



OPTIGA™ Trust M2 ID2

-- 安全易用的阿里Link ID²物联网安全通证与终端安全系统化解决方案

姚碧 2020.09.09



物联网 -- 构造世界的力量

- 预测到2025年全球物联网市场将有4万亿美元到11万亿美元的增长
- 预计2025年我国物联网连数近200亿个
- 2022年中国物联网市场规模将达到7500亿元



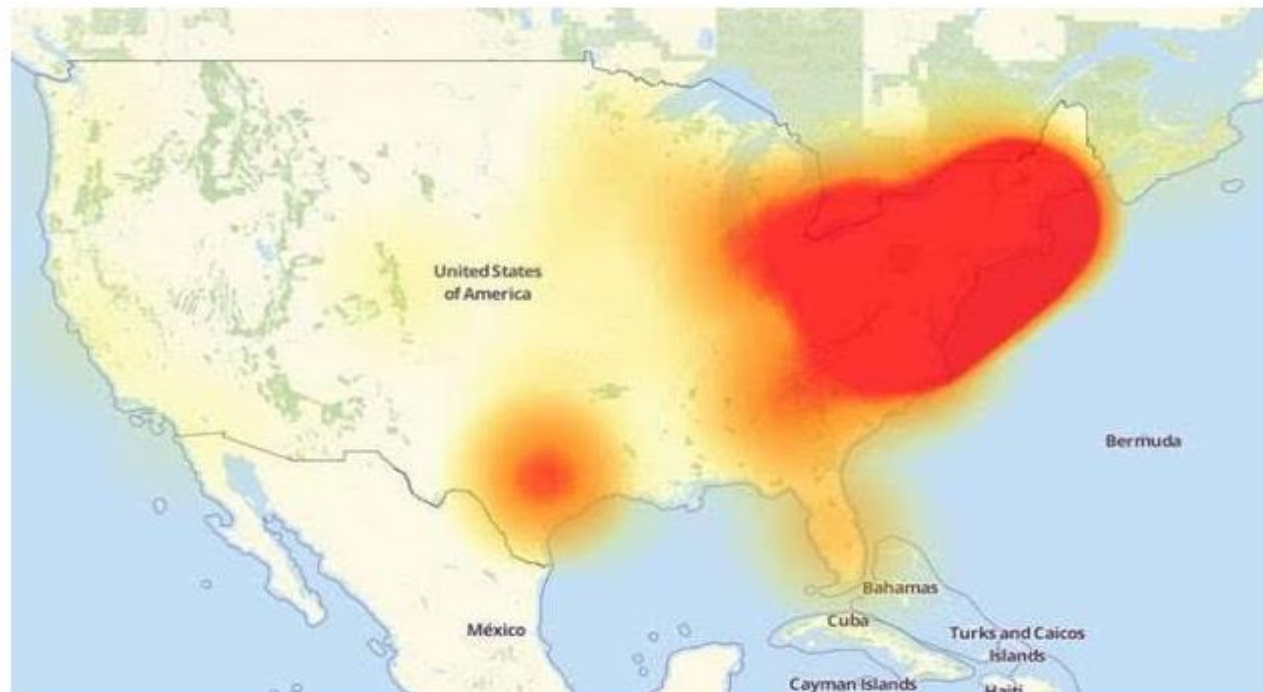
“这是一个最美好的时代，也是一个最糟糕的时代”

--狄更斯 《双城记》

大规模DDoS攻击导致美国东海岸网站集体宕机

2016-10-22 10:05

› 引用：
https://www.sohu.com/a/116847542_155403



北京时间10月22日凌晨消息，美国网站技术提供商Dyn宣布，该公司在当地时间周五早上遭遇了一次DDoS（分布式拒绝服务）攻击，从而导致许多网站在美国东海岸地区宕机，如Netflix、Twitter、Spotify和Reddit等。

“这是一个最美好的时代，也是一个最糟糕的时代”

--狄更斯 《双城记》

智能摄像头和自动调温器被入侵，房主不寒而栗

作者: Yinzi 星期五, 二月 15, 2019 0

当我走近婴儿房，我听见一个低沉的声音正在和他说话。

引用:

<https://www.aqniu.com/hack-geek/43693.html>



一位居住在巴林顿湖的房主表示，自从其家中家用监控摄像头和自动调温器被恶意黑客入侵，他已经有10天没有好好睡过觉了。

Arjun Sud表示：不敢相信这些在自己家安装，用来保护家人的设备，现在却反过来被别人利用来对付自己。

“这是一个最美好的时代，也是一个最糟糕的时代”

--狄更斯 《双城记》

智能网联汽车爆发在即 信息安全谁来保障？

2018-06-28 18:55:44 新浪汽车

A⁻ | A⁺ | ☆

“ 尽管智能网联汽车市场巨大、爆发在即，一个真实存的问题——智能汽车信息安全却没有引起足够的重视。360智能网联汽车安全实验室负责人刘健皓在接受新浪汽车采访时表示，这关乎到汽车制造商的品牌问题，一旦信息泄露或者车辆被攻击，将是对品牌致命的打击，建议各大车企应该尽早做相应的投入。 ”

› 引用：

<http://auto.sina.com.cn/news/hy/2018-06-28/detail-iheqpwwqy3260381.shtml>





物联网将为全球经济带来巨大的价值，
但这种商业潜力必须与**安全**相伴而生

安全方案的实现方式



没有安全

所有内容开放给所有人

可读性

可复制

可分析

信任根



基于软件实现的安全

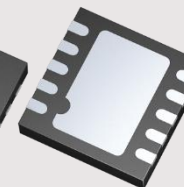
防御逻辑通道上的非法访问及
减少软件自身漏洞所带来的风险

易于访问与读取

易于复制与篡改

易于分析与理解

无法做到可信任的根



基于硬件的安全

防御针对硬件的攻击
以及高强度的软件攻击

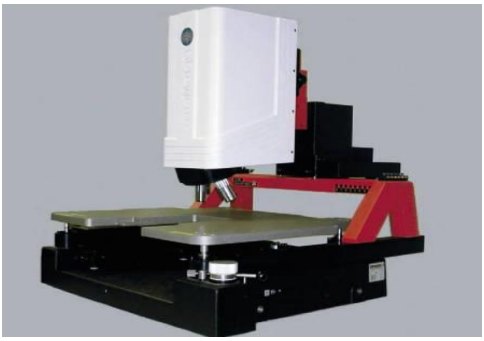
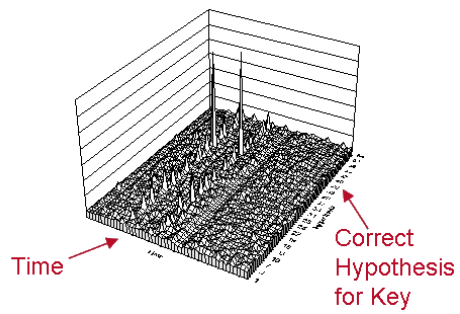
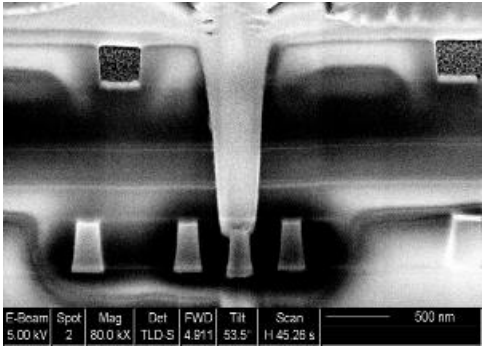
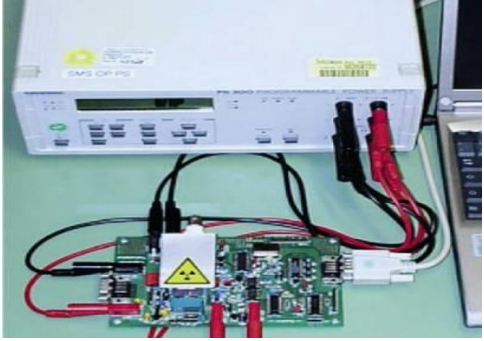
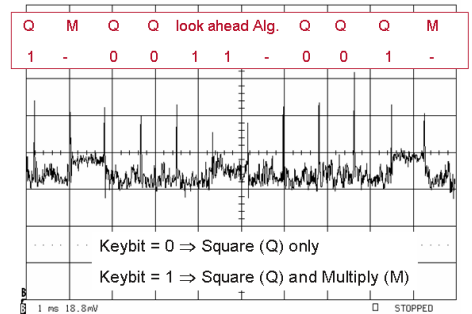
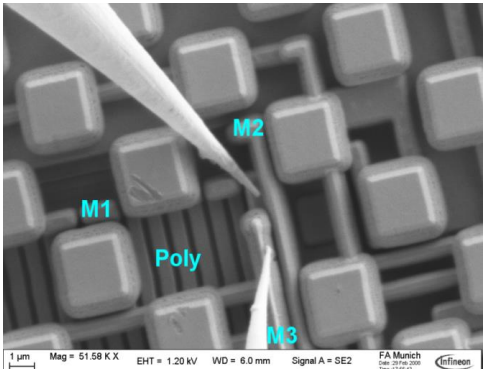
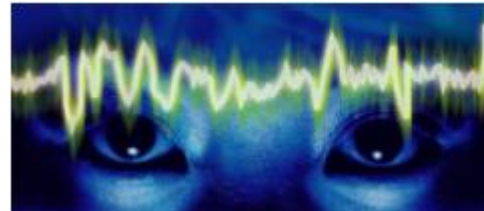
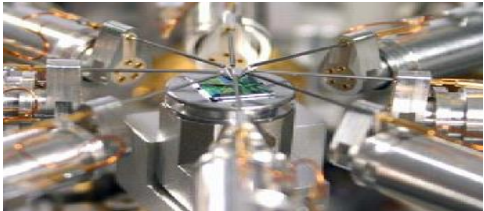
硬件逻辑保护自身代码不被读取

即便通过反向工程也无法轻易的被复制

专用的设计以及非标准的代码实现，
难于分析与理解

为系统提供可信任根

针对硬件攻击的三种类型

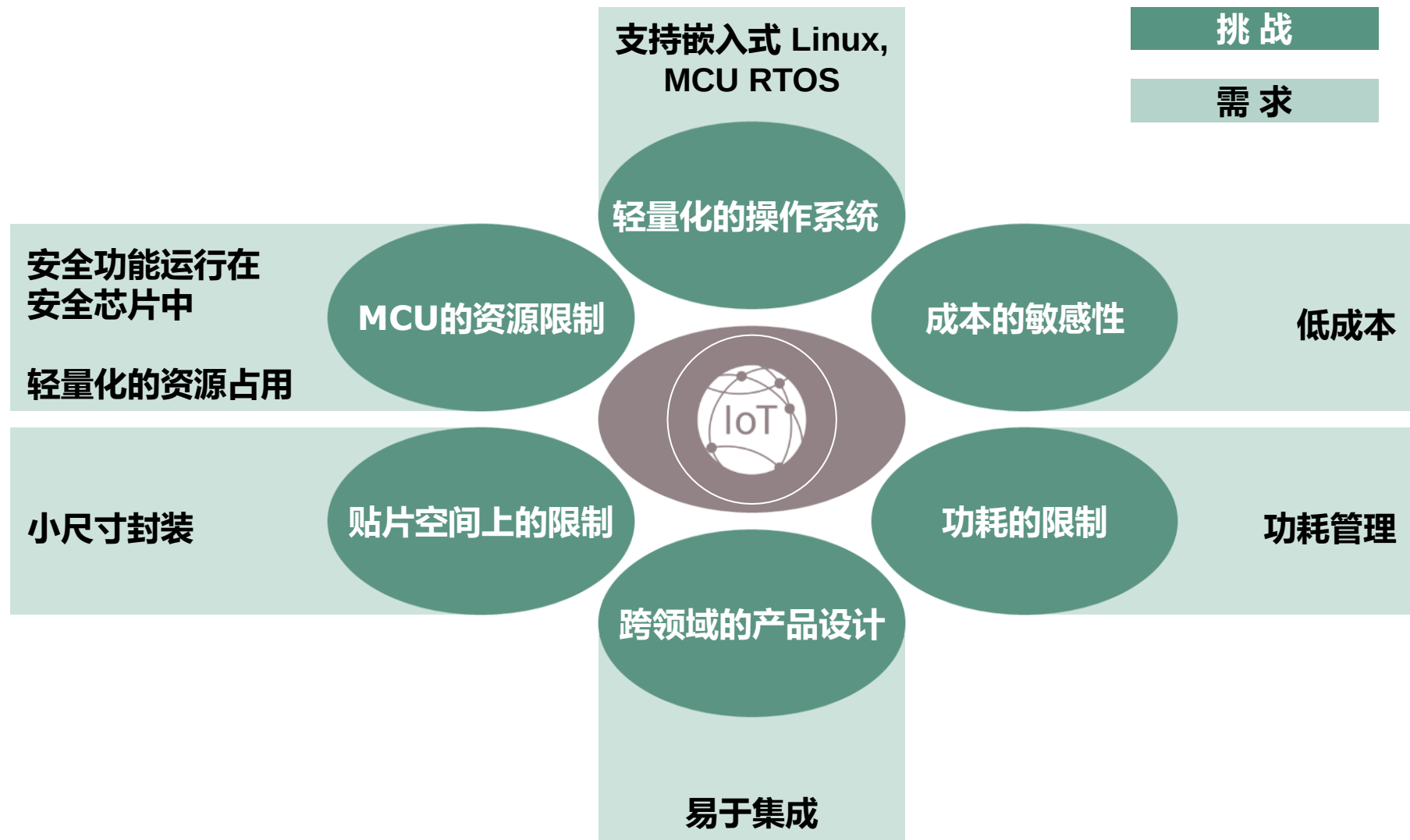


侵入式攻击

非侵入式攻击

半侵入式攻击

物联网设备设计面临的挑战与需求



OPTIGA™ Trust M2 ID2为物联网安全量身定制

易于开发

- › 完整交钥匙式的解决方案
- › 客户定制化证书烧录
- › 基于硬件抽象层架构的主端C源码包
- › 完善的评估工具

优异的安全特性

- › 基于 CC EAL 6+ (high) 认证的
安全控制器
- › 支持X.509 证书
- › 符合AIS-31认证标准的真随机数
发生器 (TRNG)
- › OPTIGA™ Shielded Connection
加密的通讯接口
- › CA 证书动态更新

灵活好用的扩展工具包

- › iTLS/iDTLS
- › 可开发者自定义的安全解决方案

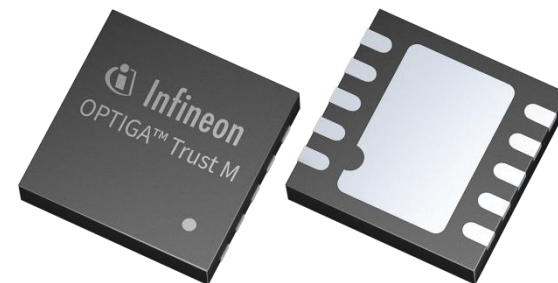
广泛的应用场景

- › 阿里Link ID²物联网安全通证
- › iTLS/iDTLS安全通信
- › 数据安全存储
- › 生命周期管理
- › 功耗管理
- › 固件安全更新
- › 平台完整性校验



产品主要参数

温度范围	-40 to +105°C	通讯接口	I2C
数据存储空间	10kB	接口速率	1 Mbit/sec
加解密算法	RSA, AES, SHA	封装	USON-10
量产时间	2020年	尺寸	3 x 3 mm



ICA安全评定证书

证书编号: IoT-A-Func-00013


IoT 合作伙伴计划

ICA 安全合规评定证书

单位名称
英飞凌科技(中国)有限公司

产品型号
OPTIGA™ Trust M2 ID2

依据标准
《ID2 安全应用指令规范V1.1》

检测工具版本
id_test_suite_v1.0

上述产品符合ICA联盟安全标准，特发此证，以兹证明。

理事长 

颁发机构: 杭州云谷物联网标准发展中心

发证日期: 2020年2月13日 有效期至: 2022年2月12日

证书编号: IoT-A-Cert-00012


IoT Connectivity Alliance

ICA 载体安全等级评定证书

单位名称
英飞凌科技(中国)有限公司

产品型号
OPTIGA Trust M2 ID2

依据标准
《ICA/T 2019-210-02 IoT 载体安全分级体系规范》

评定等级
Level 3

上述产品符合ICA联盟安全标准，特发此证，以兹证明。

理事长 

颁发机构: 杭州云谷物联网标准发展中心

发证日期: 2020年7月3日 有效期至: 2022年7月2日

OPTIGA™ Trust M2 ID2 为客户带来多元化的效益



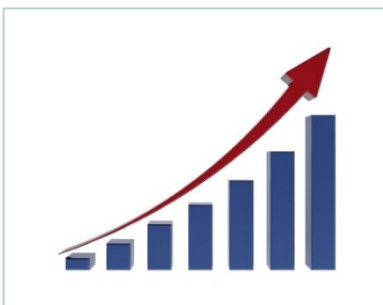
安全

最适合物联网设备的安全解决方案，保护您的业务以及您的客户的数据与权益



经济

易于集成与访问的终端系统安全解决方案，减少了您产品设计与运维的投入，并加快了产品投入市场的时间



差异化

保障您的产品在新的功能和新的商业模式上做到差异化，在竞争中保持领先并实现增长



Part of your life. Part of tomorrow.