SWRhapsody

IOT

于4月 23, 2019由**SWRhapsody**发布

Introduction

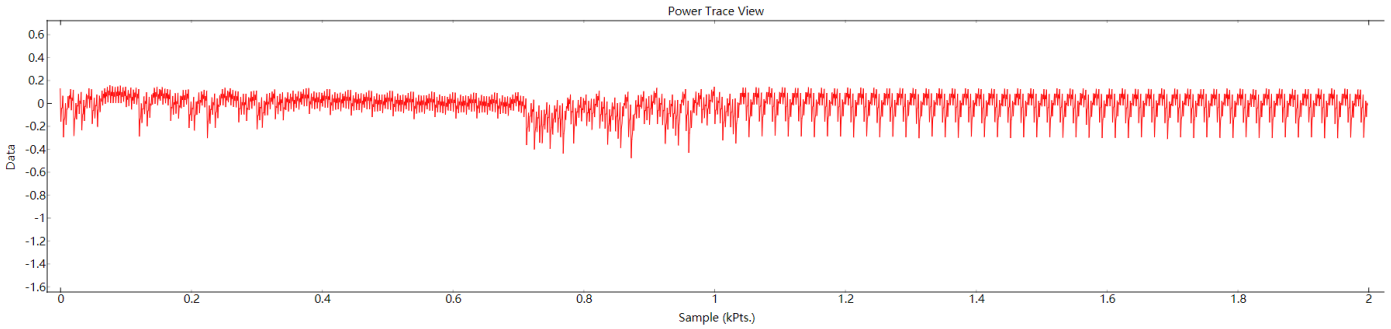
又有好久没有写博客了，英国这边课程还是挺头疼的，忙的时候作业多的要死。

这篇博客记录写IOT相关的知识，部分为课程的实验内容。

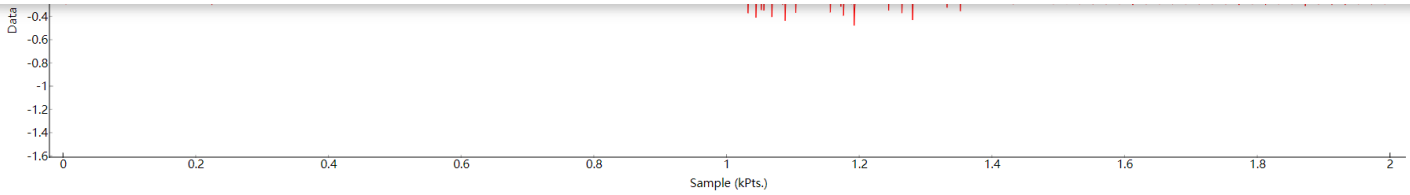
Correlation power attack

Correlation power attack（CPA）算是侧道攻击的一种，主要是同过设备在运算加密算法时不同的运算消耗的能量不一样来破解密钥的攻击。

下图是执行不同次数的乘法运算时的 power trace



运行10次乘法运算



运行20次乘法运算

可以明显的看到中间有一段乘法运算波形的重复。具体的攻击细节可以看 ChipWhisperer 的官方 wiki[1]，wiki 上的 tutorial 讲的比较详细这里就不细讲了。

mfoc

大体上和[2]没有区别，教你如何克隆一张保护不够完善的卡，部分国内的校园卡（水卡之类的）可以直接复制。试了一下，这边大部分在用的各种卡（公交卡这样的）扇区都有保护。

Replay attack

简单的重放攻击，使用 LimeSDR 和 Radio Hacker 一套的软件可以执行对无线车钥这类的攻击。如果使用 Rolling Code 保护稍微麻烦的，需要解码后分析。

Reference

[1] ChipWhisperer Wiki

[2] Cloning a MIFARE Classic 1k

分类: UNCATEGORIZED

0 条评论

SWRhapsody

名称 *

电子邮件 *

网站

在想些什么?

发表评论

近期文章

携程Apollo YAML 反序列化

CVE-2020-5410

CodeQL部分源码简读

服务器与网关的不一致

CodeQL 部分使用记录

近期评论

文章归档

2020年8月

SWRhapsody

分类目录

SWRhapsody

Uncategorized

相关文章

UNCATEGORIZED

WordPress Social Warfare XSS

Introduction Plugin name: Social Wa 阅读更多…

UNCATEGORIZED

自动化程序修复

Automatic patch generation Introduc 阅读更多…

UNCATEGORIZED

Criminology

Introduction 网络安全也要学习犯罪学了吗，每次写这类文章都 阅读更多…