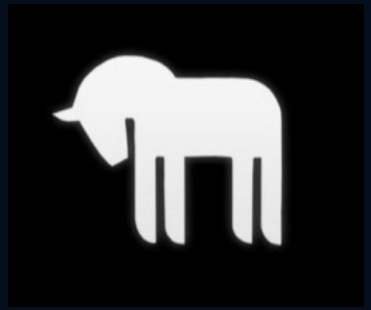
智能设备中的侧信道攻击面

李海粟 | 前重庆邮电大学信息安全协会副会长，卫星地面站站长

About me



- 重庆邮电大学 微电子科学与工程专业 大四
- 大二实习于奇虎360 Unicorn team
- 大三实习于北京智慧云测 DPLS Lab

主旨

FIT 2019

$$r = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \overline{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \overline{Y})^2}}.$$

$$\oint_{\partial V} \mathbf{E} \cdot d\mathbf{a} = \frac{Q_V}{\epsilon_0},$$

$$\oint_{\partial S} \mathbf{E} \cdot d\mathbf{l} = -\frac{d}{dt}\int_S \mathbf{B} \cdot d\mathbf{a},$$

$$\oint_{\partial V} \mathbf{B} \cdot d\mathbf{a} = 0,$$

$$\oint_{\partial S} \mathbf{B} \cdot d\mathbf{l} = \mu_0 I_S + \mu_0\epsilon_0\frac{d}{dt}\int_S \mathbf{E} \cdot d\mathbf{a}.$$

$$f(X) = \frac{exp[-\frac{1}{2} \cdot (x-m)' \cdot C^{-1} \cdot (x-m)]}{[(2\pi)^n \cdot det(C)]^{1/2}}$$

$$I(X;Y) = \sum_{y \in Y}\sum_{x \in X} p(x,y)\log\left(\frac{p(x,y)}{p(x)\,p(y)}\right)$$

主旨

推动侧信道安全在hack领域落地

目录

- 智能设备中的侧信道
- 软件攻击面和简单缓解
- Q&A

侧信道攻击

Side-channel attacks on high-security electronic safe locks

DEF CON 24

plore@tuta.io

错误注入攻击汽车电子

Fault injection on automotive diagnostic protocols

Bypassing the security of protected UDS implementations

Ramiro Pareja
Riscure Security Lab
pareja@riscure.com

Santiago Cordoba
Riscure Security Lab
cordobapellicer@riscure.com

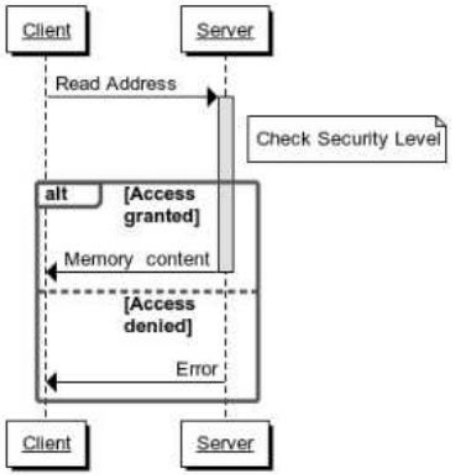
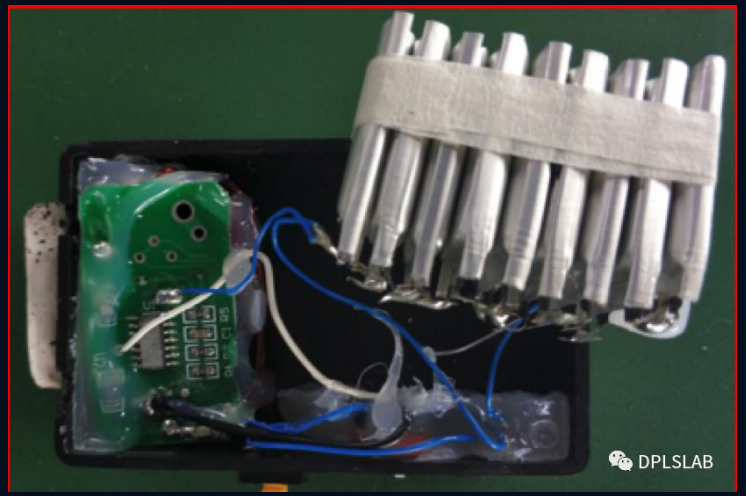
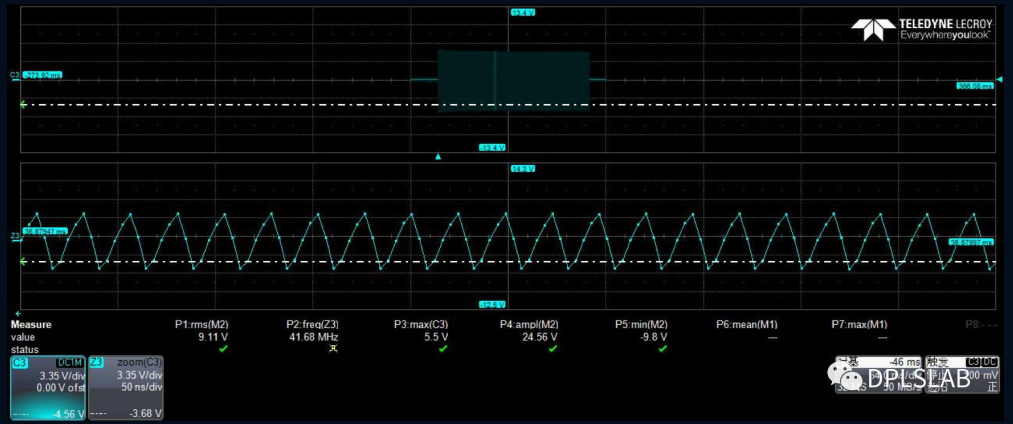


Figure 2: ReadMemoryByAddress flow

错误注入攻击智能门锁


DPLSLAB


TELEDYNE LECROY
Everywhereyoulook
Measure
value
status
P1:rms(M2)
9.11 V
P2:freq(Z3)
41.68 MHz
P3:max(C3)
5.5 V
P4:ampl(M2)
24.56 V
P5:min(M2)
-9.8 V
P6:mean(M1)
P7:max(M1)
3.35 V/div
0.00 V ofst
-4.56 V
3.35 V/div
50 ns/div
-3.68 V
DPLSLAB

侧信道攻击智能卡

FIT 2019

Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards

Junrong Liu[1], Yu Yu[1,2,3], François-Xavier Standaert[4], Zheng Guo[1,5], Dawu Gu[1], Wei Sun[1], Yijie Ge[1], and Xinjun Xie[6]

[1] School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China
Email: {liujr,yyuu,guozheng,dwgu,ruudvn}@sjtu.edu.cn
[2] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093)
[3] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China
[4] ICTEAM/ELEN/Crypto Group, Université catholique de Louvain, Belgium
Email: fstandae@uclouvain.be
[5] Shanghai Viewsource Information Science & Technology Co., Ltd
[6] Shanghai Modern General Recognition Technology Corporation

Breaking Korea Tansit Card with Side-Channel Analysis Attack - Unauthorized recharging -

Tae Won Kim[1,2], Tae Hyun Kim[1], and Seokhie Hong[2]

[1] SNTWORKS, Gyeonggi-do, South Korea
[2] Center for Information Security Technologies, Korea University, Seoul, South Korea

分析

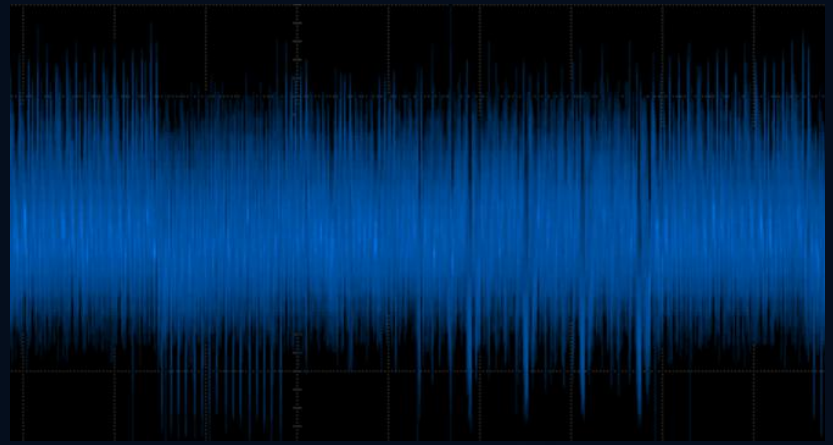
所有的攻击点都在 —— 鉴权

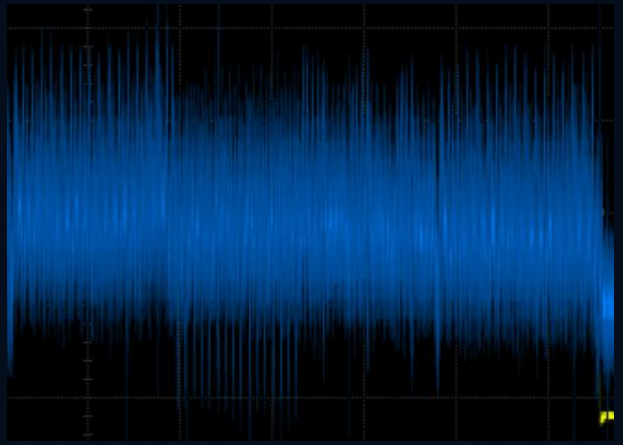
鉴权信息泄露，鉴权过程跳过，权限检查跳过

鉴权执行　　验证权限

密钥泄露

使用密码学算法的信息泄露





密钥泄露

硬件上 —— 使用安全IP算法核

软件上 —— 随机延时，掩码，伪轮

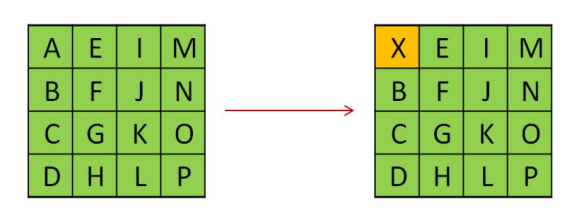
PIN码泄露

```
strcpy(str1, "abcdef");
strcpy(str2, "abbbbb");
strcpy(str3, "abcccc");
strcpy(str4, "abcddd");
ret1 = strcmp(str1, str2);
ret2 = strcmp(str1, str3);
ret3 = strcmp(str1, str4);
```

PIN码泄露防御

数据处理位置随机化，逻辑处理时间统一化，增加噪音

错误注入密码学算法



2X⊕3B⊕C⊕D	2E⊕3F⊕G⊕H	2I⊕
2B⊕3C⊕D⊕X	2F⊕3G⊕H⊕E	2J⊕
2C⊕3D⊕X⊕B	2G⊕3H⊕E⊕F	2K⊕
2D⊕3X⊕B⊕C	2H⊕3E⊕F⊕G	2L⊕

$S(2X⊕3B⊕C⊕D⊕K_{10,0}) ⊕K_{11,0}$
$S(2B⊕3C⊕D⊕X⊕K_{10,1}) ⊕K_{11,13}$
$S(2C⊕3D⊕X⊕B⊕K_{10,2}) ⊕K_{11,10}$
$S(2D⊕3X⊕B⊕C⊕K_{10,3}) ⊕K_{11,7}$

图片来自Riscure《Unboxing the White-Box —— Practical attacks against Obfuscated Ciphers》

注入不良编码

FIT 2019

不同状态的编码之间，汉明距离过近，通过错误注入导致状态的翻转。

特别关键的数据，使用纠错码或者保存多份。

注入不良编码

使用复杂多位的编码，关键状态表示和关键数据的传输不应使用布尔变量或简单高低电平表示。

0 -> 10101010

1 -> 01010101

注入默认状态

```
switch (state)
{
    case 1: exit(); break;
    case 2: exit(); break;
    case 3: exit(); break;
    case 4: exit(); break;
    default: pass();
}
```

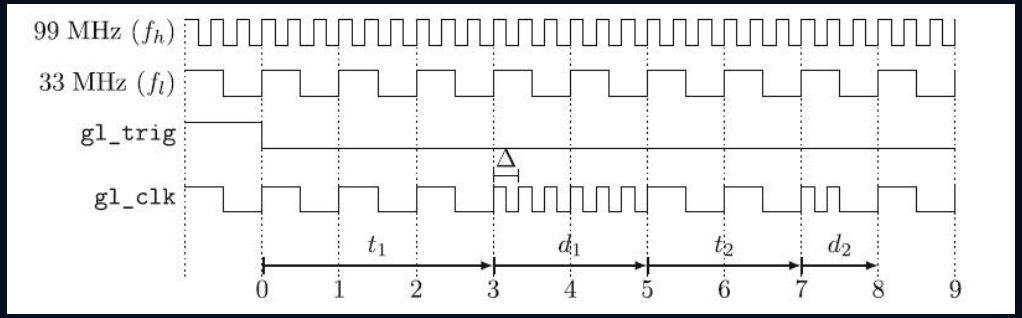
通过错误注入，使执行流进入默认状态，完成权限的提升。

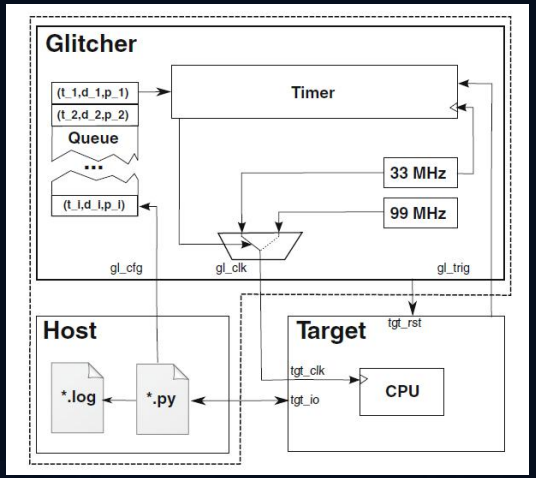
注入判断

通过错误注入，跳过某些语句的执行，更改判断结果，提升权限。

注入判断

时钟Glitch





引用自Why Cryptography Should Not Rely on Physical Attack Complexity by Juliane Krämer (Springer 2015)

注入判断

敏感操作应该使用

冗余校验

```
   103:          if (c==4657)
C:0x001B    E50D      MOV       A,0x0D
C:0x001D    B43109    CJNE      A,#0x31,C:0029
C:0x0020    E50C      MOV       A,0x0C
C:0x0022    B41204    CJNE      A,#0x12,C:0029
   104:          {
   105:              pass();
C:0x0025    120039    LCALL     pass(C:0039)
   106:          }
   107:          else
C:0x0028    22        RET
   108:          {
   109:              fail();
C:0x0029    12003A    LCALL     fail(C:003A)
   110:          }
C:0x002C    22        RET
```

防御总结

部分指令可以被跳过 → 冗余校验

部分Bit位可能被更改 → 冗余编码

主动感知

尾声

侧信道和错误注入的攻防，和所有的信息安全攻防一样，是一个螺旋上升的过程，防御方案要经过验证才是可信的。

侧信道和错误注入的防御，在金融和版权保护领域已经有很长时间的应用历史，可以借鉴。

Q&A

微博

未涉及内容

针对密码算法攻击的算法（CPA，模板攻击...）

能量轨迹处理（滤波，对齐，特征提取...）

.....


CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS
重慶郵電大學
1950

FREEBUF | FIT

THANKS