KCon

KCon 2019 無界

2019

IOT安全 - 测信道实战

演讲人：KEVIN2600

@Kevin2600

议程

. 测信道的那点事

. 测信道案例简析

. 测信道 Power Analysis

测信道的那点事

测信道

测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，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

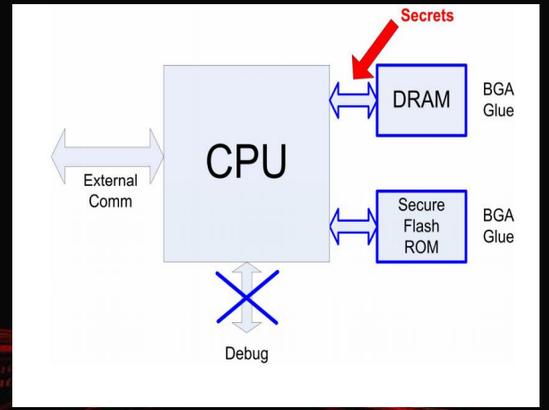
测信道

. Public key signature check

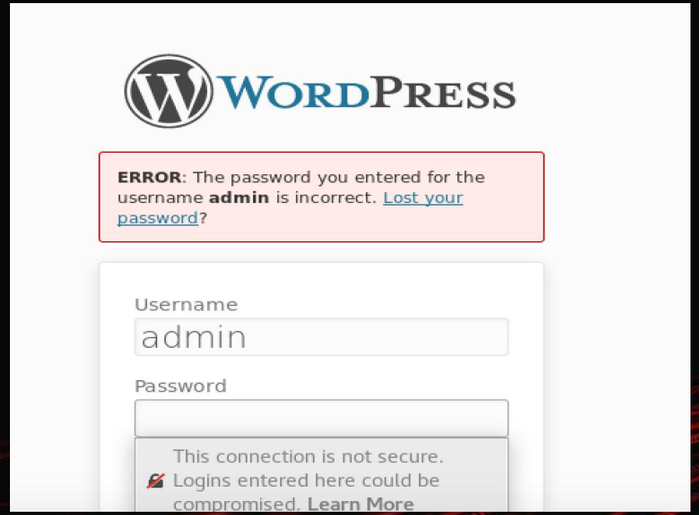
. Bootloader 加固 (bootdelay = 0)

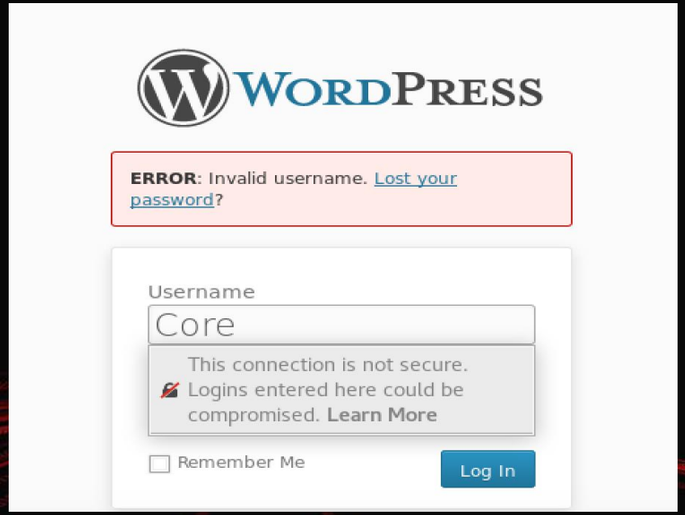
. 屏蔽调试端口 UART; JTAG; SPI; I2C

. 电子设备全部物理隔离 (Air Gapping)

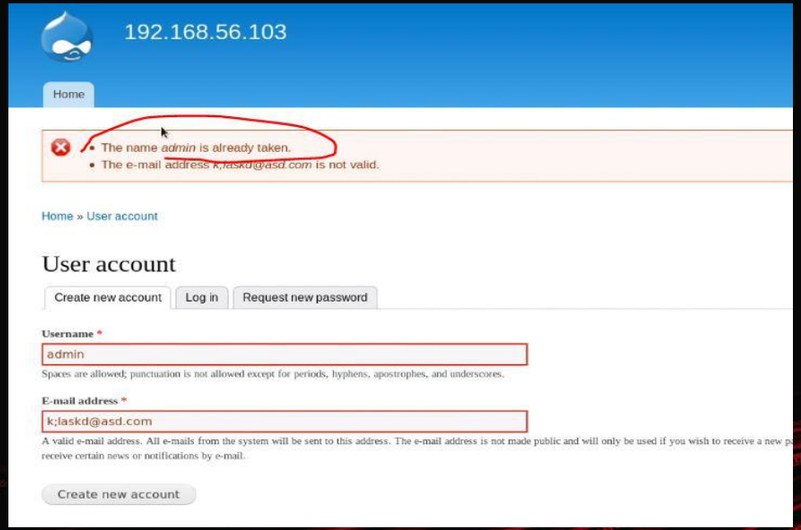


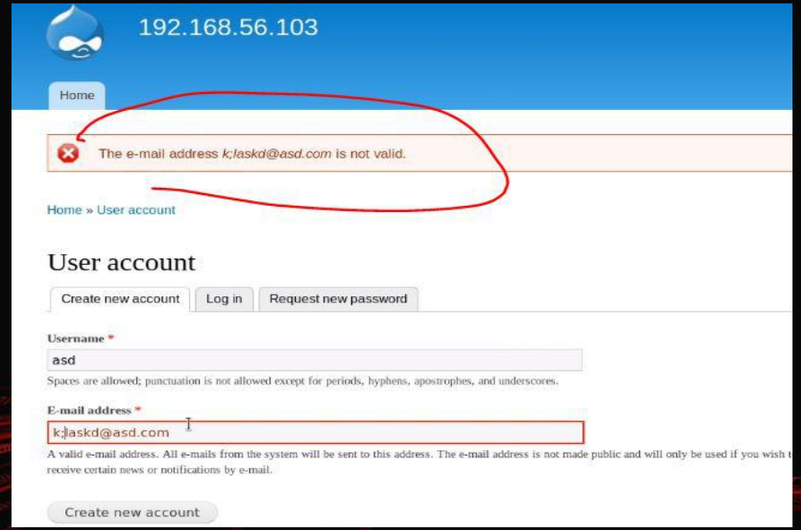
测信道 WordPress



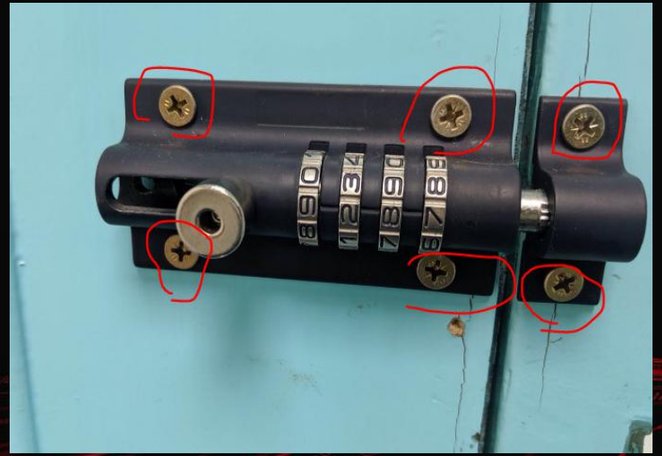


测信道 Drupal

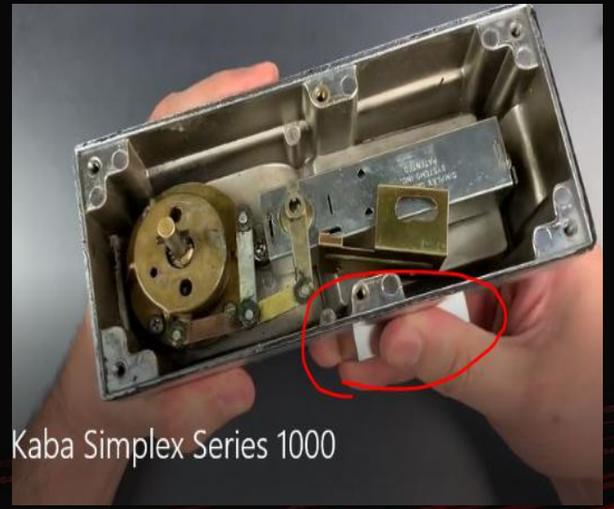

192.168.56.103
Home
The name admin is already taken.
The e-mail address k;laskd@asd.com is not valid.
Home » User account
User account
Create new account
Log in
Request new password
Username *
admin
Spaces are allowed; punctuation is not allowed except for periods, hyphens, apostrophes, and underscores.
E-mail address *
k;laskd@asd.com
A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will only be used if you wish to receive a new p
receive certain news or notifications by e-mail.
Create new account

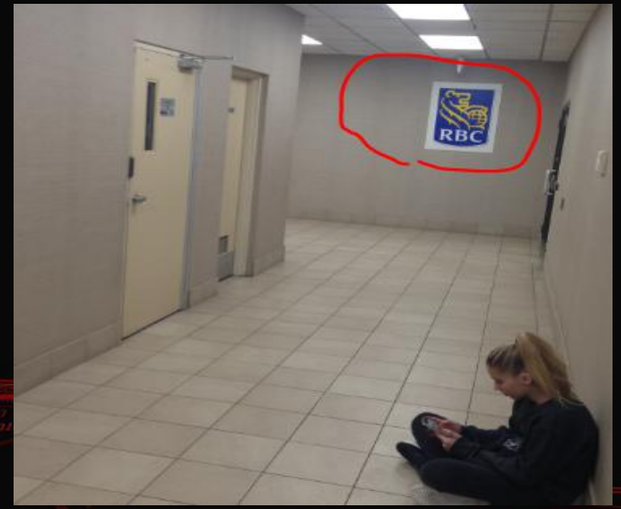

192.168.56.103
Home
The e-mail address k;laskd@asd.com is not valid.
Home » User account
User account
Create new account
Log in
Request new password
Username *
asd
Spaces are allowed; punctuation is not allowed except for periods, hyphens, apostrophes, and underscores.
E-mail address *
k;laskd@asd.com
A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will only be used if you wish t
receive certain news or notifications by e-mail.
Create new account

测信道门禁



测信道门禁





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)

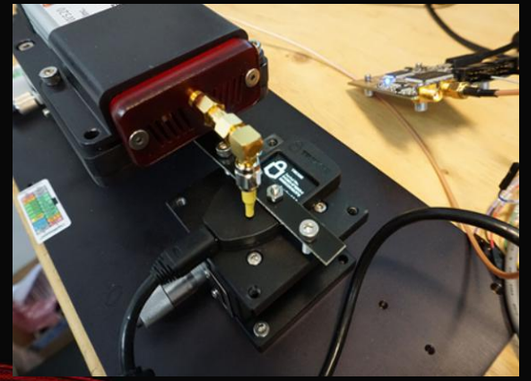
主动式:

: Xbox360 Glitch 攻击 (运行 unsigned code)

: 智能网关 Hue NAND Glitch (得到 Root 权限)

: 通过毛刺注入成功获取硬件钱包 Trezor 闪存敏感信息

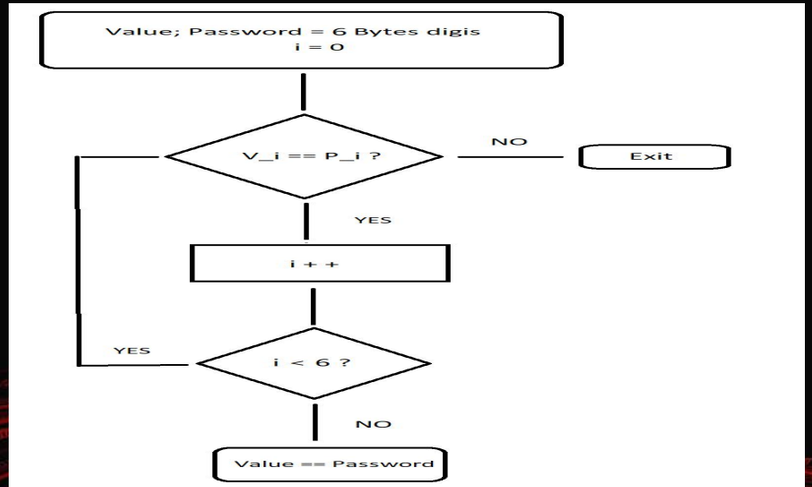
: 以色列 Ben-Gurion 大学通过 USB 发送电磁信号 (USBee)

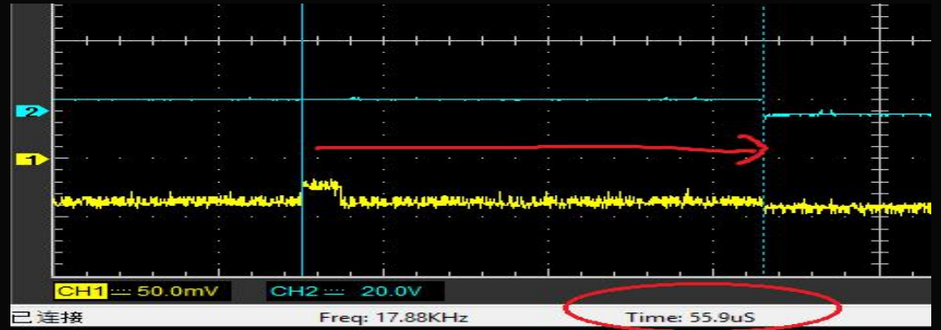


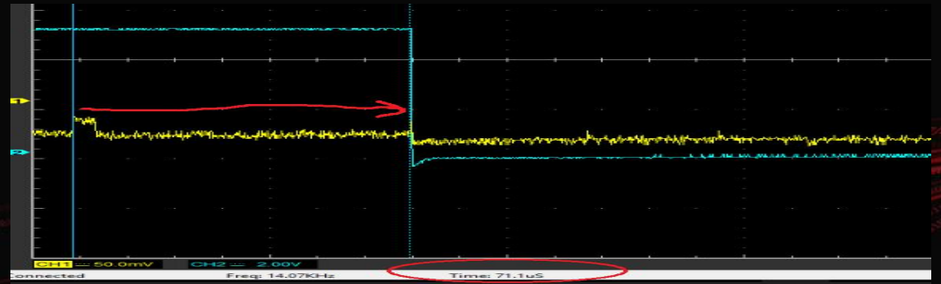
测信道案例简析

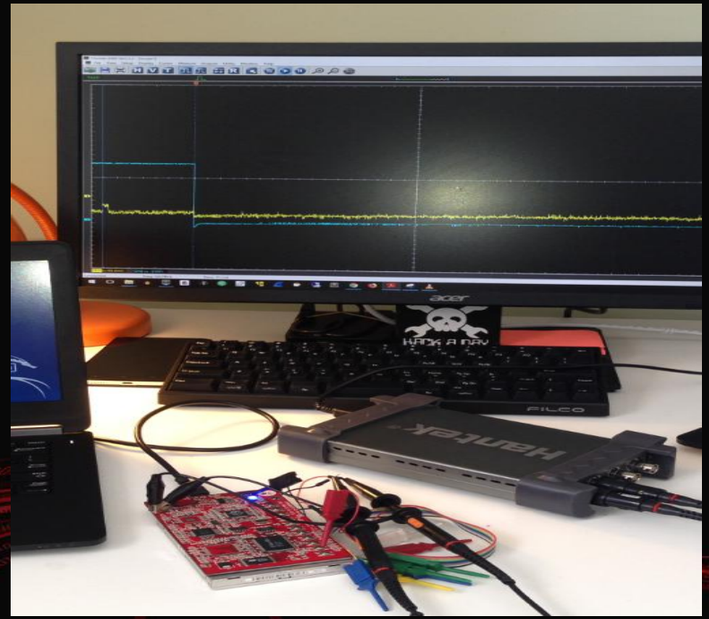
时耗分析

```
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;

        }
}
```

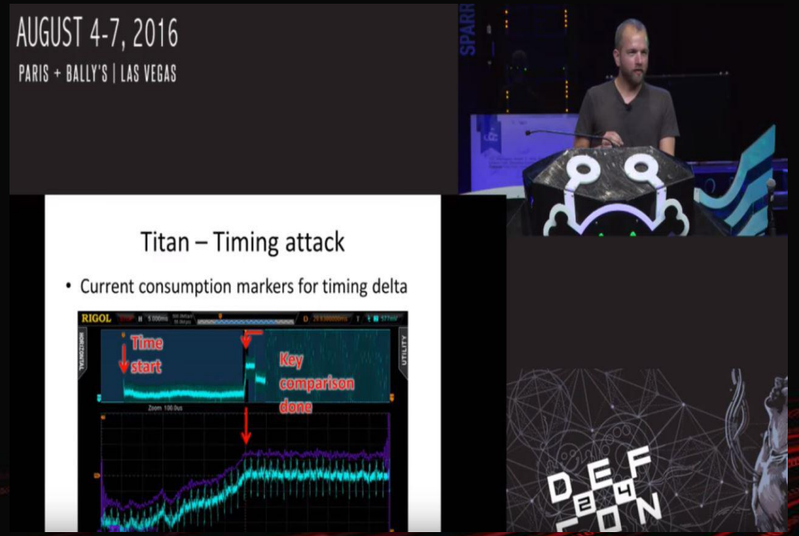



CH1 50.0mV
CH2 20.0V
已连接
Freq: 17.88KHz
Time: 55.9uS


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


acer
HACK A DAY
FILCO
Hantek

时耗分析



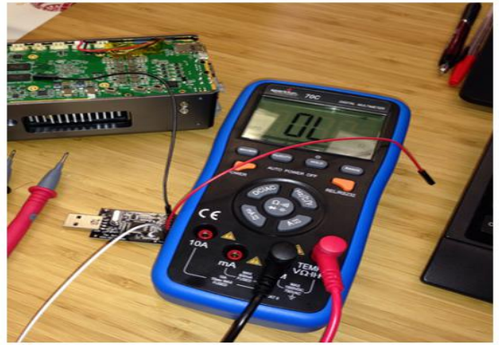
Titan – Timing attack

- Entire six-digit keypad sequence is captured before starting comparison to key from EEPROM
- Pseudocode of Titan keycode comparison:

```
bool check_code(int enteredCode[6], int actualCode[6])
{
    for (int digit = 0; digit < 6; digit++)
        if (enteredCode[digit] != actualCode[digit])
            return false;

    return true;
}
```

Each iteration takes another 28 µs

NAND-Glitch



Got Root?

NAND-Glitch

物联网设备网关 (WinkHub)

通过网页对其进行访问 (set_dev_value.php)

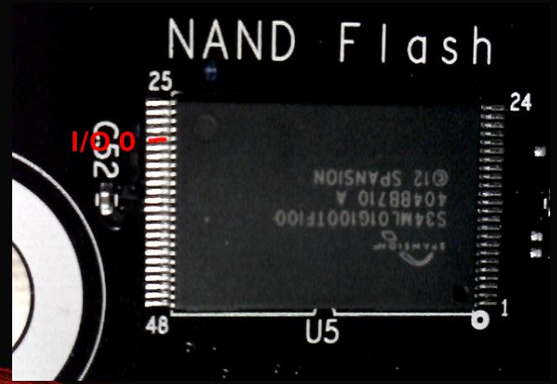
curl “192.168.01/set_dev_value.php” -d “nodeId=a&attrId=; uname -a;”

NAND-Glitch

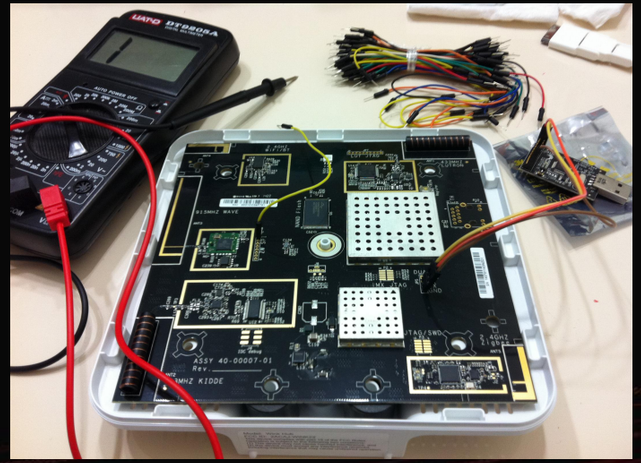
. NAND Flash 通常存储固件; Bootloader; 内核以及root files

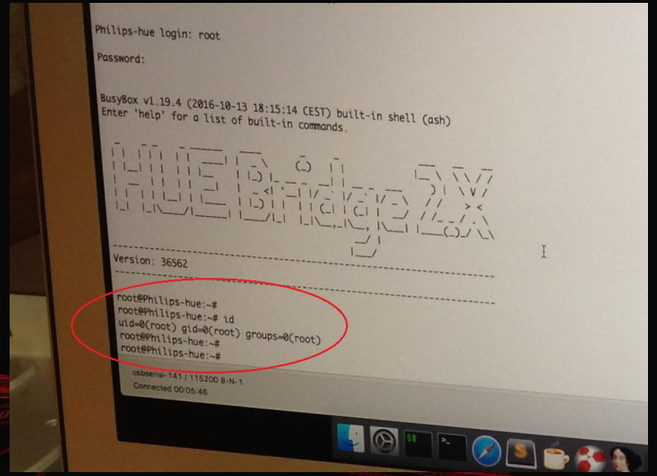
. 使用数据线在系统启动, 读取 NAND 内核信息瞬间, 短接 I/O pin

. 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



NAND-Glitch




Philips-hue login: root
Password:
BusyBox v1.19.4 (2016-10-13 18:15:14 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
Version: 36562
root@Philips-hue:~#
root@Philips-hue:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Philips-hue:~#
root@Philips-hue:~#

测信道 Power Analysis

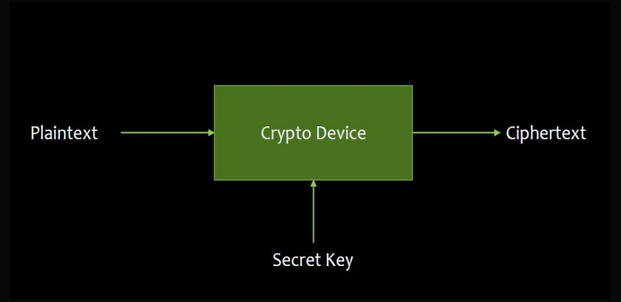
功耗分析

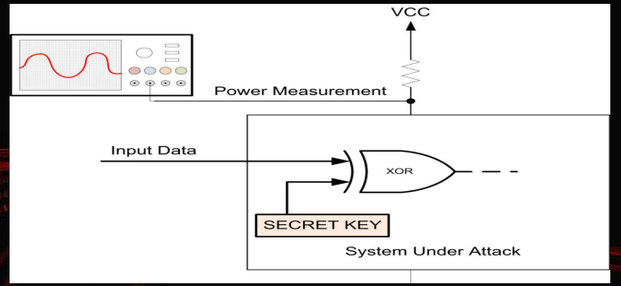
. Power analysis (Simple & Differential)

. 处理器运行不同指令在功耗需求上也不近相同

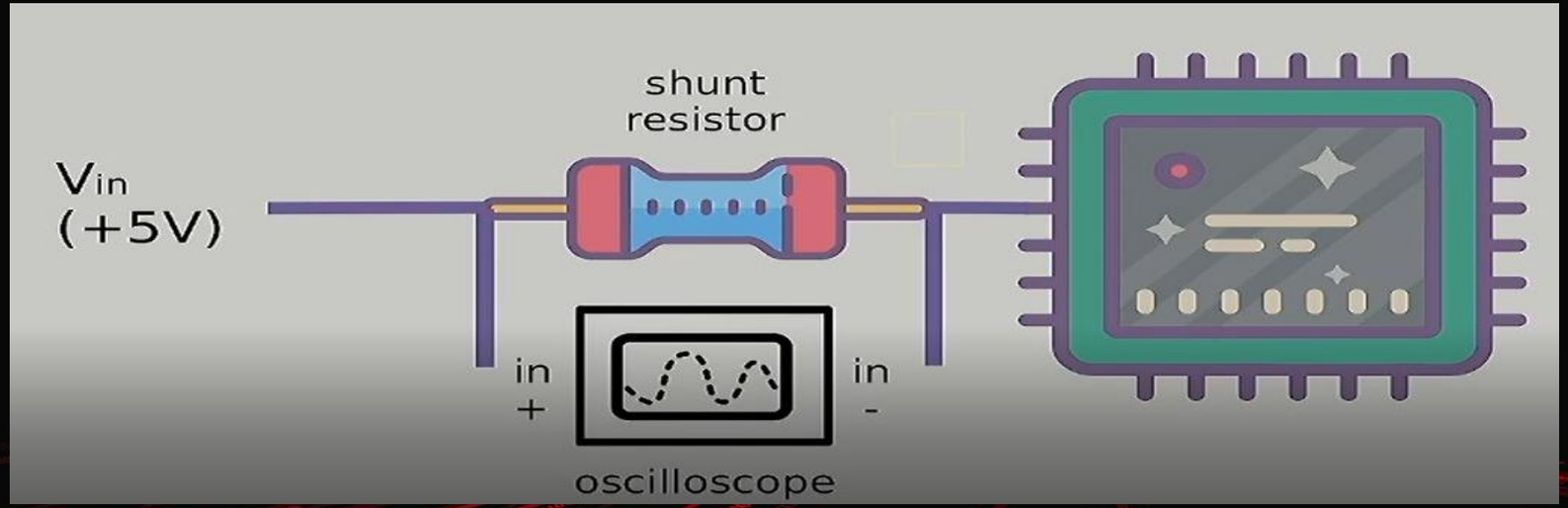
. 需要了解目标设备所采用的加密算法

. 信号的采集必须在加密或解密的过程中完成





功耗分析



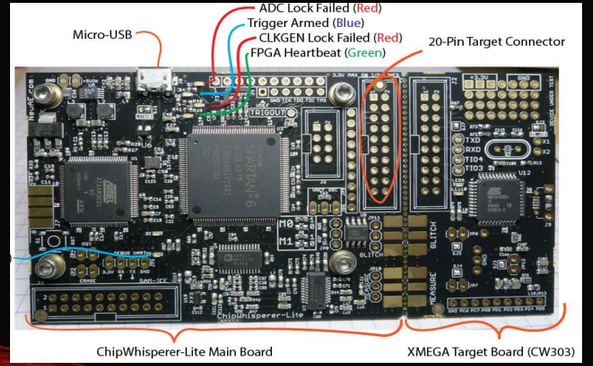
功耗分析 (ChipWhisperer)

. 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 差分功耗分析获取诸如 RSA; AES; 3DES 等加密密钥

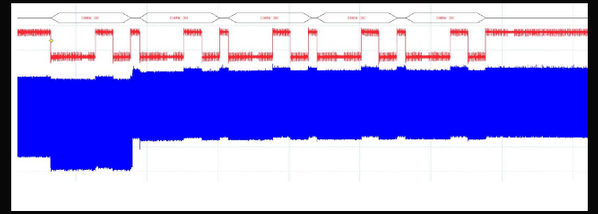


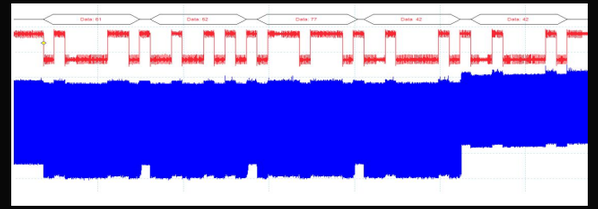
功耗分析 (SPA)

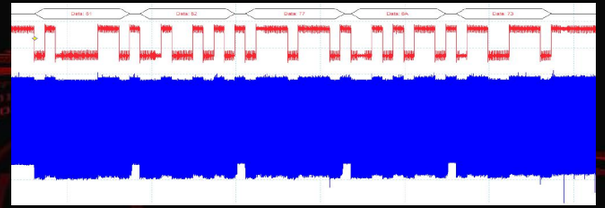
. 处理器运行验证指令在功耗表现上不尽相同

. 密码验证过程功耗表现 (密码错误 -->无限循环)

. 寻找目标设备在特定时刻 (加密/解密) 功耗图形的差异

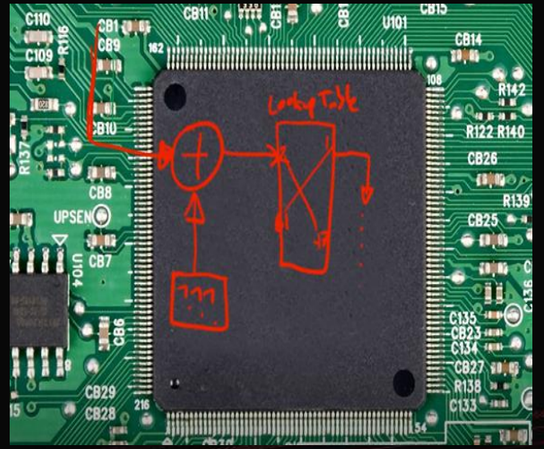




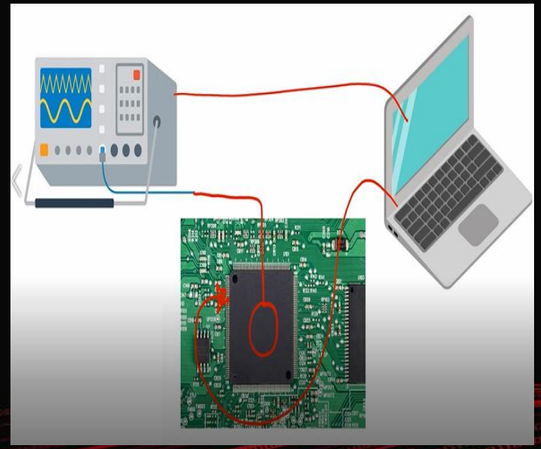


功耗分析 (SPA)

功耗分析 (DPA)



目标设备

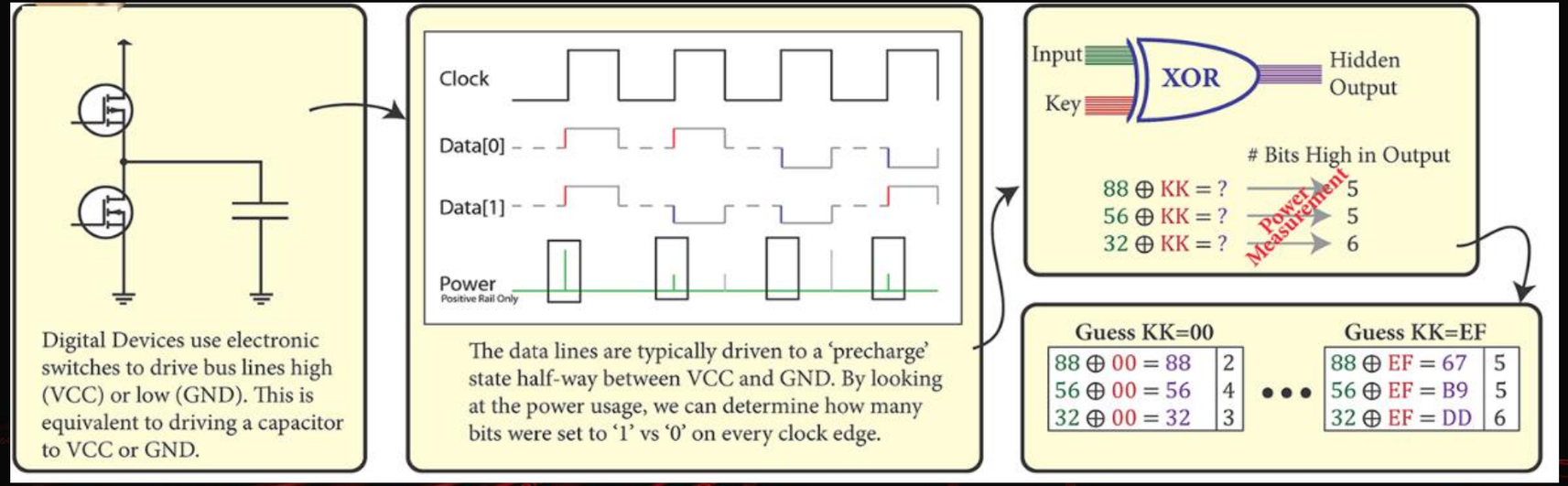


测量方法

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

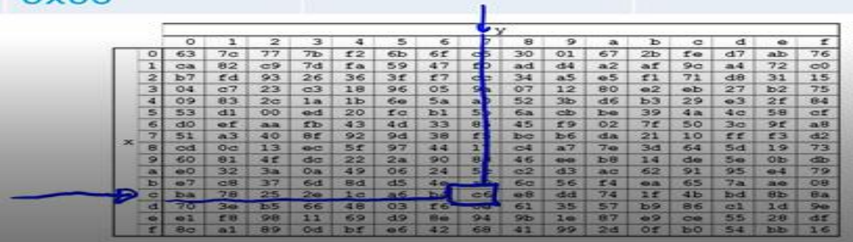
测量结果

功耗分析 (DPA)

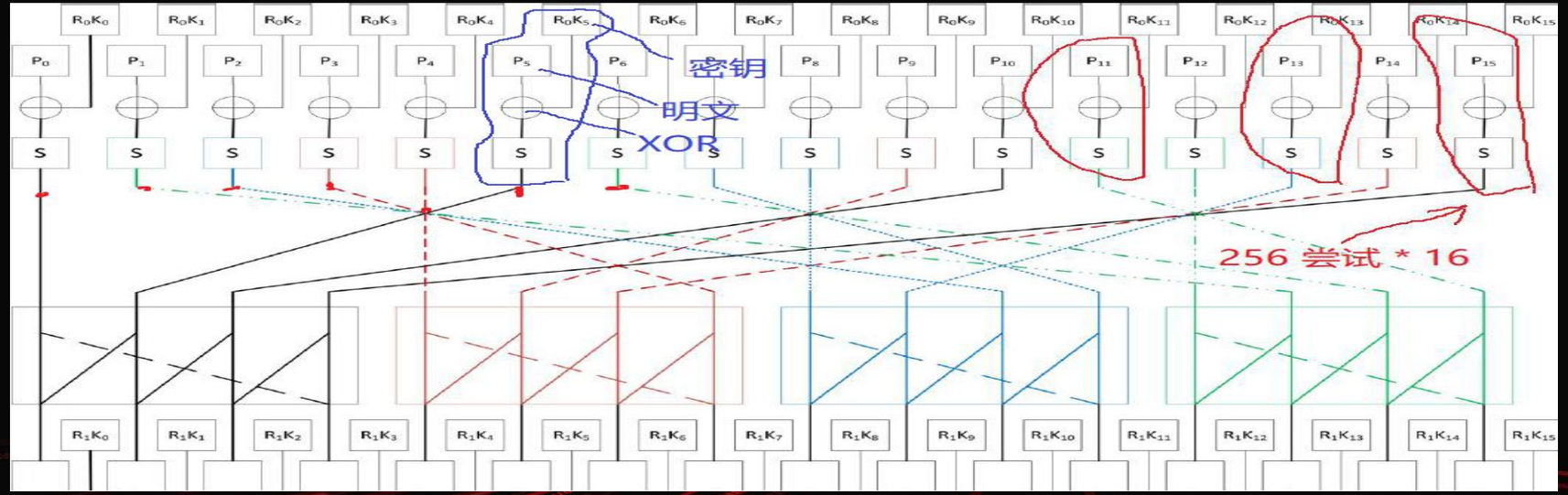

Digital Devices use electronic switches to drive bus lines high (VCC) or low (GND). This is equivalent to driving a capacitor to VCC or GND.
Clock
Data[0]
Data[1]
Power
Positive Rail Only
The data lines are typically driven to a 'precharge' state half-way between VCC and GND. By looking at the power 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 = ? 5
56 ⊕ KK = ? 5
32 ⊕ KK = ? 6
Power Measurement
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

功耗分析 (DPA)

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			

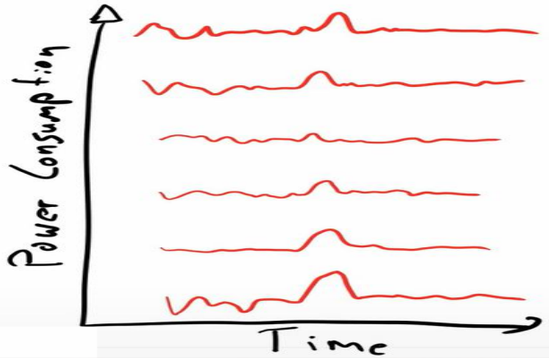


功耗分析 (AES-128)



功耗分析 (DPA)

Correlation Power Analysis



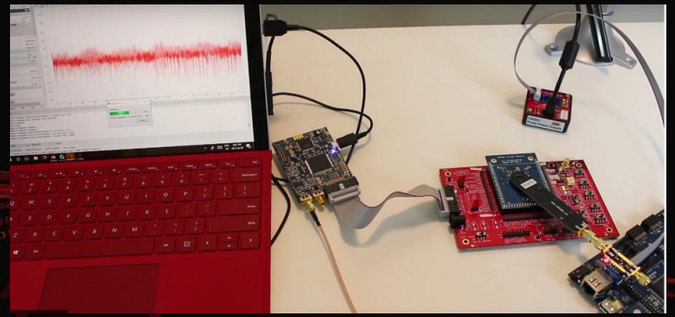
..	0x3D	..	0xFF
	4		3
	4		4
	2		4
	4		3
	6		6
	7		5

功耗分析 (电磁信号)

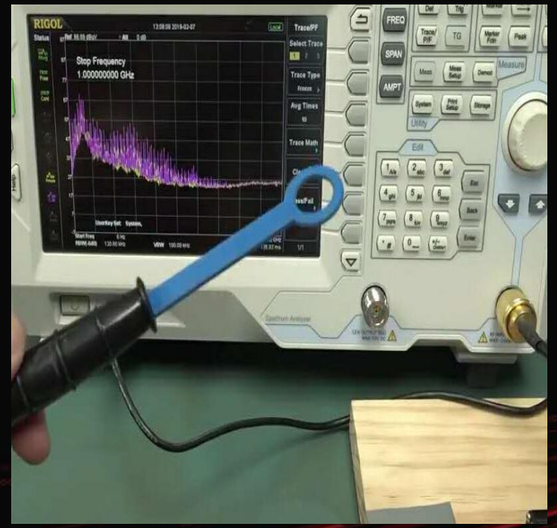
. 电磁波可通过 H 探头和软件无线电设备远程获取

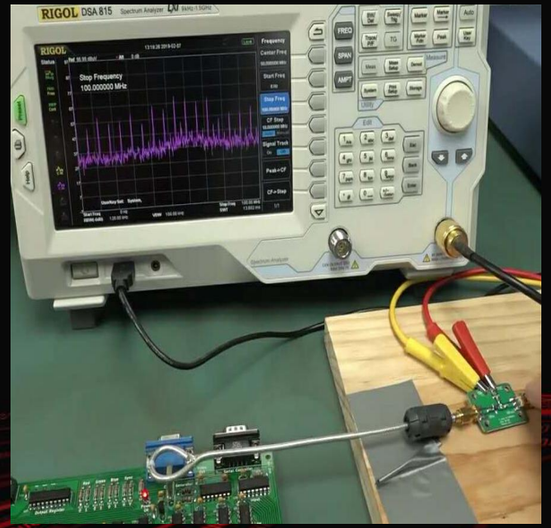
. 芯片01转换产生电磁波从空气中泄漏, 其中包含密钥指纹信息

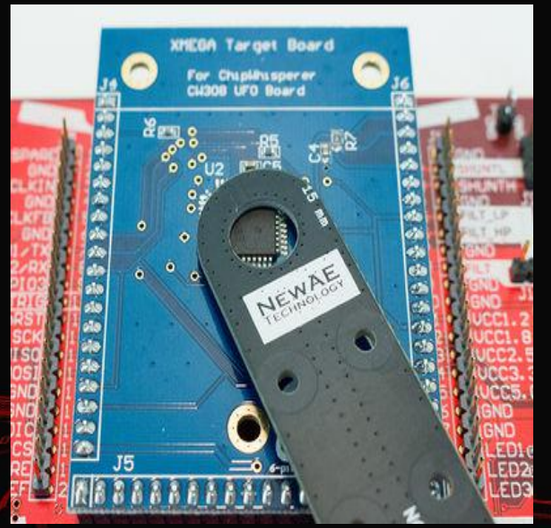
. Tel Aviv 大学科研人员通过测量分析电磁发射获取 GnuPG 密钥信息



功耗分析 (电磁信号)


RIGOL
Stop Frequency
1.000000000 GHz


RIGOL DSA 815
Stop Frequency
100.000000 MHz


XMEGA Target Board
For ChipWhisperer
CW308 UFO Board
NEWAE
TECHNOLOGY
J5

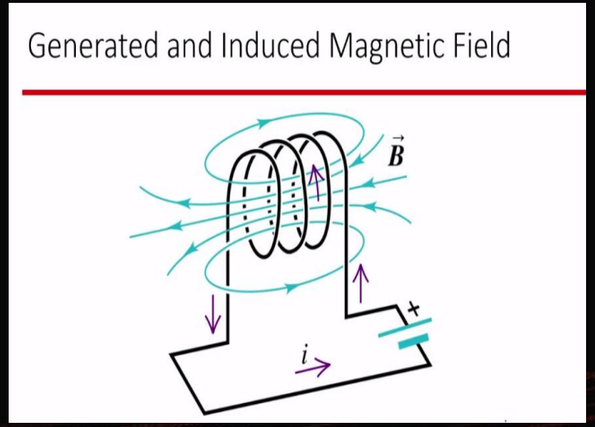
功耗分析 (DPA)

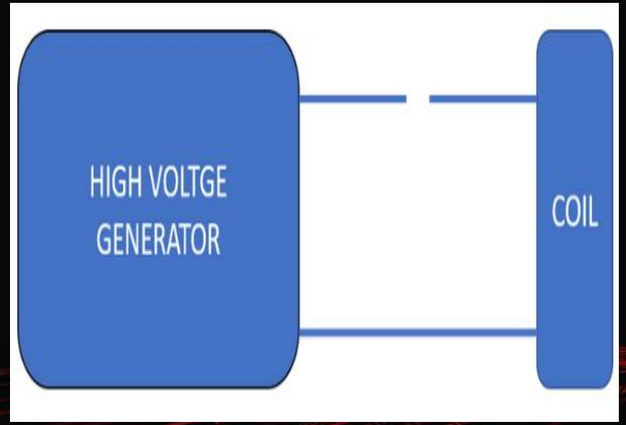
One More Thing ..

测信道 EMFI

```
#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;
}
```

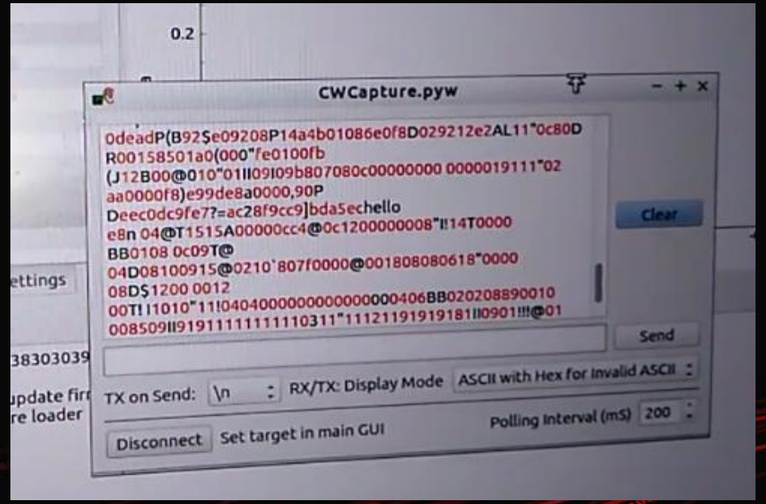
测信道 EMFI

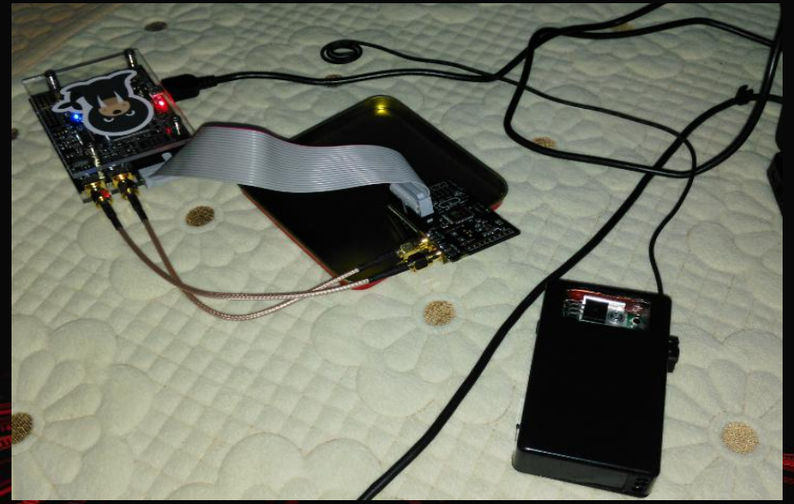

Generated and Induced Magnetic Field
$\vec{B}$
+
i


HIGH VOLTGE
GENERATOR
COIL

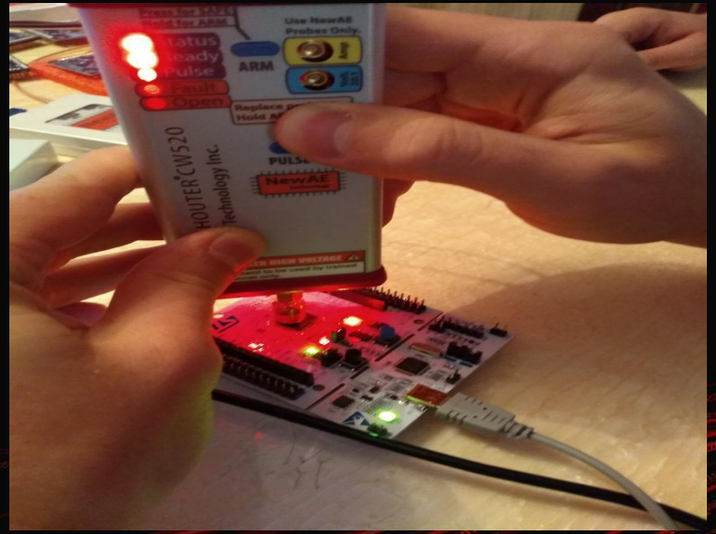
测信道 EMFI

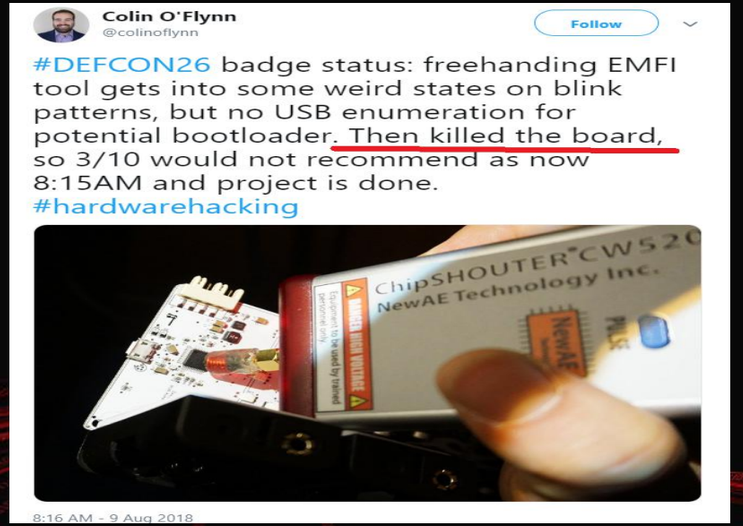
测信道 EMFI


0.2
CWCapture.pyw
0deadP(B92$e09208P14a4b01086e0f8D029212e2AL11"0c80D
R00158501a0(000"fe0100fb
(J12B00@010"01II09I09b807080c00000000 0000019111"02
aa0000f8)e99de8a0000,90P
Deec0dc9fe7?=ac28f9cc9]bda5echello
e8n 04@T1515A00000cc4@0c1200000008"!!14T0000
BB0108 0c09T@
04D08100915@0210`807f0000@001808080618"0000
08D$1200 0012
00T!!1010"11!040400000000000000406BB020208890010
008509II9191111111111310311"11121191919181II0901!!!@01
Clear
Send
TX on Send: \n
RX/TX: Display Mode
ASCII with Hex for Invalid ASCII
Disconnect
Set target in main GUI
Polling Interval (mS)
200



测信道 EMFI


ARM
NewAE
ChipSHOUTER CW520
NewAE Technology Inc.


Colin O'Flynn
@colinoflynn
Follow
#DEFCON26 badge status: freehanding EMFI tool gets into some weird states on blink patterns, but no USB enumeration for potential bootloader. Then killed the board, so 3/10 would not recommend as now 8:15AM and project is done.
#hardwarehacking
ChipSHOUTER CW520
NewAE Technology Inc.
8:16 AM - 9 Aug 2018

Summary

百分百安全的系统并不存在

边信道分析与防御, 硬件安全必备技能

完美的设计, 实施过程中百密一疏, 将导致系统完全崩溃

谢谢观看

演讲人：KEVIN2600