arm

推动物联网长远发展，安全至关重要

Chet Babla
新兴业务集团副总裁

ARM HOLDINGS是SoftBank的子公司

Arm-全球机遇的缔造者

可授权的半导体技术研发全球领导者

专注于自由灵活的创新产品

基于文化且共享成功的业务模式的合作伙伴关系

70%

的全球人口使用Arm技术

1000 +

Arm生态系统合作伙伴

1300亿+

截至目前已装运的Arm架构芯片

arm

历次计算机技术浪潮

第一次浪潮 | 主机

第二次浪潮 | 个人计算机与软件

第三次浪潮 | 互联网

第四次浪潮 | 移动和云

arm

第五次计算机技术浪潮
数据驱动的时代

产生数据

传输数据

处理数据

1万亿台设备互联的机会

arm

物联网通过数字化转型实现价值

生产力提升 – 自动化、传感器驱动的洞察、智能制造

新业务模式 – 从“产品销售”模式向“一切即服务”营收模式的转变

客户体验提升 – 获取实时数据，获得灵活支持

截止2025年，全球将产生11万亿美元的经济价值*

*McKinsey Global Institute，2017年

arm

错综复杂的物联网
需要端对端安全

连接

配置

管理

开发设备

数据是否值得信赖？
我的应用是否有漏洞？
我的业务是否有漏洞？

安全

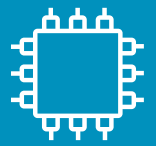
arm

确保物联网设备安全
安全性等不及亡羊补牢

分析
威胁建模

设计
硬件与固件设计规格

实施
固件源代码



验证
独立测试

需要分析的安全性威胁

物理攻击

- 非侵入式
- 侵入式

软件攻击

- 缓冲区溢出
- 中断
- 恶意软件

通讯攻击

- 中间人攻击
- 弱RNG
- 代码漏洞

生命周期攻击

- 代码降级
- 所有权变动
- 未经授权的生产过剩
- 深入调试

arm

基本设备安全目标

安全存储

认证

安全启动

唯一
实例ID

信任基隔离

TRNG
服务

安全更新流程

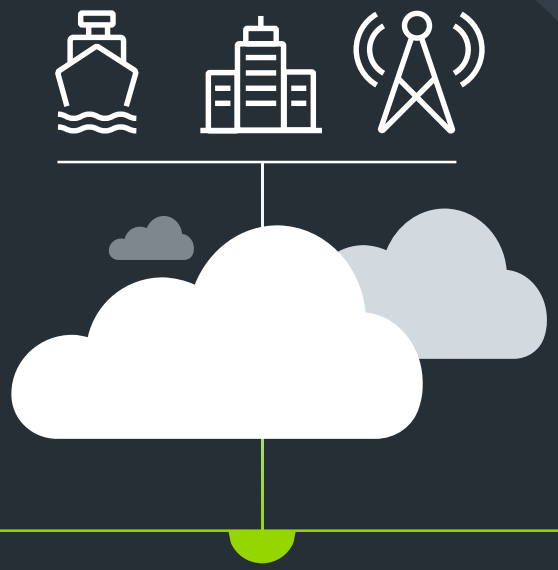
安全性生命周期

验证更新

防回滚功能

arm

平台安全架构（PSA）
开放安全框架与认证计划



psacertified™

www.psacertified.org

arm PSA

建立可信的设备与数据

arm

PSA方法示例–智能计量

过程流

系统描述

↓

资产

↓

威胁

↓

安全性目标

↓

安全性要求

产出

资产：计量数据的完整性和保密性

↓

威胁：远程SW攻击

↓

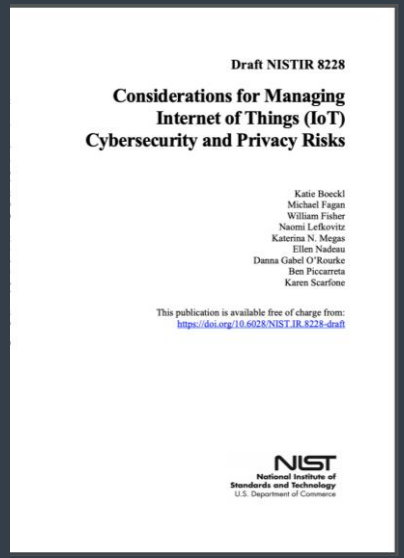
安全性目标：强加密

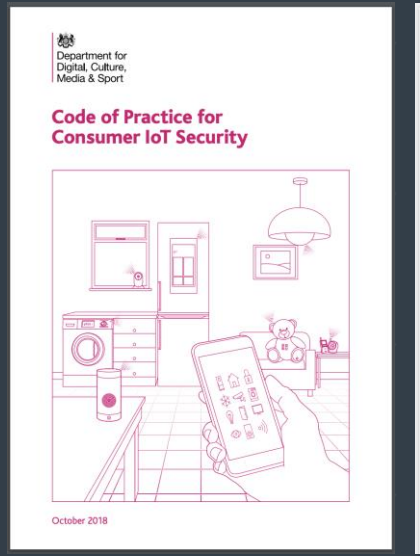
↓

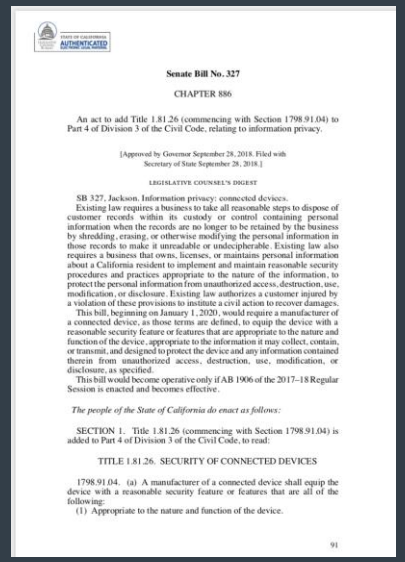
安全性要求：基于硬件的密钥存储

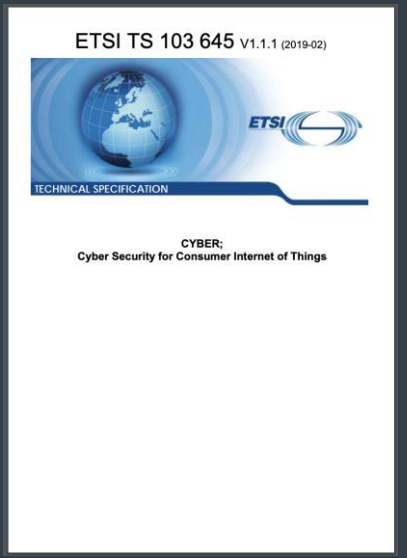
arm

政府与行业组织正逐渐认识到物联网安全威胁









美国：NIST　英国：DCMS　美国：加利福尼亚州　欧盟：ENISA　ETSI　GSMA

arm

物联网必须实现端对端安全

安全性取决于最薄弱的环节

设备到数据的安全性

arm

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה