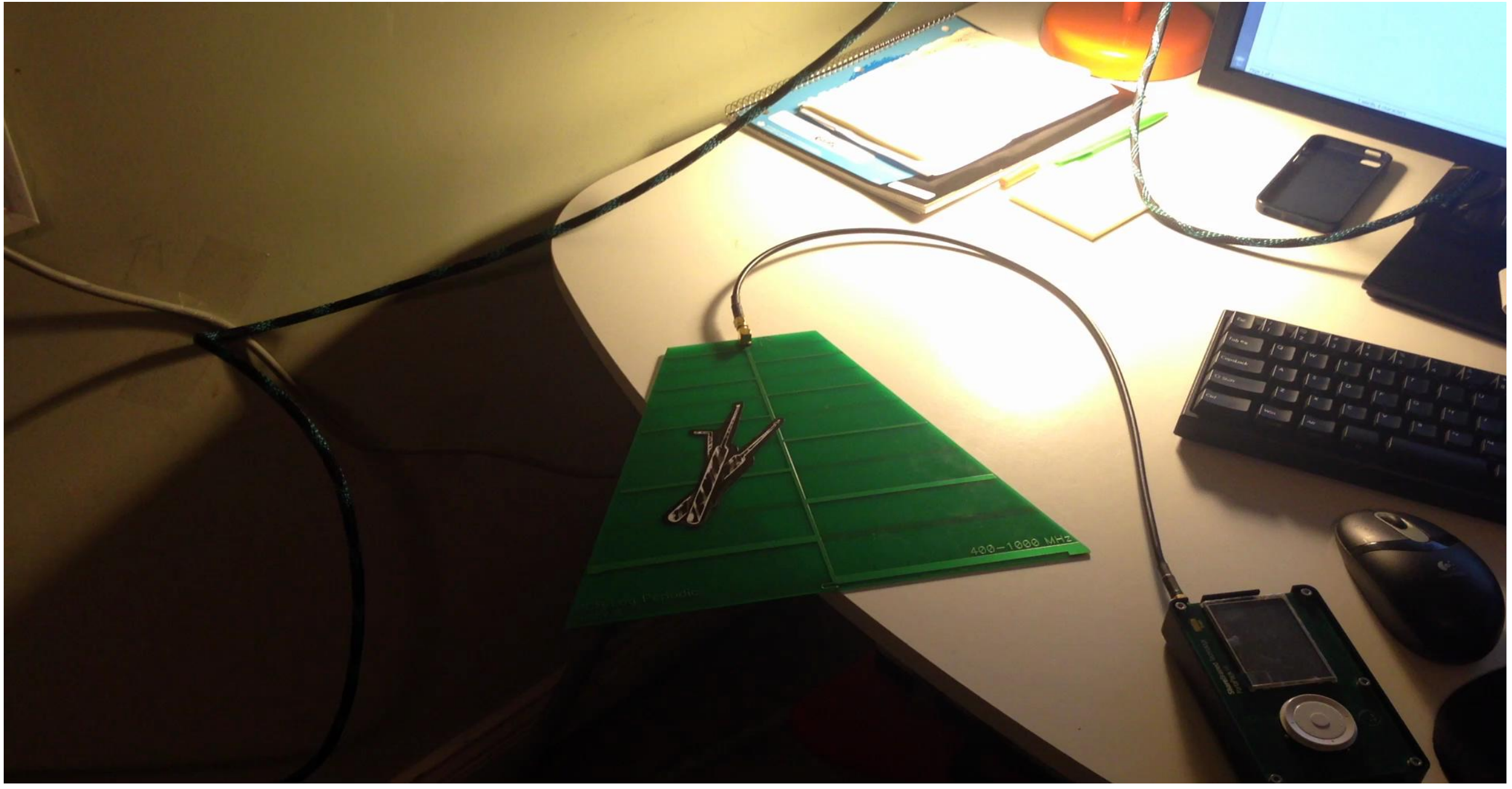
. 电子设备利用电磁波信号, 发射信息内容从而泄漏机密 (Soft-Tempest)

. 电子设备电磁信号可被解码并还原, 达到远程监控目的 (Hard-Tempest)

. 美国NSA 和北约组织制定安全标准, 要求对涉密设备进行电磁屏蔽, 并严格限制泄漏电磁辐射的强度



视频演示



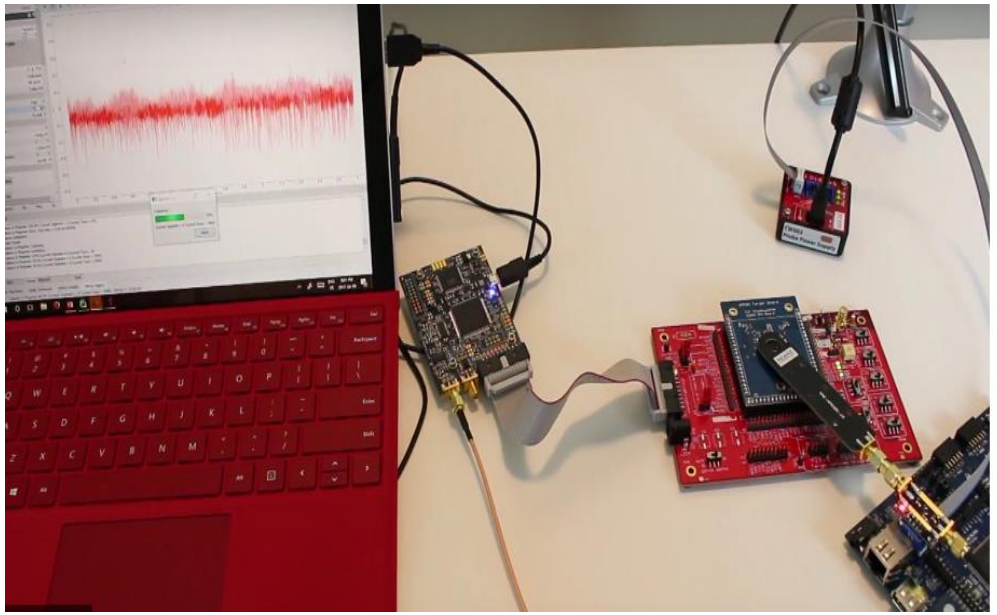
电磁信号分析

. Tel Aviv 大学科研人员通过测量分析电磁发射获取 GnuPG 密钥信息

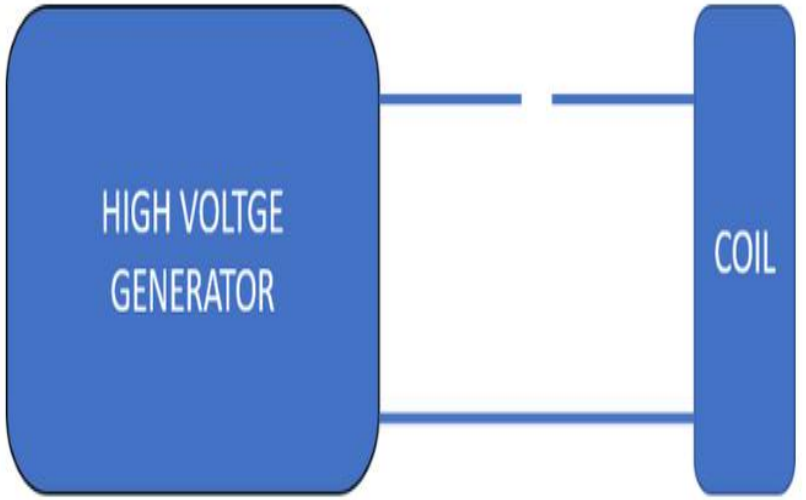
. 电磁波可通过H探头和便宜的软件无线电设备远程获取

. 芯片解密过程中执行的计算量不同, 所需电量也不同

. 芯片01转换产生电磁波从空气中泄漏, 其中包含密钥指纹信息



电磁注入



. EMP-Jammer 高能电磁场发射器 (危险!!!)

. 瞬间大量电流通过导体将产生高能电磁场

. 电磁注入将造成电子设备故障或意外惊喜 ;)

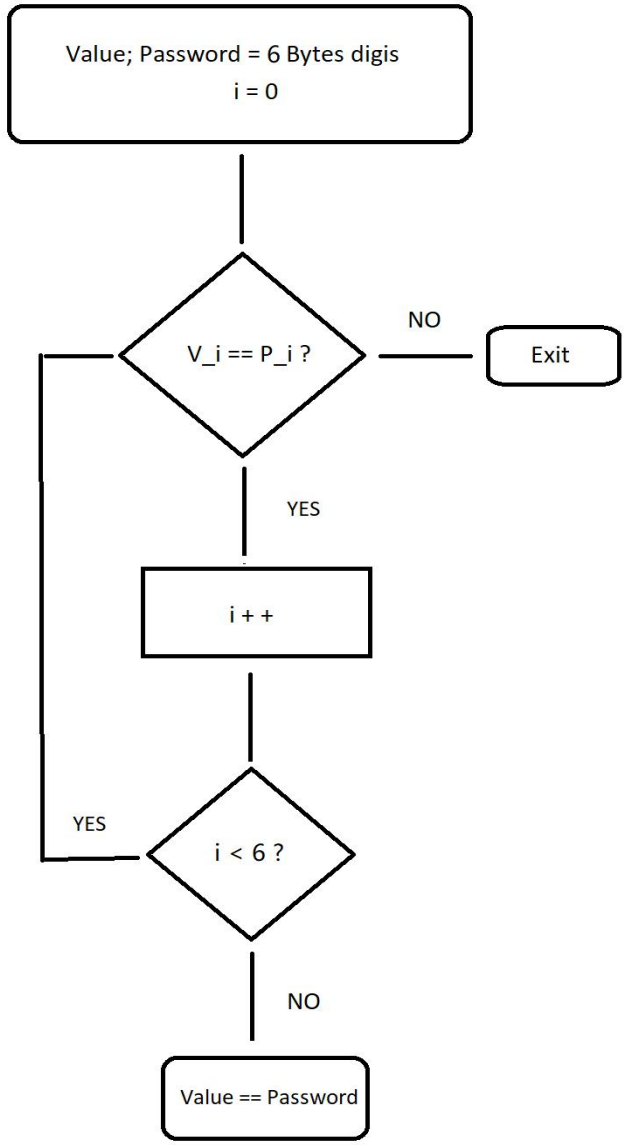
. 将设备放入塑料袋或铝箔包裹可防止电磁攻击

视频演示

边信道案例 – Timing Attack

密码比对

```
unsigned char correctpin[6] = {1,2,3,4,5,6};
unsigned char enteredpin[6];

read_pin_from_buttons(enteredpin);

for (i = 0; i < 6; i++){

      if (correctpin[i] != enteredpin[i]){
            return;

      }
}
```



时序攻击

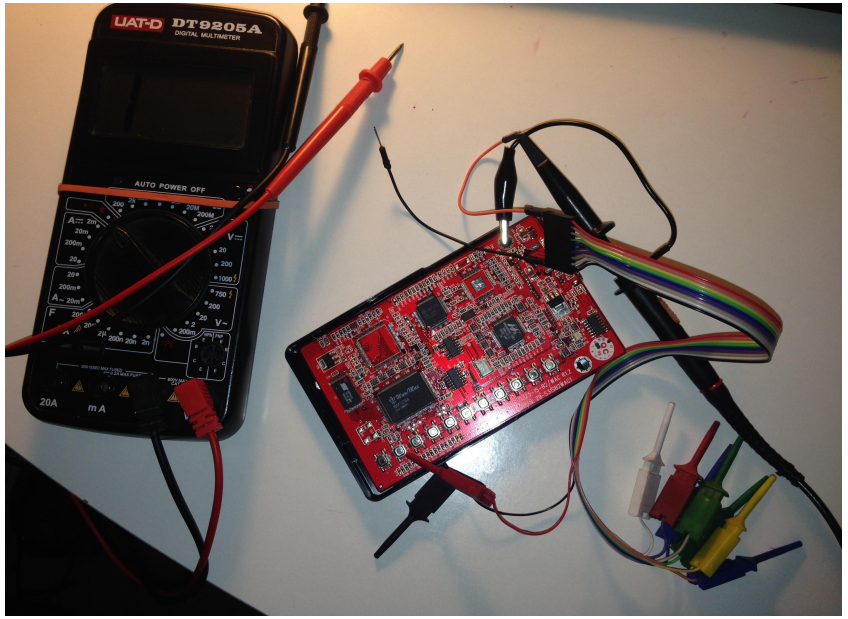
. 仅需普通示波仪即可完成攻击

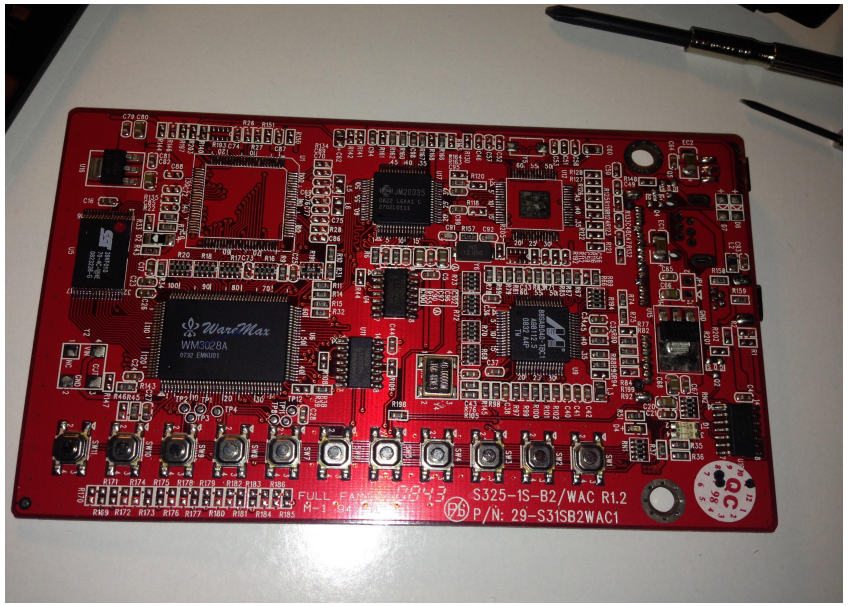
. 密码位输错给予相对反应 (LED 灯亮)

. 不安全的函数 memcmp() (单字节比对)

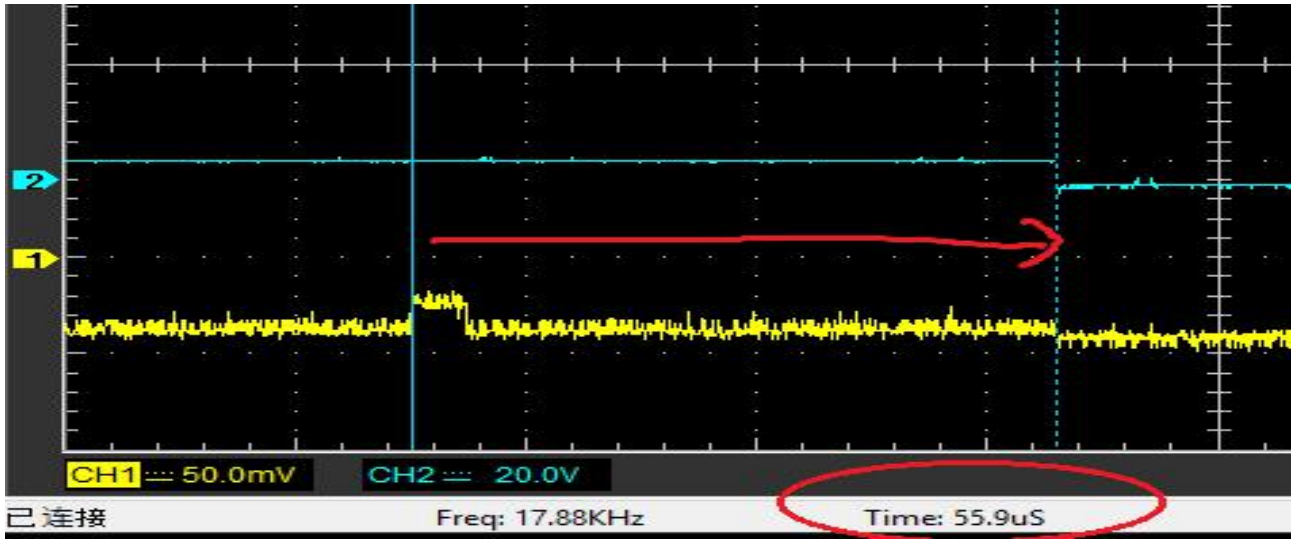
. 密码位比对的时间越久, 猜中可能性越大

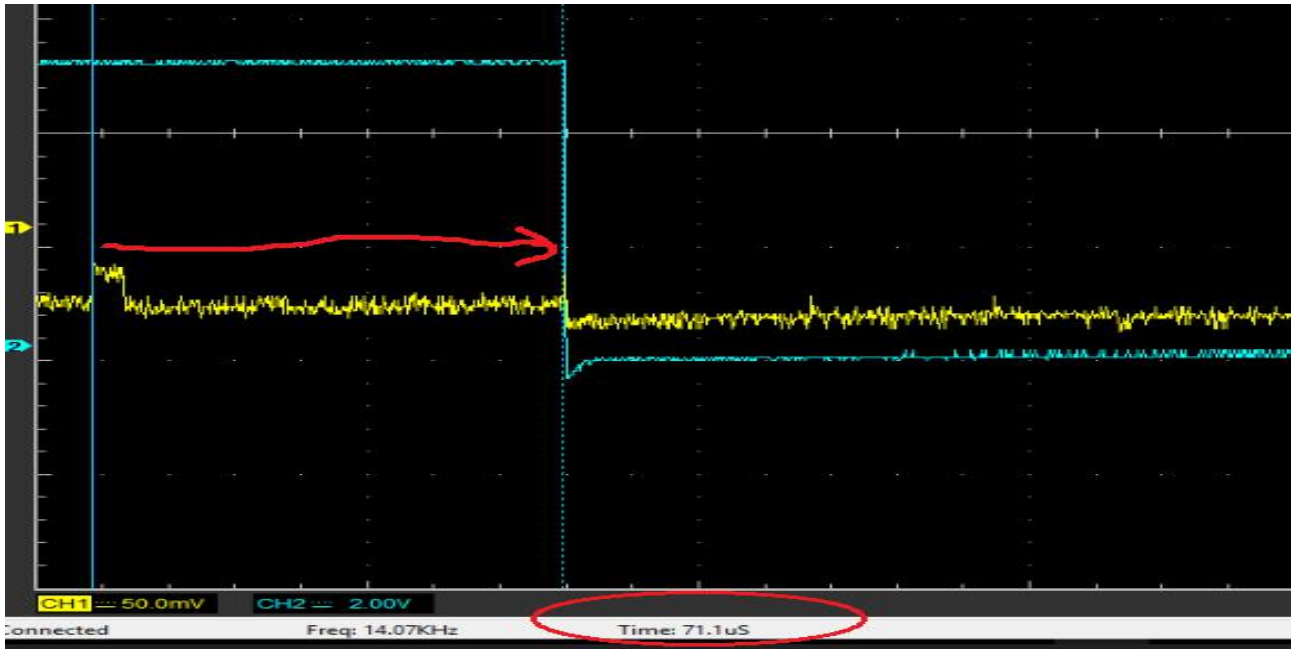
. 降低猜测空间 (6*6*6*6*6*6 = 46656) --> (6+6+6+6+6+6 = 36)

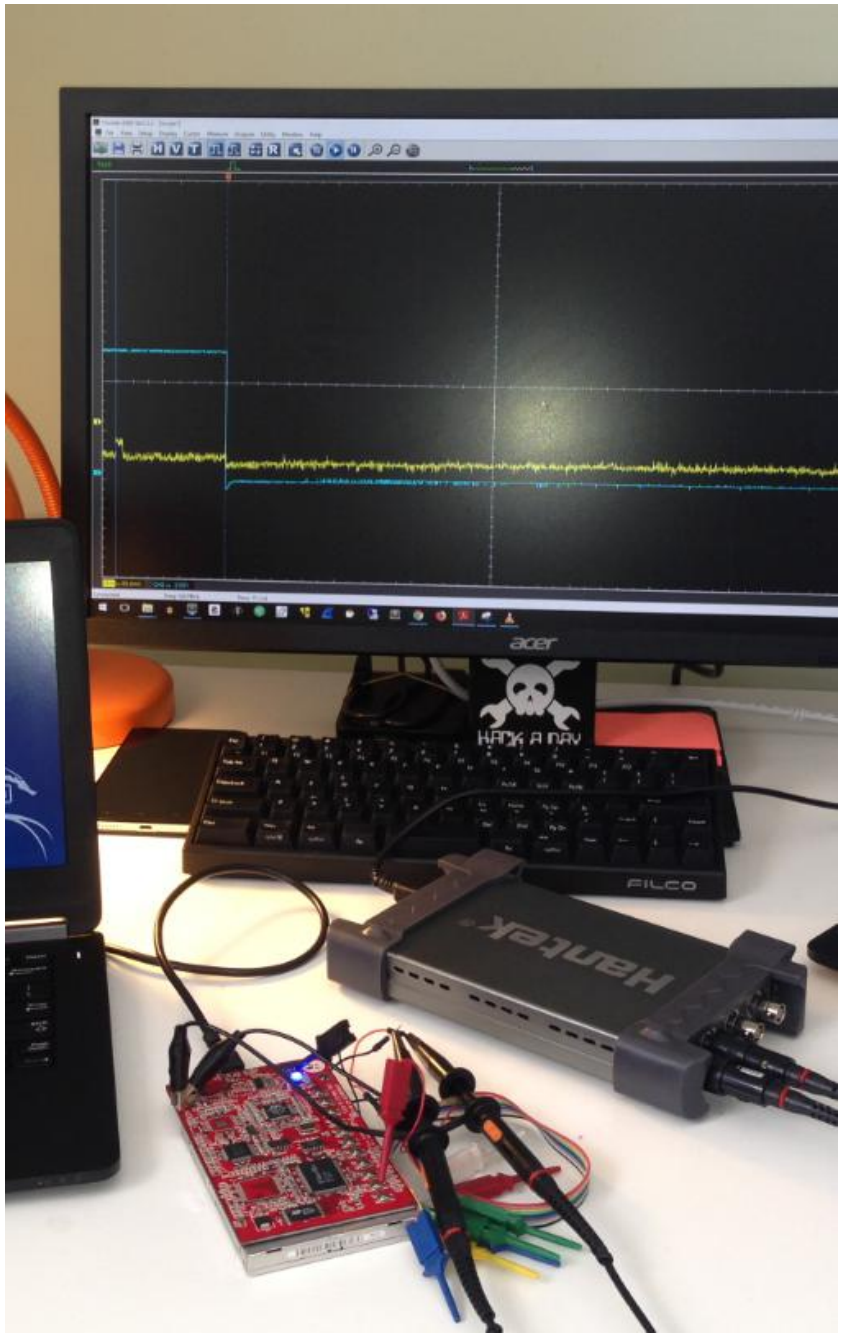




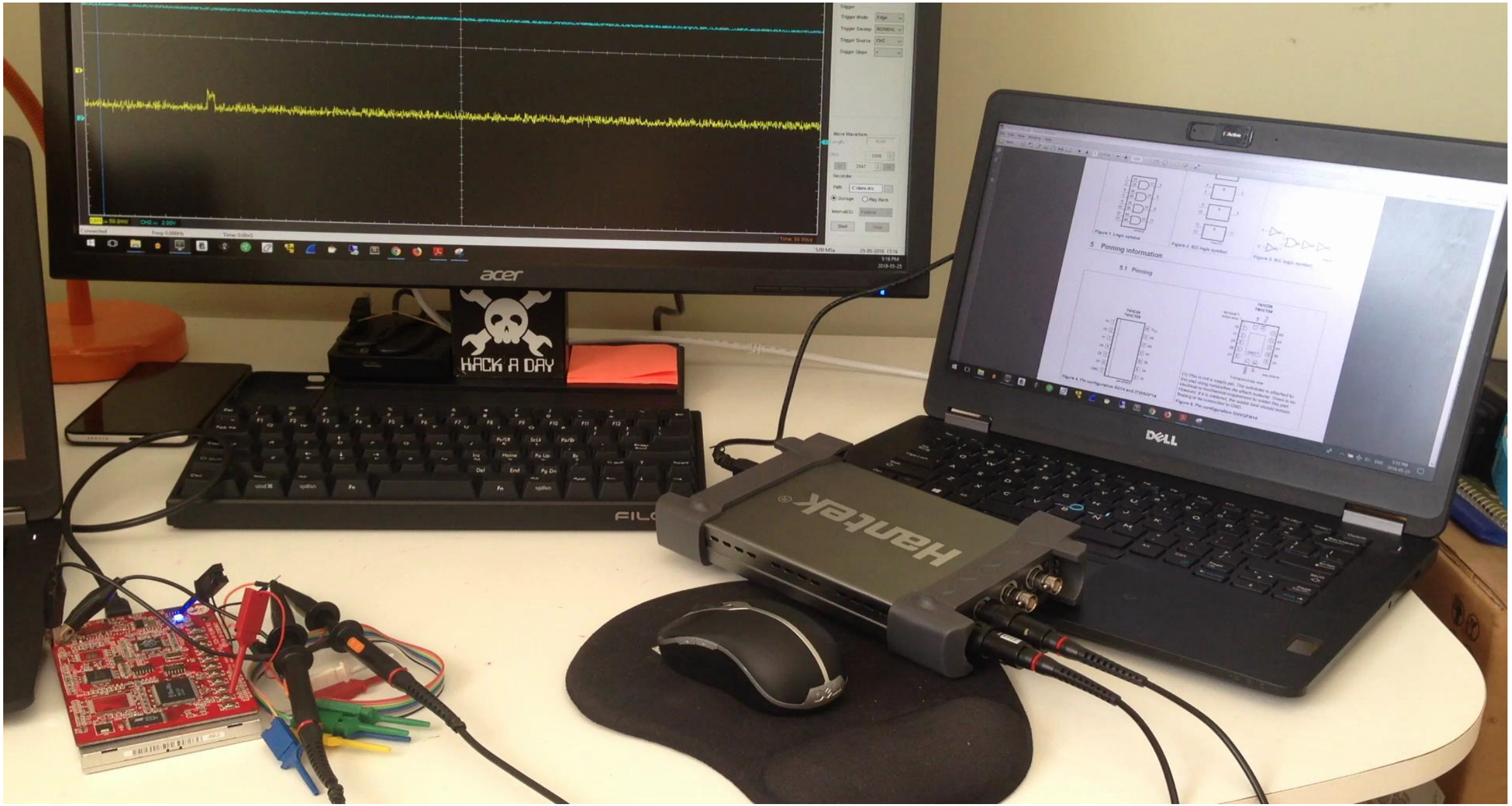
时序攻击


CH1 50.0mV
CH2 20.0V
已连接
Freq: 17.88KHz
Time: 55.9uS


CH1 50.0mV
CH2 2.00V
Connected
Freq: 14.07KHz
Time: 71.1uS


acer
HACK A DAY
FILCO
Hantek

视频演示


acer
HACK A DAY
DELL
Hantek
5 Pinning information
5.1 Pinning

边信道案例 – Fault Injection


sparkfun
70C
DIGITAL MULTIMETER
AUTO POWER OFF
RANGE
REL/RS232
10A
mA


Mic
LEDs
Fan
Reset
Power ON
Recovery


Esc

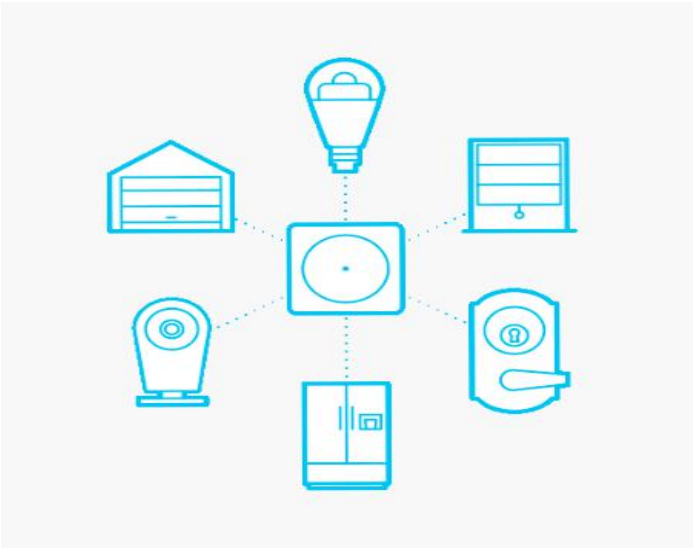
Got Root?

网关 (WinkHub)

. 物联网设备网关 WinkHub (ARM; RAM; NAND)

. 完美的将不同产品连接在一起 (GE; Nest; Dropcam; Philips)

. 支持 Zwave (915Mhz); RF (433Mhz); WIFI/Bluetooth/Zigbee (2.4G)



Got Root ?

通过网页对其进行访问 (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;

?>
```

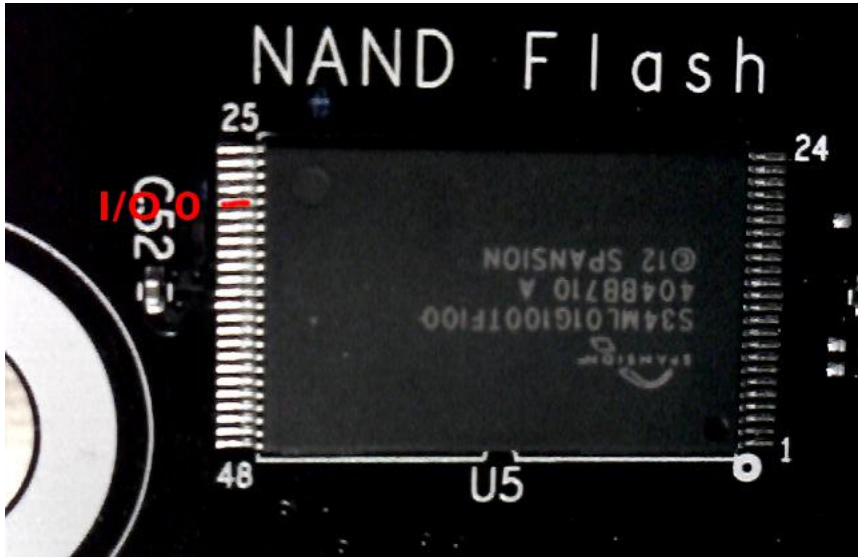
已被厂家打了补丁 :(

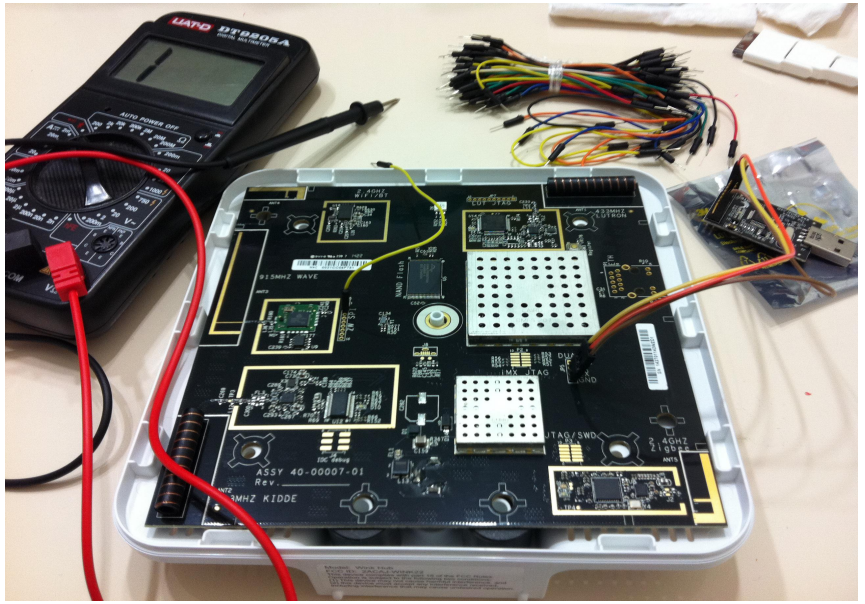
NAND-Glitch

. NAND Flash 通常存储固件; Bootloader; 内核以及root files

. 使用数据线在系统启动, 读取 NAND 内核信息瞬间, 短接 I/O pin 以达到数据阻断目的

. 在正确的时间点, 阻止 Bootloader 读取正确的内核数据从而进入 shell 模式

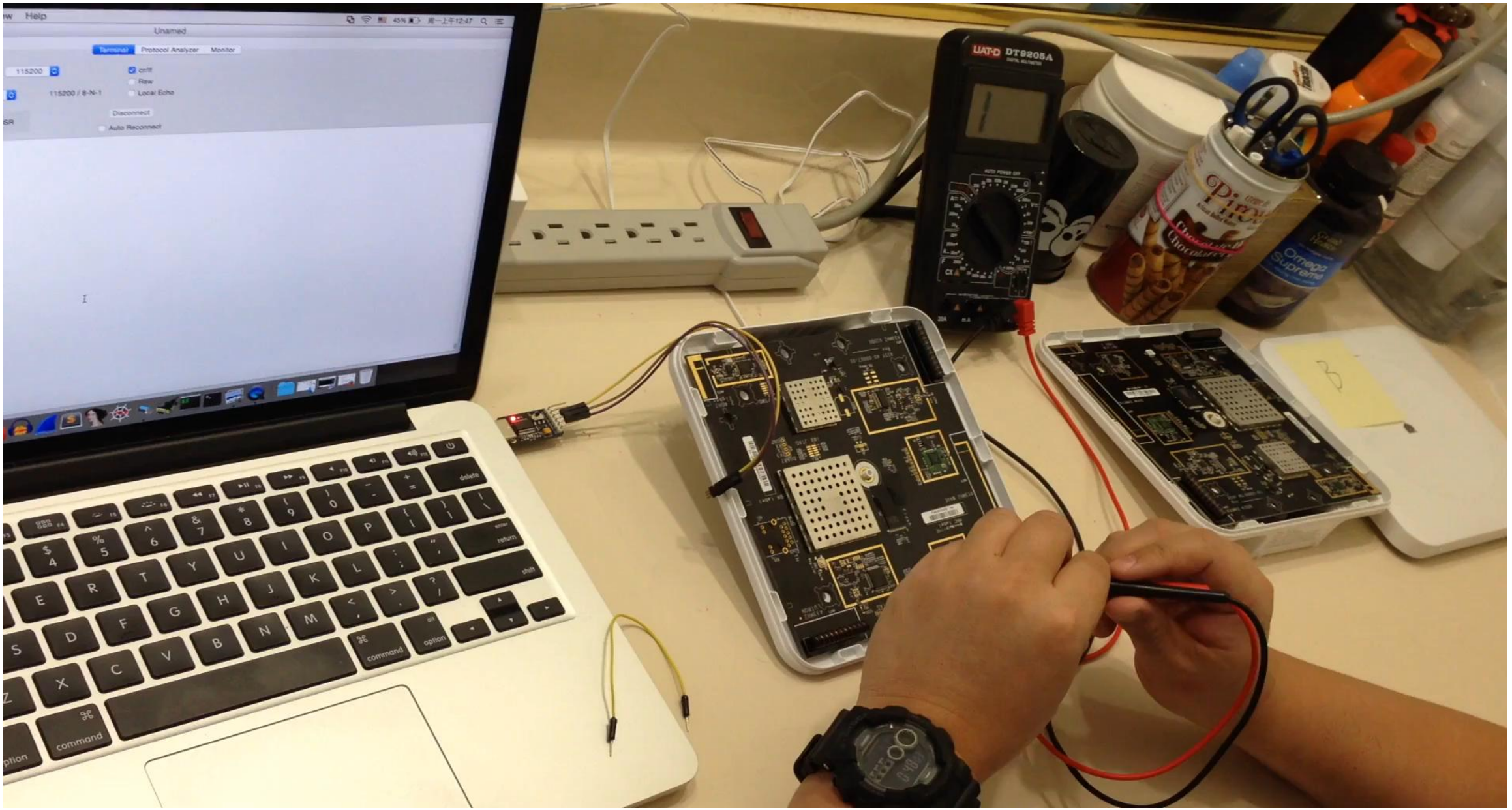




Got Root !

```
boot_updater=run updater_boot || run updater_boot_bad
bootargs=noinitrd console=ttyAM0,115200 rootfstype=ubifs ubi.mtd=5 root=ubi0:rootfs rw gpmi badupdater
bootcmd=mtdparts default; run boot_getflag || echo Falling back to updater...; run boot_updater
bootdelay=0
bootfile=uImage
ethact=FEC0
ethaddr=00:04:00:00:00:00
ethprime=FEC0
filesize=1
loadaddr=0x42000000
mtddevname=u-boot
mtddevnum=0
mtdids=nand0=gpmi-nand
mtdparts=mtdparts=gpmi-nand:3m(u-boot),4m(updater-kernel),28m(updater-rootfs),8m(database),8m(app-kernel),-(app-rootfs)
partition=nand0,0
serialno=152201606WZD1
stderr=serial
stdin=serial
stdout=serial
updater_args=setenv bootargs 'noinitrd console=ttyAM0,115200 rootfstype=ubifs ubi.mtd=2 root=ubi0:rootfs rw gpmi';
updater_boot=run updater_args && nand read ${loadaddr} updater-kernel 0x00300000 && bootm ${loadaddr}
updater_boot_bad=run appboot_args; setenv bootargs ${bootargs} badupdater; nand read ${loadaddr} app-kernel 0x00400000; bootm ${loadaddr}
ver=U-Boot 2014.01-14400-gda781c6-dirty (Apr 30 2014 - 22:35:38)

Environment size: 1775/16379 bytes
=>
```

视频演示


Help
Unnamed
Terminal
Protocol Analyzer
Monitor
115200
115200 / 8-N-1
Disconnect
Auto Reconnect
UAT-D DT9205A
command
option

网关 (Philips Hue)

. 飞利浦 Hue 系列智能家居灯控解决方案

. 采用 Zigbee 作为 Hue 与灯泡的无线通讯协议

. 案例 1: Hue 网关可通过 NAND Glitch 方式 Rooting

. 案例 2: 通过功耗分析提取硬编码 AES 密钥, 绕过固件升级认证

Got Root !

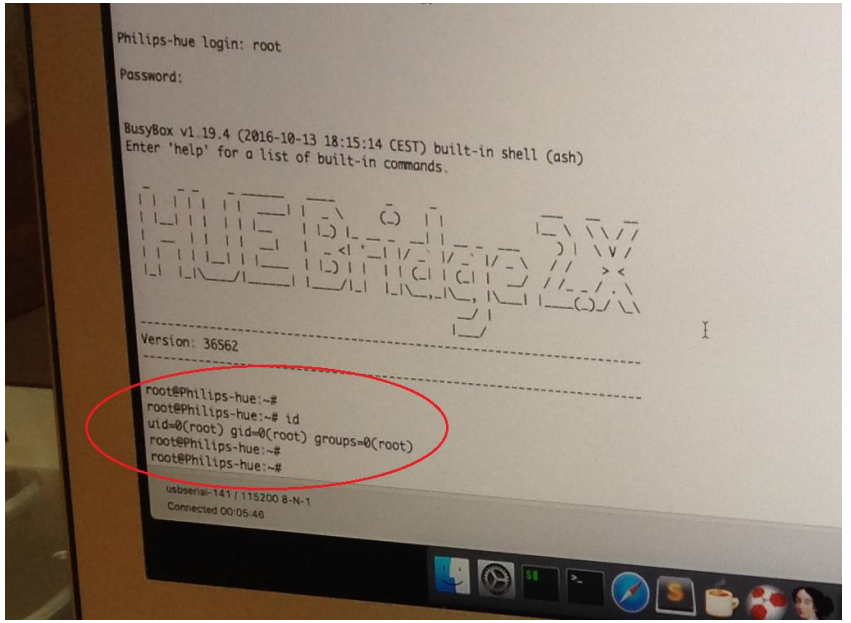
. setenv bootdelay 3

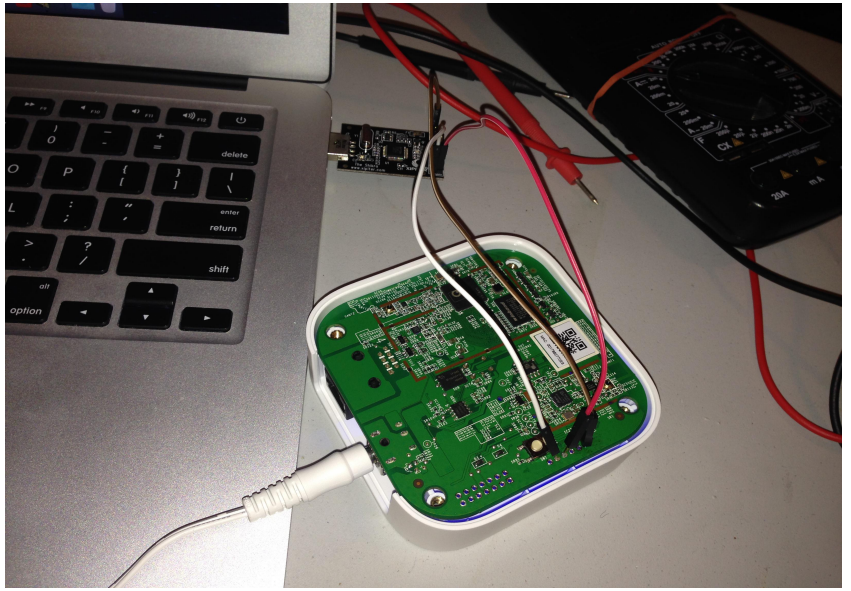
. setenv security '$1$3vGNd7Q3$ISqFeo1VkmQV6nyriUV0V/'

. saveenv & reset

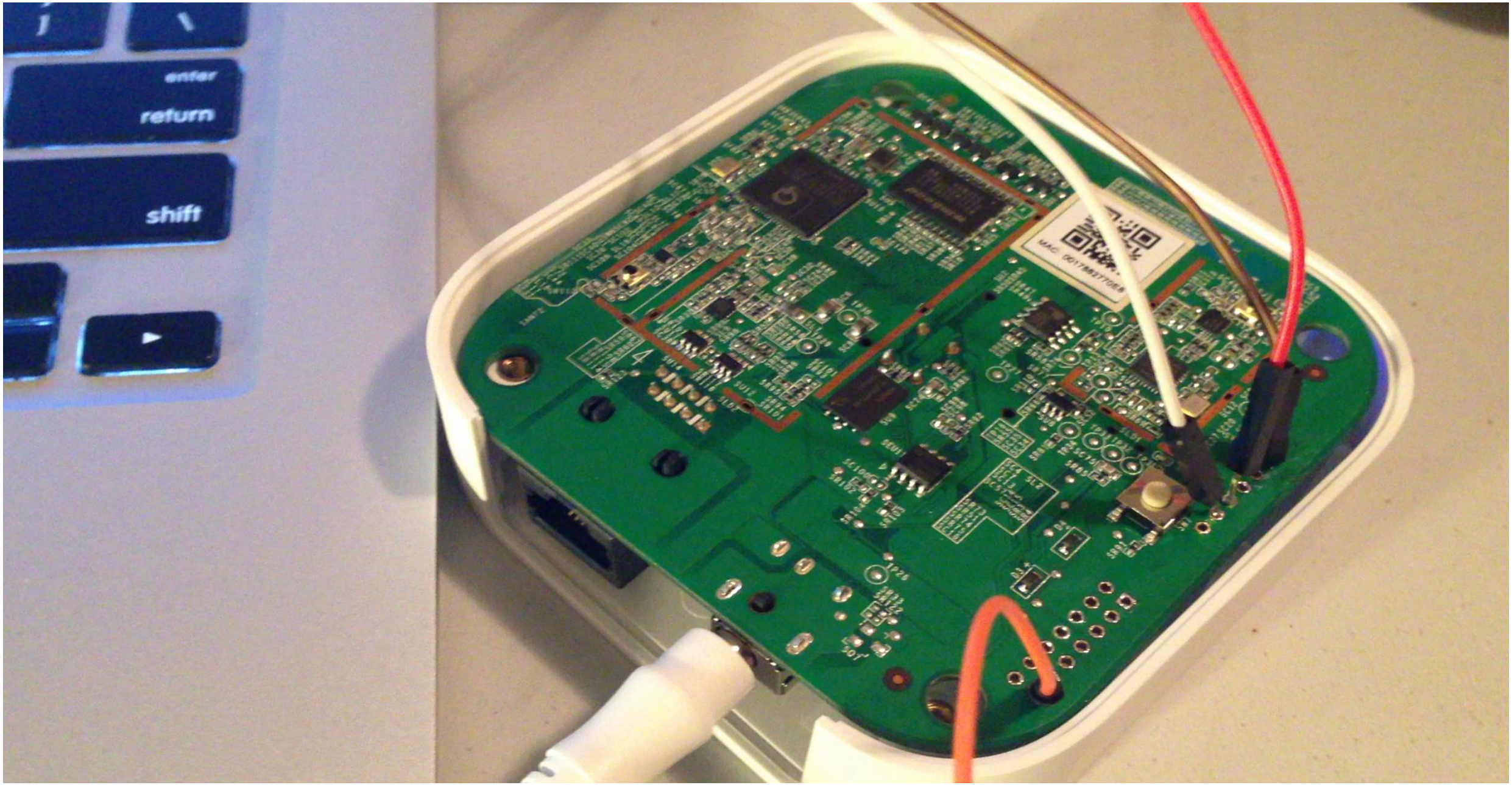
. HUE 默认 bootdelay 为 0, 且 root 哈希值都不同

. 在 U-Boot 启动读取内核信息瞬间短接 NAND SPI



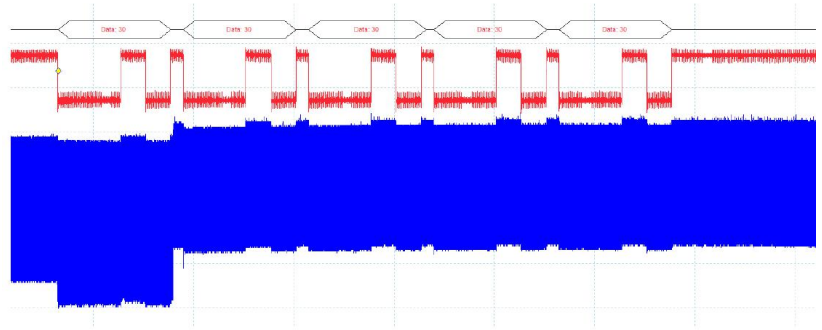


视频演示



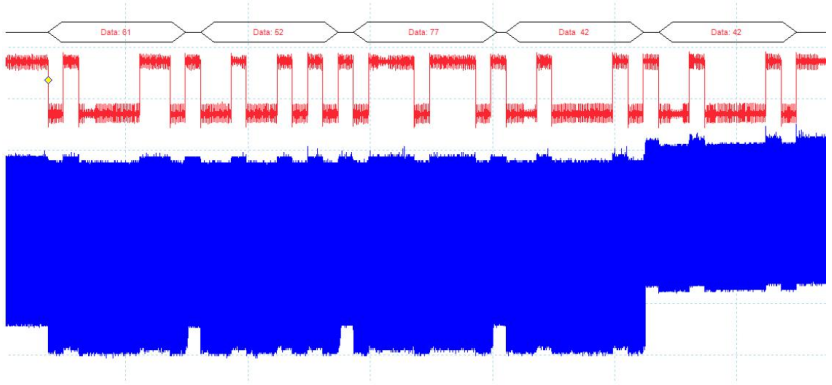
边信道案例 – Power Analysis & Glitch Attack

SPA - 简单功耗分析



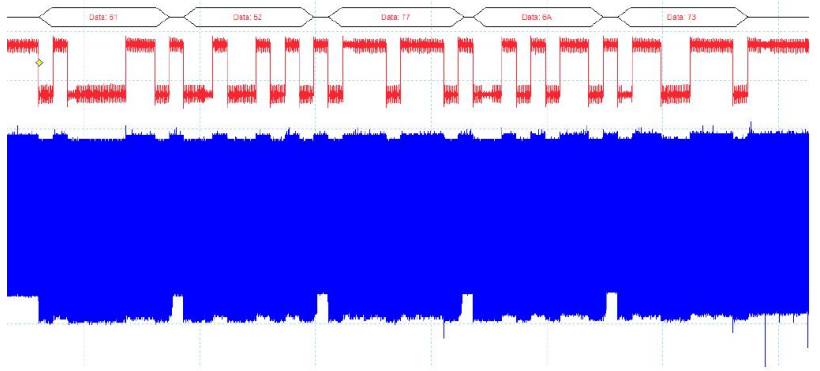
. 1998年 Paul Kocher 等将功耗分析带入民众视野

. 处理器运行不同指令在功耗需求上也不近相同



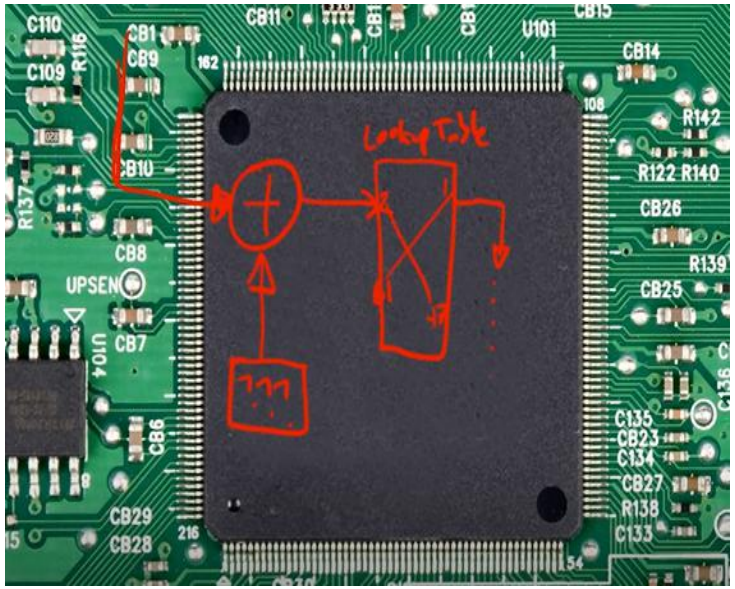
. 寻找目标设备在特定时刻 (解密) 功耗图形的差异

. 安全 Bootloader-TinySafeBoot (密码错误 -->无限循环)

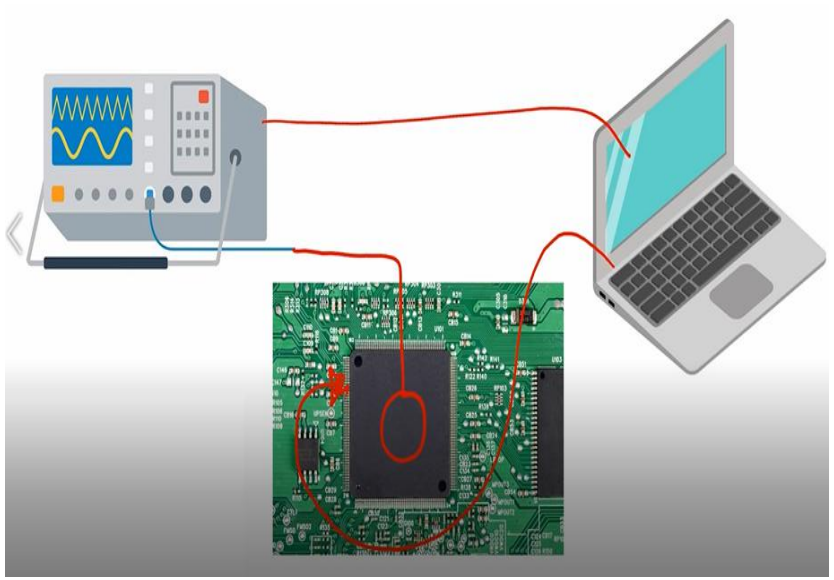


. RSA 进行平方和乘法运算时的功耗表现可被识别

DPA - 差分功耗分析



目标设备

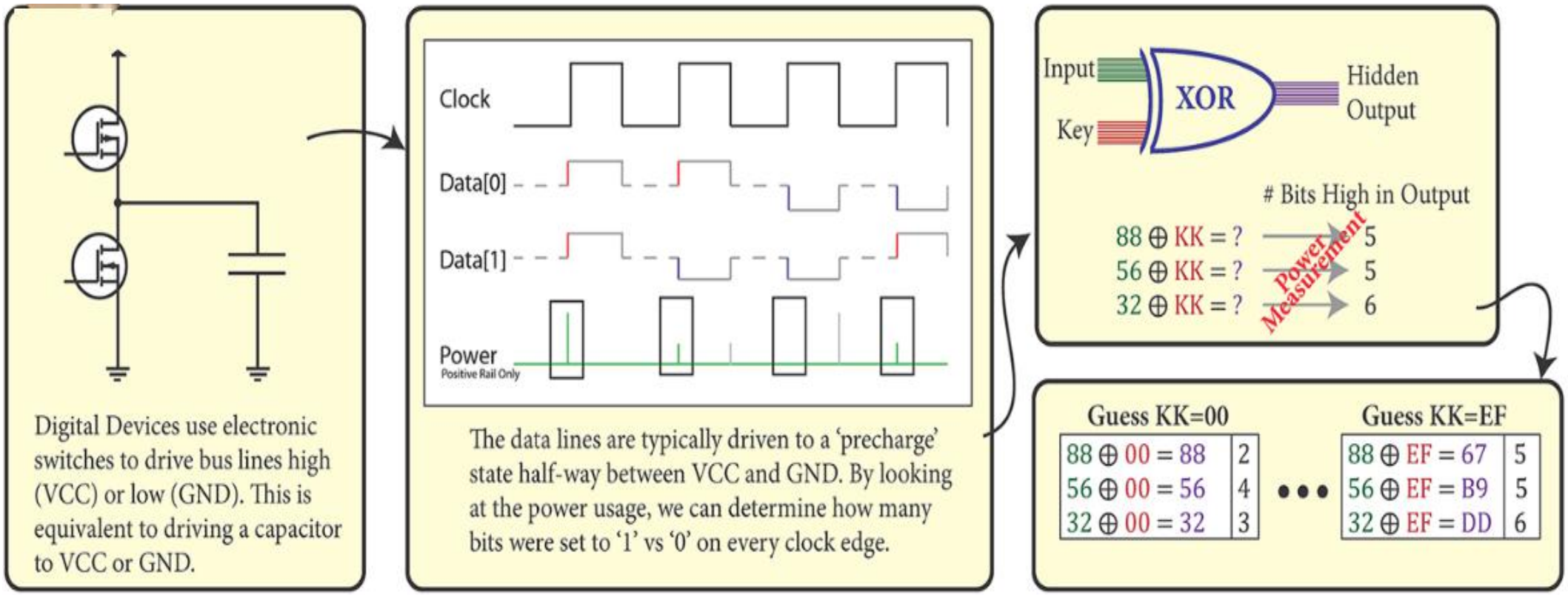


测量方法

Input Data	Power Measurement
0xC7	
0x1F	
0x2C	
0x89	
0x01	
0xD2	

测量结果

DPA - 差分功耗分析

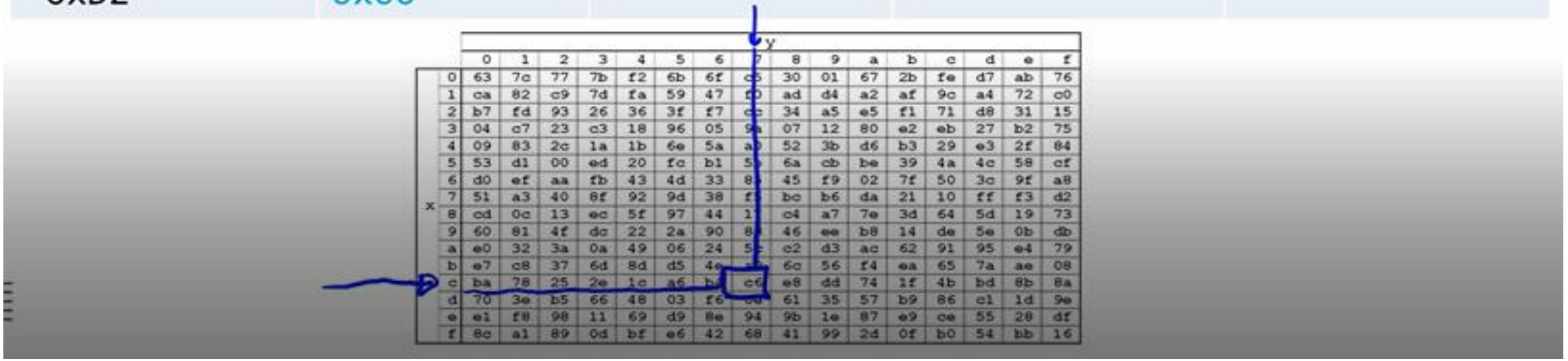

Digital Devices use electronic switches to drive bus lines high (VCC) or low (GND). This is equivalent to driving a capacitor to VCC or GND.
Clock
Data[0]
Data[1]
Power
Positive Rail Only
The data lines are typically driven to a 'precharge' state half-way between VCC and GND. By looking at the power usage, we can determine how many bits were set to '1' vs '0' on every clock edge.
Input
Key
XOR
Hidden Output
Bits High in Output
88 ⊕ KK = ?
56 ⊕ KK = ?
32 ⊕ KK = ?
Power Measurement
5
5
6
Guess KK=00
88 ⊕ 00 = 88 2
56 ⊕ 00 = 56 4
32 ⊕ 00 = 32 3
Guess KK=EF
88 ⊕ EF = 67 5
56 ⊕ EF = B9 5
32 ⊕ EF = DD 6

DPA - 差分功耗分析

Input Data	Hyp. Key	XOR Output	Hyp. Output	Number 1's
0xC7	0x00	0xC7	0xC6	4
0x1F	0x00	0x1F	0xC0	2
0x2C	0x00	0x2C		
0x89	0x00	0x89		
0x01	0x00	0x01		
0xD2	0x00			

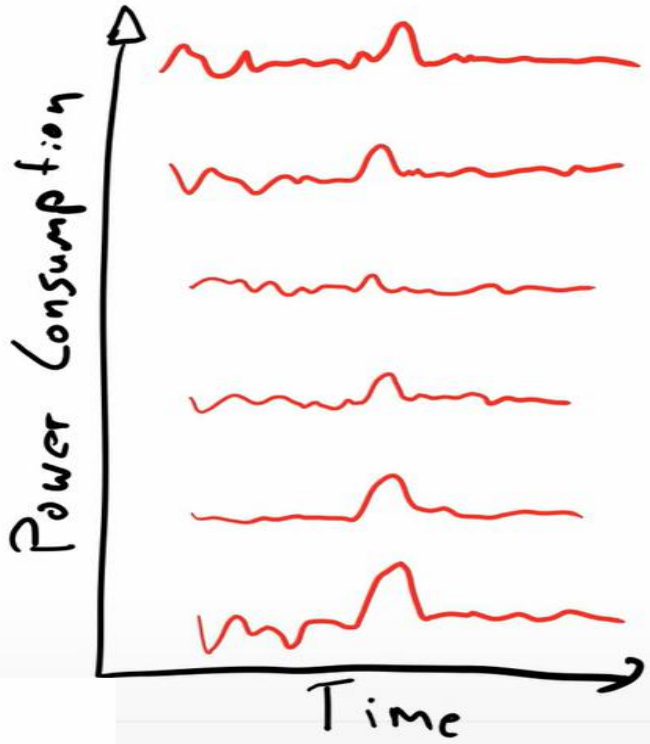
XOR

11000110



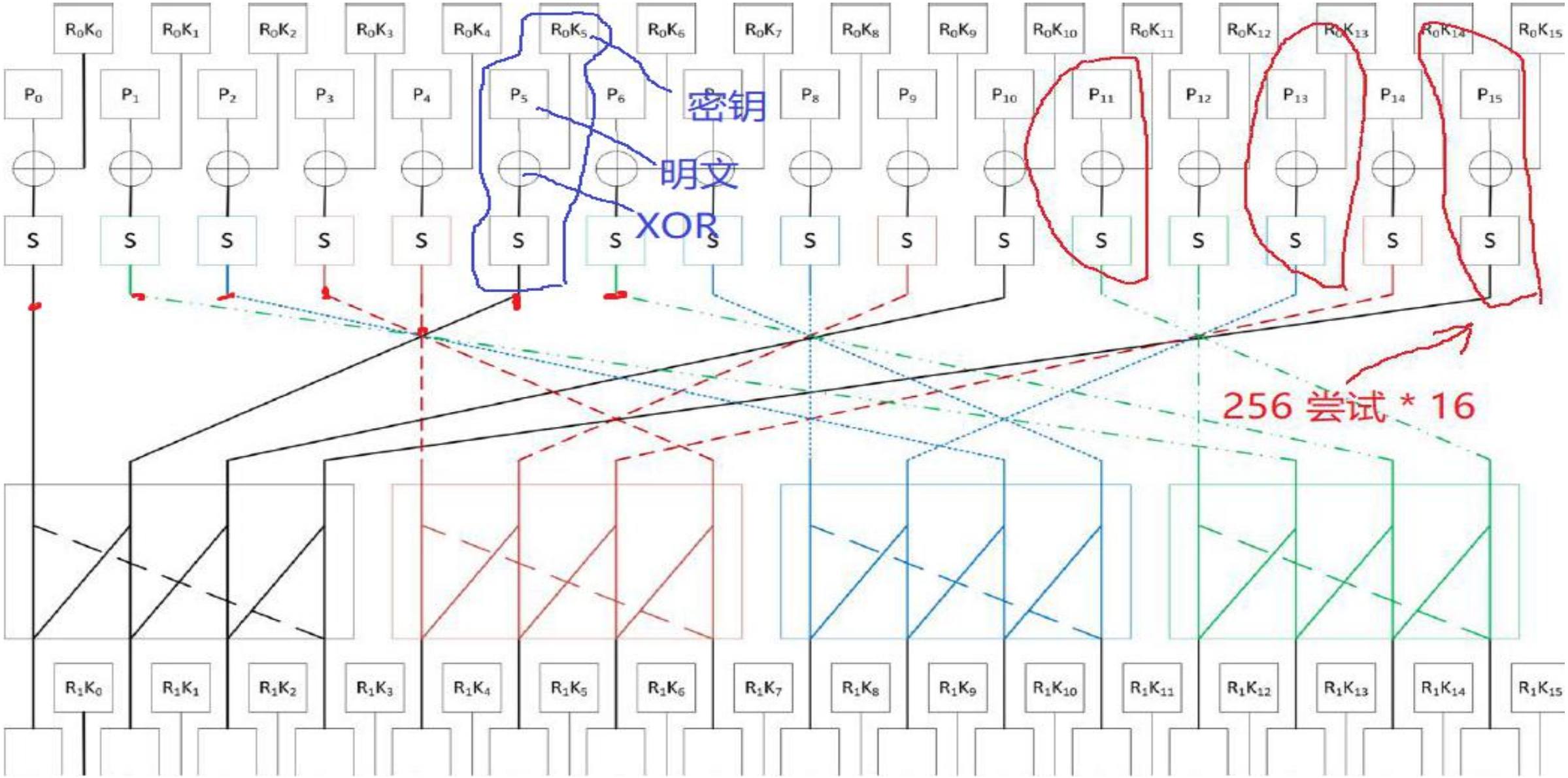
DPA - 差分功耗分析

Correlation Power Analysis



..	0x3D	..	0xFF
	4		3
	4		4
	2		4
	4		3
	6		6
	7		5

DPA - 差分功耗分析 AES-128



DPA - 差分功耗分析

Device Attacked	Year Published	Authors
Microchip HCSxxx	2008	Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, Mohammad T. Manzuri Shalmani
Atmel XMEGA	2009	Ilya Kizhvatov
Mifare DESFire MF3ICD40	2011	David Oswald, Christof Paar
Xilinx Virtex-II	2011	Amir Moradi, Alessandro Barenghi, Timo Kasper, Christof Paar
Xilinx Spartan 6	2011	Amir Moradi, Markus Kasper, Christof Paar
Microsemi ProASIC3	2012	Sergei Skorobogatov, Christopher Woods
Xilinx Virtex-4, Virtex-5	2011	Amir Moradi, Markus Kasper, Christof Paar
DS2432, DS28E01	2013	David Oswald
Yubikey 2	2013	David Oswald
Altera Stratix II	2013	Amir Moradi, David Oswald, Christof Paar, Pawel Swierczynski
Altera Stratix III	2014	Amir Moradi, David Oswald, Christof Paar, Pawel Swierczynski
Atmel ATMega128RFA1	2015	Colin O'Flynn, Zhizhang Chen

Glitch - 毛刺注入

. Glitch 注入目的在于改变目标设备的设计初衷

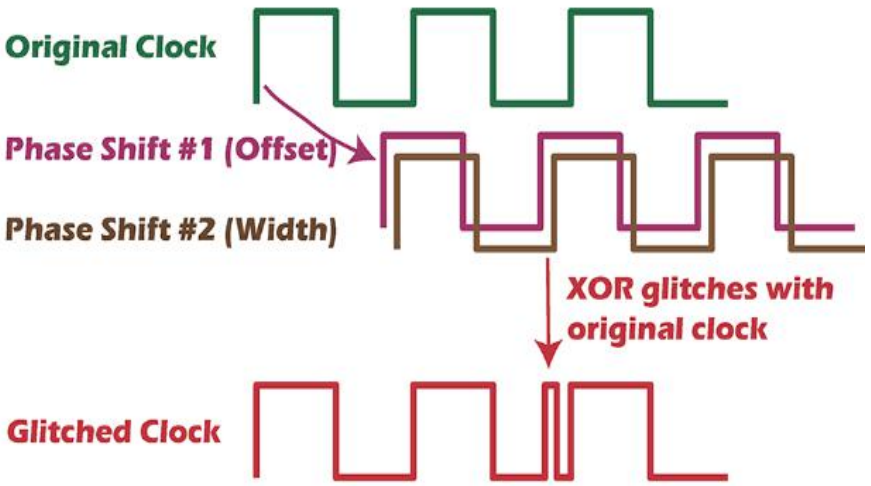
. 通过打乱程序的正常流程, 绕过密码安全认证机制

. 使用EM; 激光; 热能; 噪音; 时钟; 电压等作为注入源

. 精确的Glitch注入时间点至关重要 (手动; SAD; 模式)

. Glitch 结果具有不可预测性, 错误可能导致设备 Reset

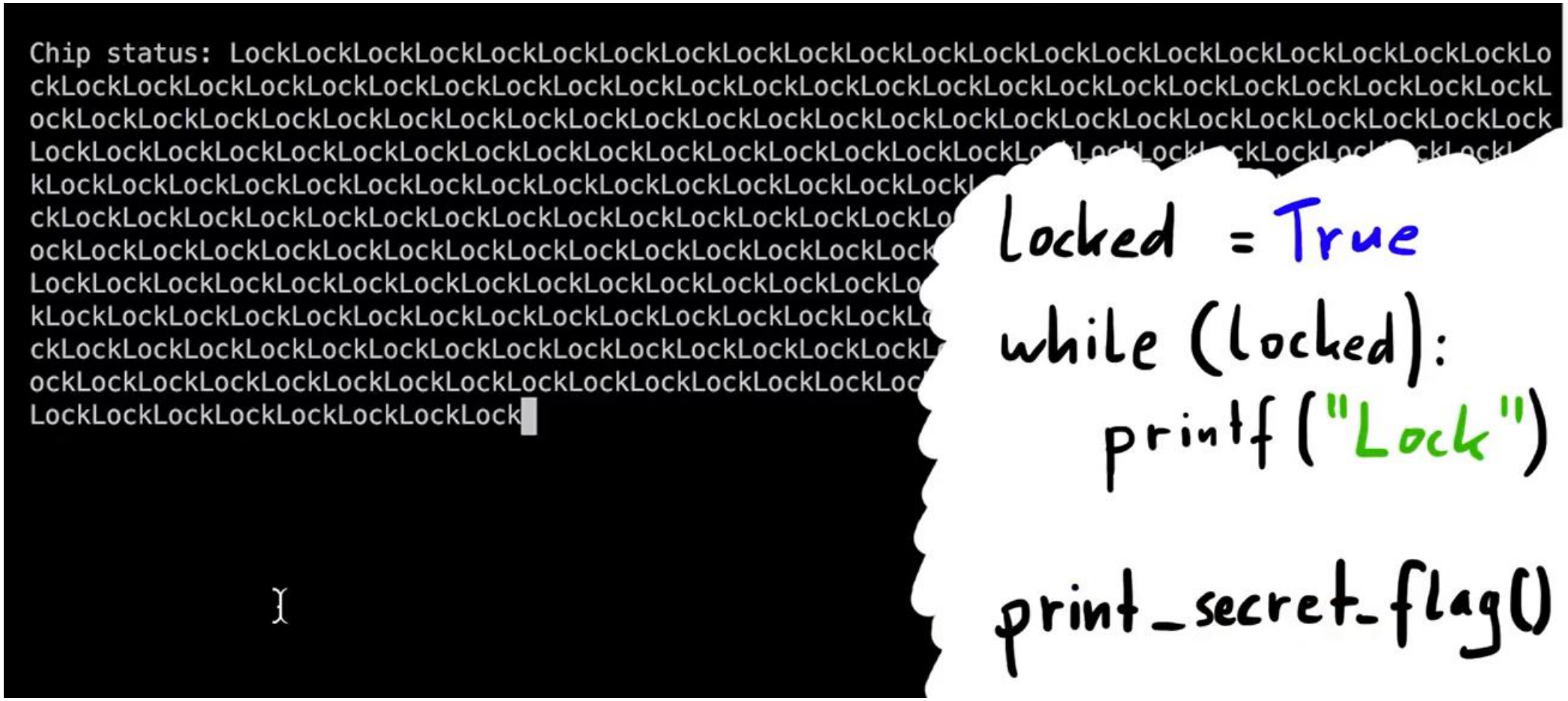
```
...
if( key_is_correct ) <-- Glitch here!
{
  open_door();
}
else
{
  keep_door_closed();
}
```



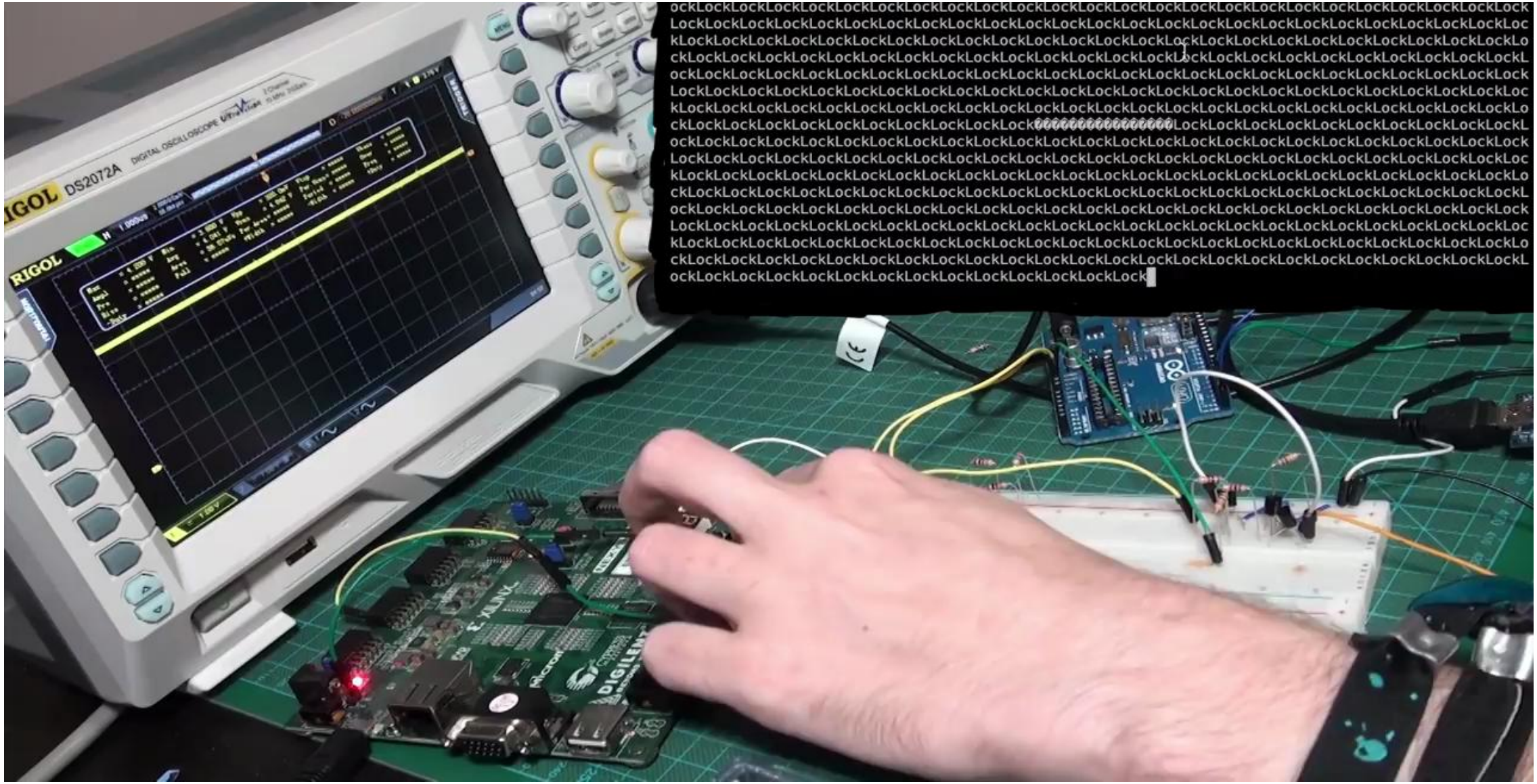
源代码 Linux-util-2.24

```
#include "auth.h"
#include "pamfail.h"

int auth_pam(const char *service_name, uid_t uid, const char *username)
{
    if (uid != 0) {
        pam_handle_t *pamh = NULL;
        struct pam_conv conv = { misc_conv, NULL };
        int retcode;

        retcode = pam_start(service_name, username, &conv, &pamh);
        if (pam_fail_check(pamh, retcode))
            return FALSE;

        retcode = pam_authenticate(pamh, 0);
        if (pam_fail_check(pamh, retcode))
            return FALSE;

        retcode = pam_acct_mgmt(pamh, 0);
        if (retcode == PAM_NEW_AUTHTOK_REQD)
            retcode =
                pam_chauthtok(pamh, PAM_CHANGE_EXPIRED_AUTHTOK);
        if (pam_fail_check(pamh, retcode))
            return FALSE;

        retcode = pam_setcred(pamh, 0);
        if (pam_fail_check(pamh, retcode))
            return FALSE;

        pam_end(pamh, 0);
        /* no need to establish a session; this isn't a
         * session-oriented activity...  */
    }
    return TRUE;
}
```

CTF 送分题


Chip status: LockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLo
ckLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLo
kLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockL
ckLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLock
LockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLo
kLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockL
ckLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockL
ockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLockLoc
LockLockLockLockLockLockLockLock
locked = True
while (locked):
printf ("Lock")
print_secret_flag()

视频演示


RIGOL DS2072A DIGITAL OSCILLOSCOPE
RIGOL
DIGILENT
XILINX

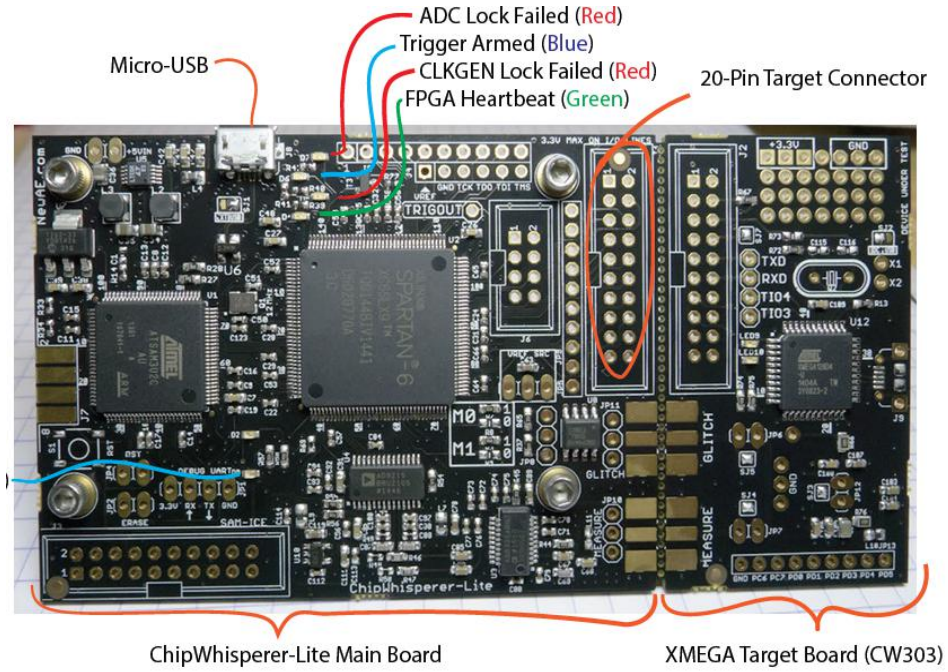
ChipWhisperer-Lite

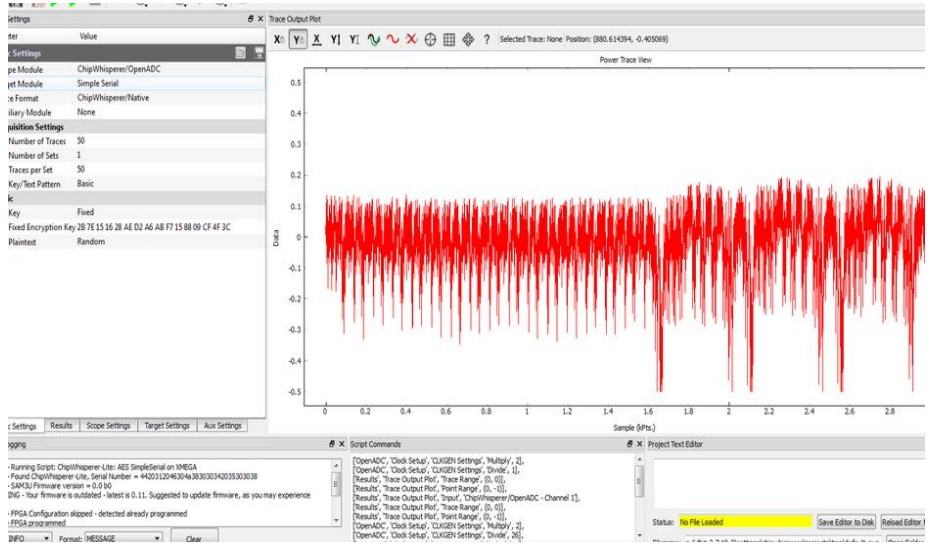
. 由 Colin O'Flynn 设计制作, 学习 SCA 功耗分析和毛刺注入神器

. 基于Python 跨平台开源软硬件项目 (Windows; Linux; MacOS)

. 可用于时序或电压毛刺注入攻击测试, 产生 <2nS 的脉冲信号

. 通过 DPA 差分功耗分析破解诸如 RSA; AES; 3DES 等加密算法





总结:

- Kein System ist Sicher: 100% 安全的系统并不存在
- 剑走偏锋的边信道攻击威力无比, 硬件安全必备技能
- 无论多完美的加密算法, 实施过程中的百密一疏, 就会导致系统安全完全崩溃

问题？