2017中国车联网安全论坛

联网汽车：构建从芯到云的安全

Connected Cars: Build A Chain of Trust from Chip to Cloud

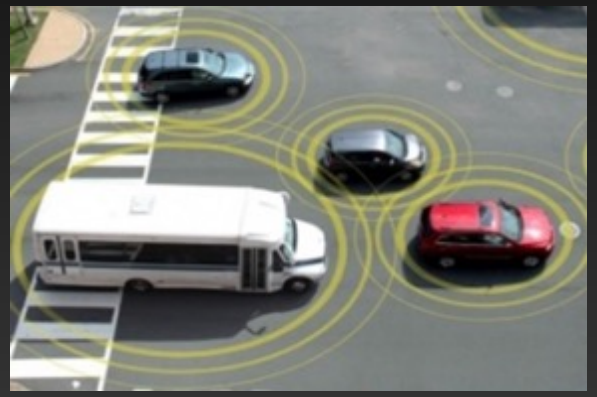
樊俊锋
fan@opsefy.com

深圳市纽创信安科技开发有限公司

Open Security Research (OSR)

目录

“万物互联”

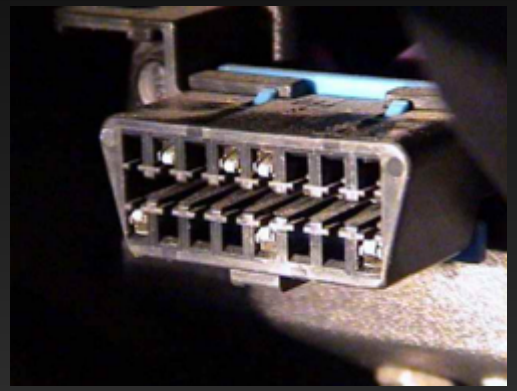


1.1 物联网攻击

- 大规模监控摄像头攻击（**2015**、**2016**）
  - 海康威视、大华、雄迈
- 远程汽车攻击（**2015**、**2016**、**2017**）
  - Jeep、比亚迪、特斯拉
- 智能家居设备攻击（**2010**至今）
  - 门锁、豆浆机、空调、冰箱、自动窗帘
- 基础设施攻击（**2014**至今）
  - 电网、港口
- 工业控制设备攻击（**2013**、**2015**）

1.2 车联网攻击

- 接触式攻击
  - OBD-II
  - 娱乐系统
    - CD/USB/iPod
- 近场攻击
  - 蓝牙
  - Keyless
  - TPMS
  - Wifi
- 网络攻击
  - GPS
  - GSM/3G/4G



1.3 攻击流程

For every 1000 lines of code,
1 to 5 bugs are introduced.
- Peiter Zatko @ Blackhat 2011

Peiter Zatko
Security analysis,
DARPA

1.4 脆弱点

- 弱登陆认证
- 固件未签名
- 固件未加密
- 密钥未保护
- 随机数质量差
- 芯片测试接口未保护
- 使用“自己设计”的密码协议
- 假定“设备处在安全网络中”
- 软件本身漏洞（版本、配置等）
- 网络端口配置漏洞
- 没有正确使用数字证书
- 手机端APP安全
- 管理平台（云）被拖库

目录

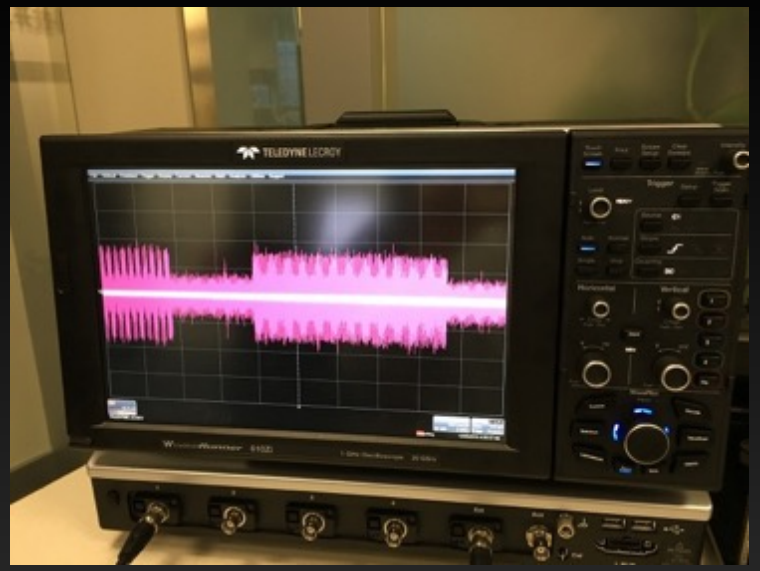
2.1 安全芯片

- “认证驱动”的高安全芯片
  - 智能卡
  - 身份证（电子护照）
  - 移动支付

- “黑客驱动”的高安全芯片
  - 品牌保护
  - 内容保护
  - 防抄板

2.2 物理攻击

- **特点：** ***“If you can’t break it with mathematics, try physics.”***
- **攻击目标**
  - 获得敏感信息
  - 伪造签名
  - 复制芯片
  - 获得更高权限
  - 修改关键数据
  - 破坏系统



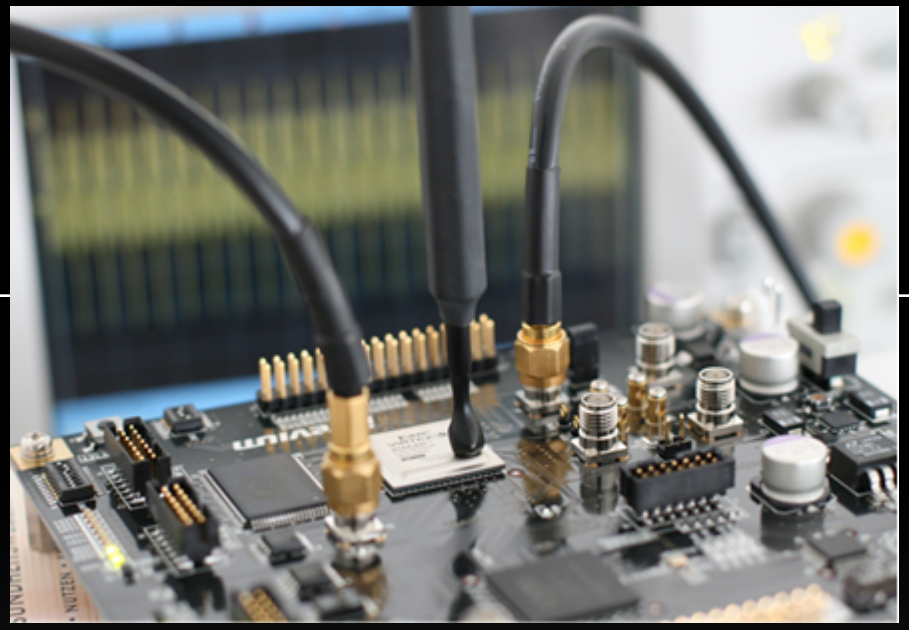
2.3 侧信道攻击

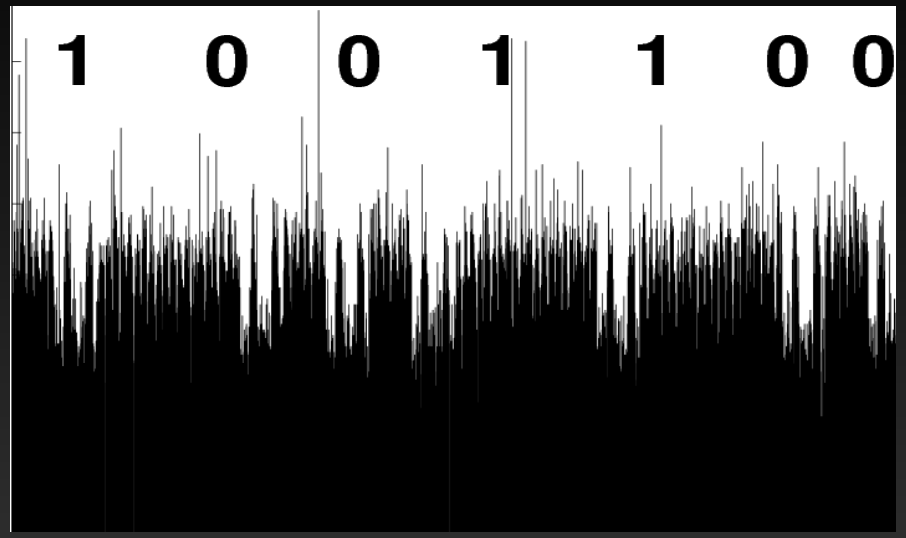
❑能量分析原理 - **Simple Power Analysis**

椭圆曲线按位扫描二进制点乘算法

$k = (k_{l-1}, k_{l-2}, \ldots, k_0)$
R ← O,

for $i=l-1$ downto 0 do
    R ← [2]**R**
    if $k_i = 1$ then
        R ← **R** + **P**
    end if
end for



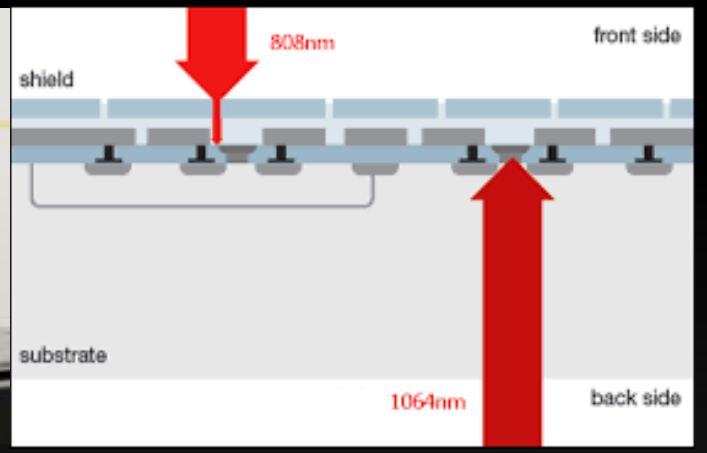


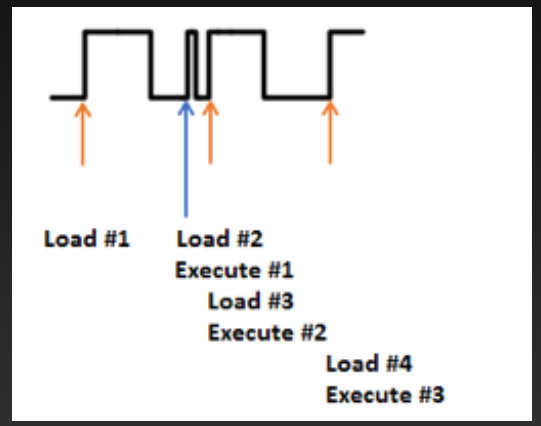
二进制点乘功耗曲线

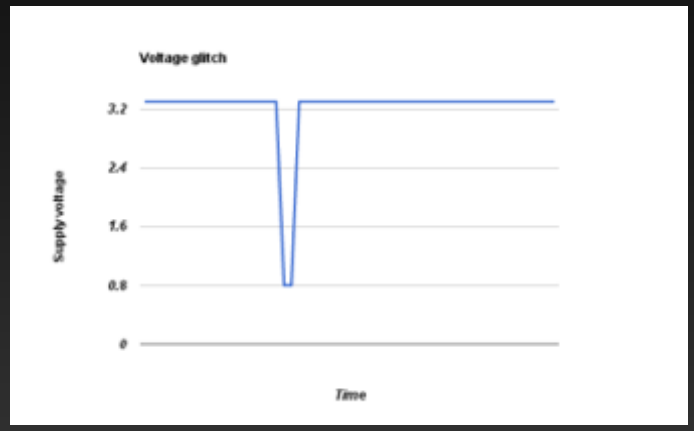
2.4 故障注入攻击

❑故障攻击

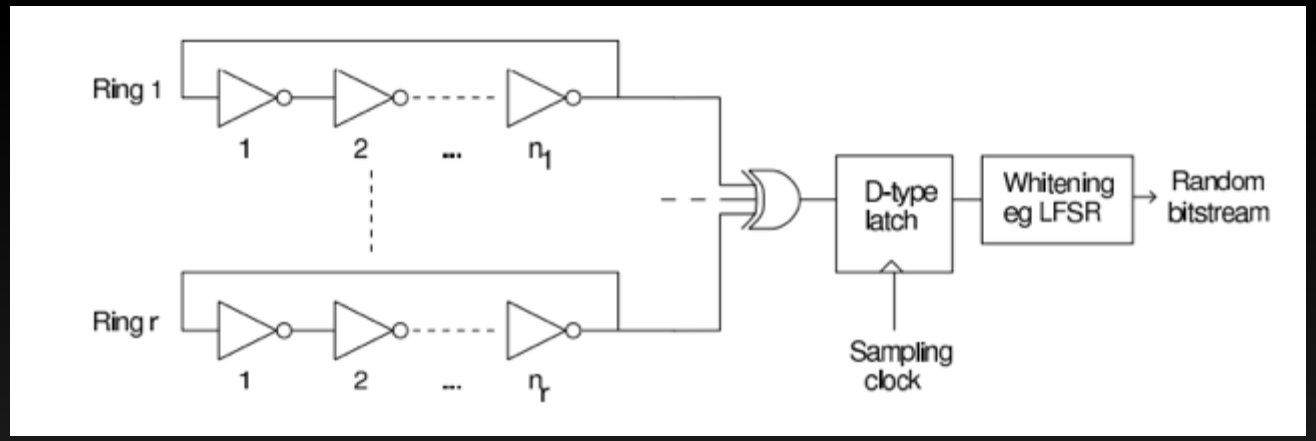
- 在芯片运行时注入故障，通过分析错误结果获得密钥
  - 电压毛刺、时钟毛刺、高低温
  - 激光、电磁场、射线
  - 对公钥、对称密码体制都有效

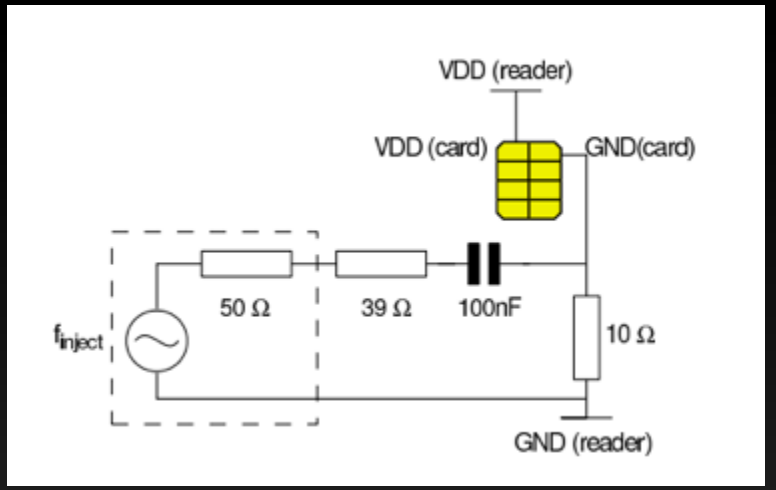


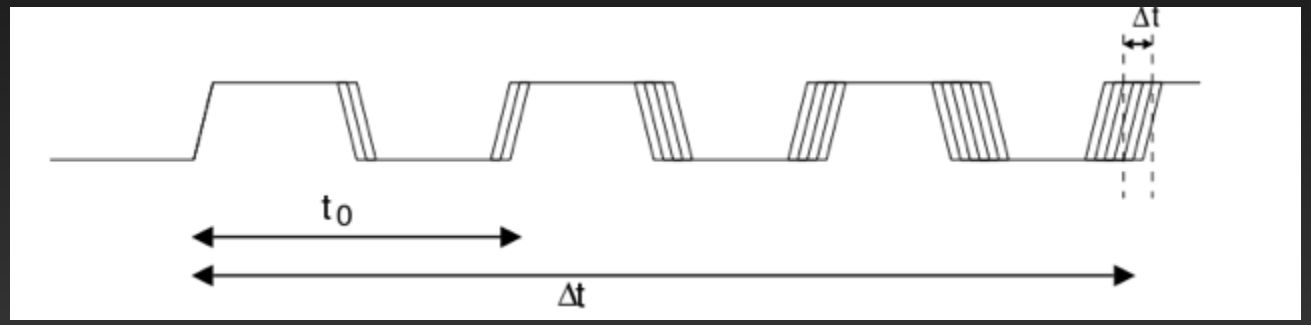


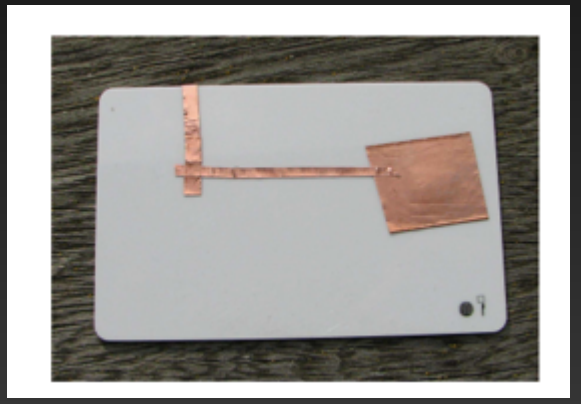


2.5 随机数发生器攻击


Ring 1
1
2
...
n_1
Ring r
1
2
...
n_r
D-type latch
Whitening eg LFSR
Random bitstream
Sampling clock


VDD (reader)
VDD (card)
GND(card)
50 Ω
39 Ω
100nF
10 Ω
f_{inject}
GND (reader)


Δt
t_0
Δt

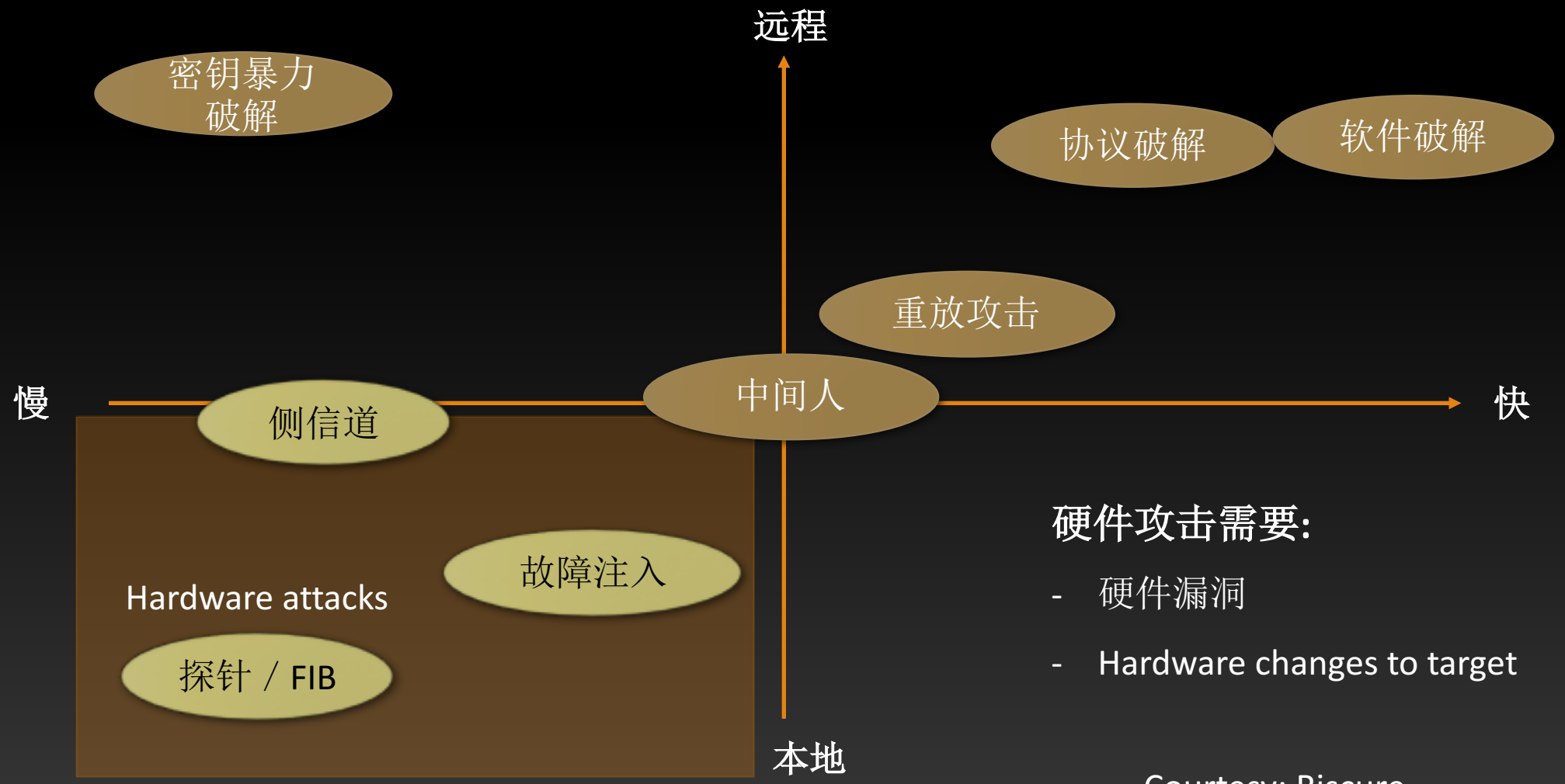


2.6 物理攻击案例

2.7 “安全芯片”城堡

- 侧信道攻击防护
  - Random masking, secure PKC algorithms, power decoupling, noise generations, random clock, secure sensors, etc.
- 故障攻击防护
  - Redundant logics, redundant execution, fault detection sensors, etc.
- 侵入式攻击防护
  - Active shield, memory encryption, bus scrambling, glue logic, etc.
- 随机数防护
  - Ture entropy source, health test, DRBG with strong crypto, etc.

2.8 软件 VS 硬件攻击

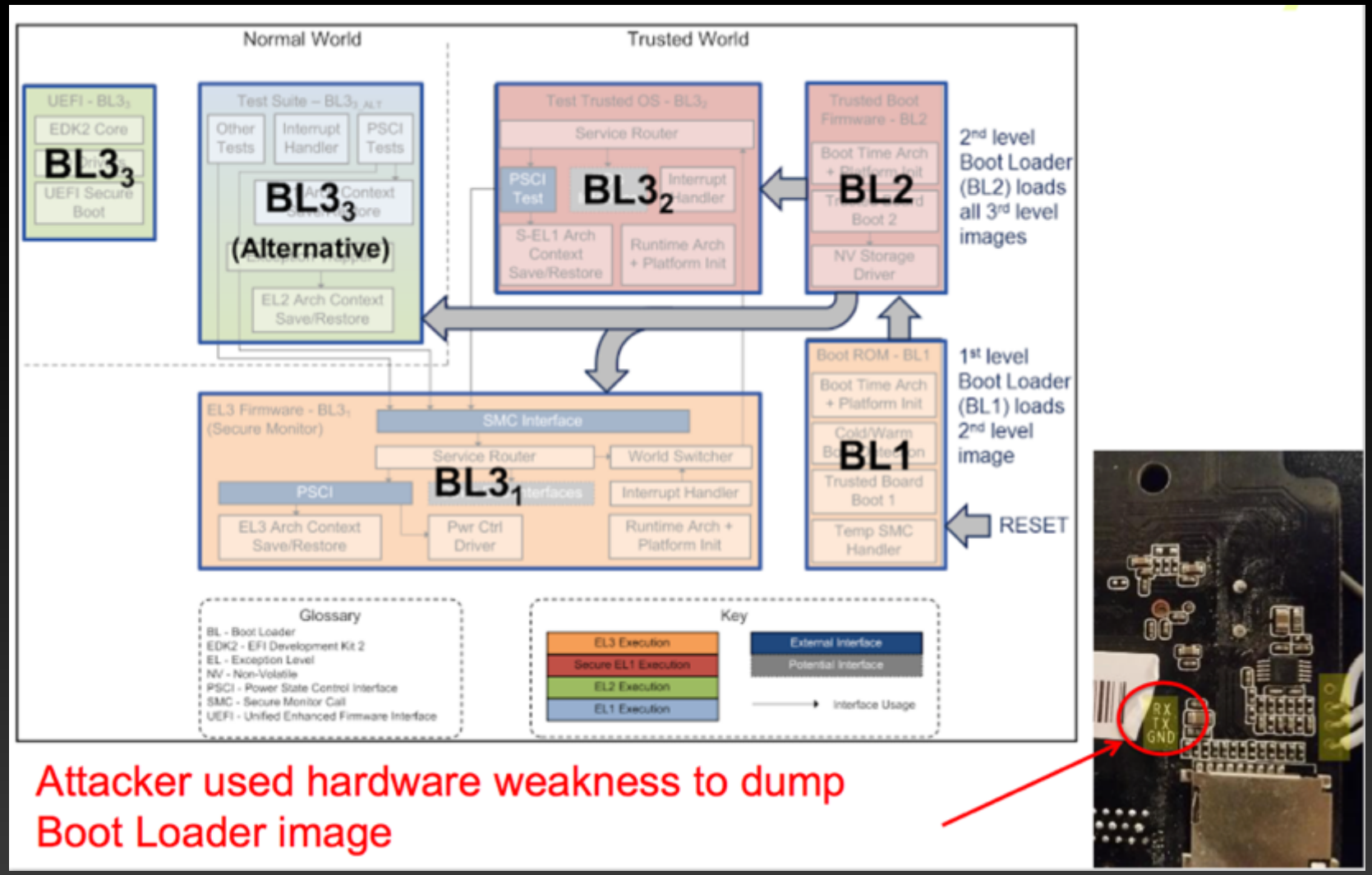


硬件攻击需要:

- 硬件漏洞
- Hardware changes to target

Courtesy: Riscure

2.9 SecureBoot攻击



slide courtesy: Riscure

目录

3.1 为什么需要安全硬件？

- 产生真随机数
- 保存密钥和证书
- 安全密码运算（加密、解密、签名、验签等）
- 固件保护
- 数据保护
- 安全升级（OTA）

3.2 生命周期安全

Registration
Identification
Payment

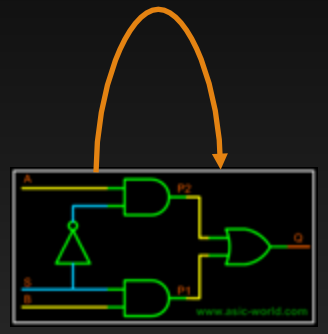
Boot ROM

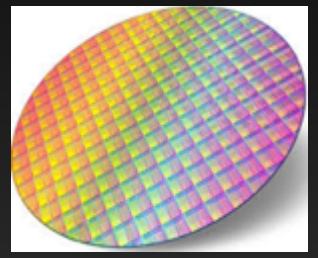
RootKey

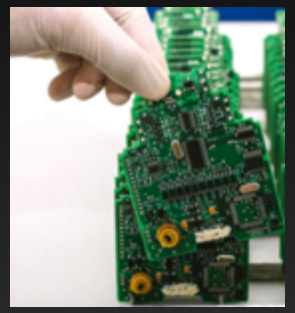
Firmware

Firmware
Update

Commands
& reports







Commands

Design House

Foundry &
Testing

PCB Factory

IoT Product

Final User

3.3 纯软件方案

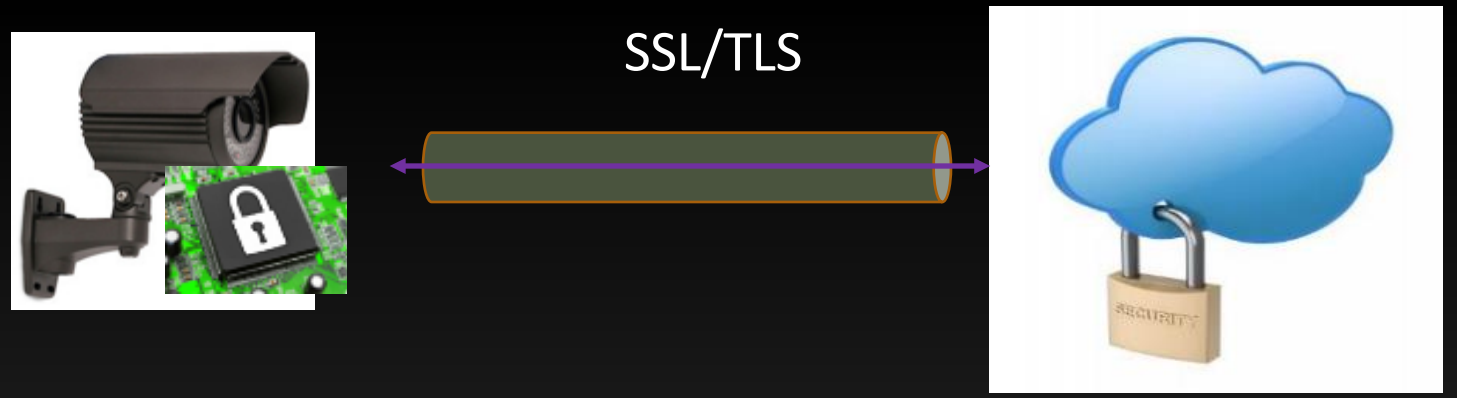
方案：MCU安装SSL

SSL/TLS

脆弱点1	随机数质量较差
脆弱点2	密钥的产生、存储和使用不安全（物理攻击）
脆弱点3	固件安全无法保证，没有灾难恢复机制

3.4 SE方案

方案：MCU＋SE



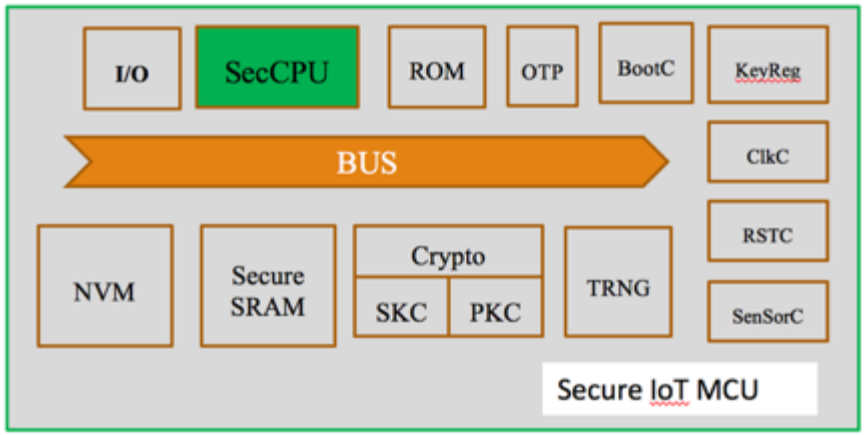
脆弱点1　固件和数据安全：难以抵御物理攻击

优点1　密钥的产生、存储和使用得到保护（物理攻击）

优点2　身份认证安全得到保护

3.5 安全MCU方案

方案：高安全MCU



SSL/TLS

优点1 固件和数据安全

优点2 密钥的产生、存储和使用得到保护（物理攻击）

优点3 身份认证安全得到保护

3.6 安全目标

- 安全固件(加密/签名)
- 安全秘钥存储
- 端到端加密
- 强用户认证
- 安全存储
- 设备唯一识别
- 灾难恢复

3.7 安全测评

关于纽创信安（OSR）

- “一个信息安全企业”
  - 成立于2014年末，团队20+人，坐标深圳 / 北京；
- 客户 & 合作伙伴
  - 华为、国家电网、阿里巴巴、比特大陆、奥联、汇顶、中天、艾派克等
- 产品 & 服务
  - IP和方案： 密码算法IP设计、系统安全方案设计
  - 安全测评：密码芯片、TEE、物联网、车联网安全测评

联系我们

- 地址： 深圳市南山区科技南十二路11号
  方大大厦1202
- 网站： www.opsefy.com
- 电话： +86 755 8695 0263