



构建基于密码芯片的物联网安全体系

Secure IoT architecture based on cryptographic hardware

樊俊锋

深圳市纽创信安科技发展有限公司
(Open Security Research, Inc.)

摘要

- IoT黑客长什么样？
- IoT设备有哪些脆弱性？
- 怎样提升IoT安全性？
- 密码芯片能贡献什么？

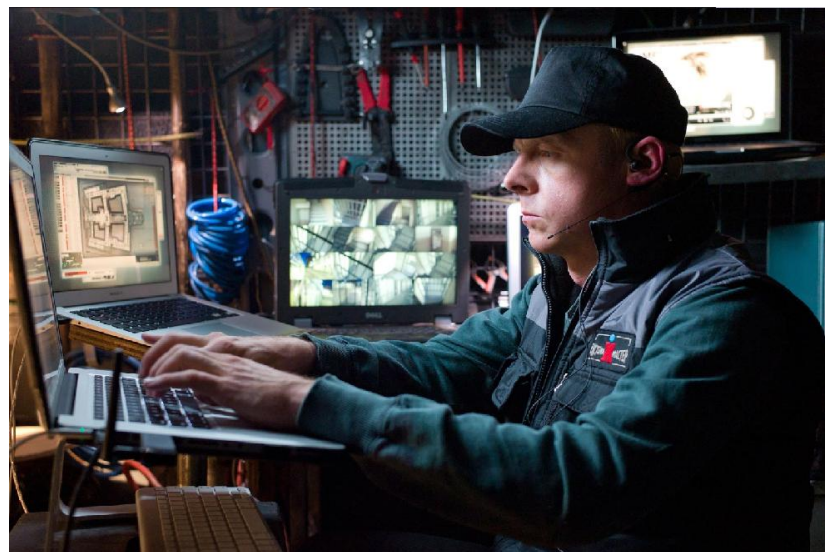
□ 网络黑客.....在地球的另一端



□ 近场黑客.....邻居、路人甲或面包车



□ 上天入地无所不能的入室型黑客

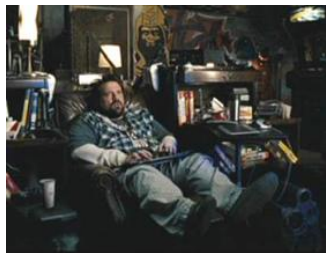


□ 用户型黑客



威胁程度 - 对用户而言

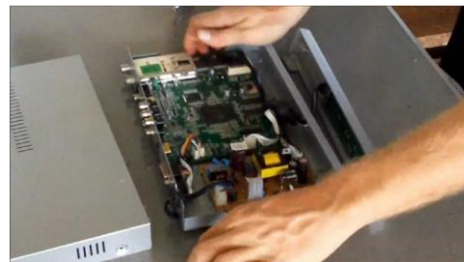
网络黑客



入室黑客



用户黑客



近场黑客

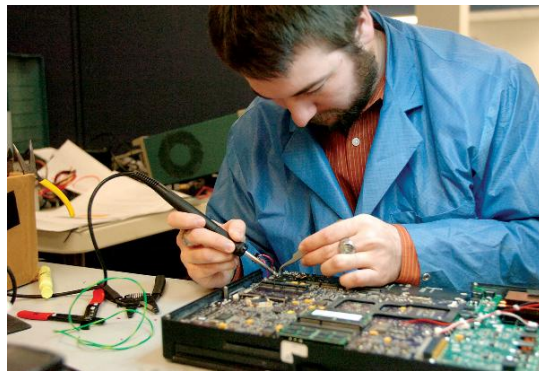


威胁程度 - 对产品企业而言

软件攻击



硬件攻击



.....除非，硬件Hack可以被低成本复制.....

案例-1: Nest温控器

□ “Smart Nest Thermostat: A Smart Spy in Your Home”, Blackhat 2014



Device Programming

- ROM is capable of booting device to boot from USB!
- Boot configuration pins are set by Nest hardware
- Device will boot from USB if sys_boot[5] is high
- Circuit board exposes sys_boot[5] on an unpopulated header...

black hat
USA 2014

案例-2: ZigBee系统

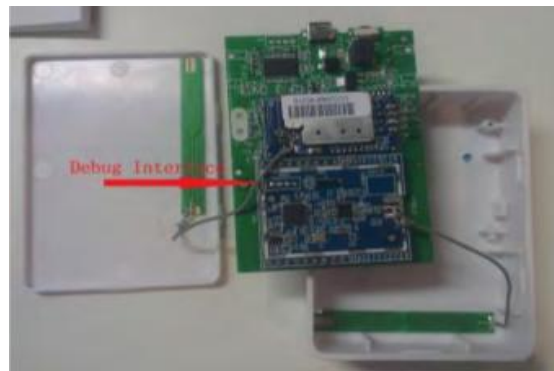
□ “I’M A NEWBIE YET I CAN HACK ZIGBEE”, Defcon 2015



Zigbee Bulb



Gateway



案例-3: 酒店门锁

- ❑ “My Arduino can beat up your hotel room lock” ,
Blackhat 2012



Open command

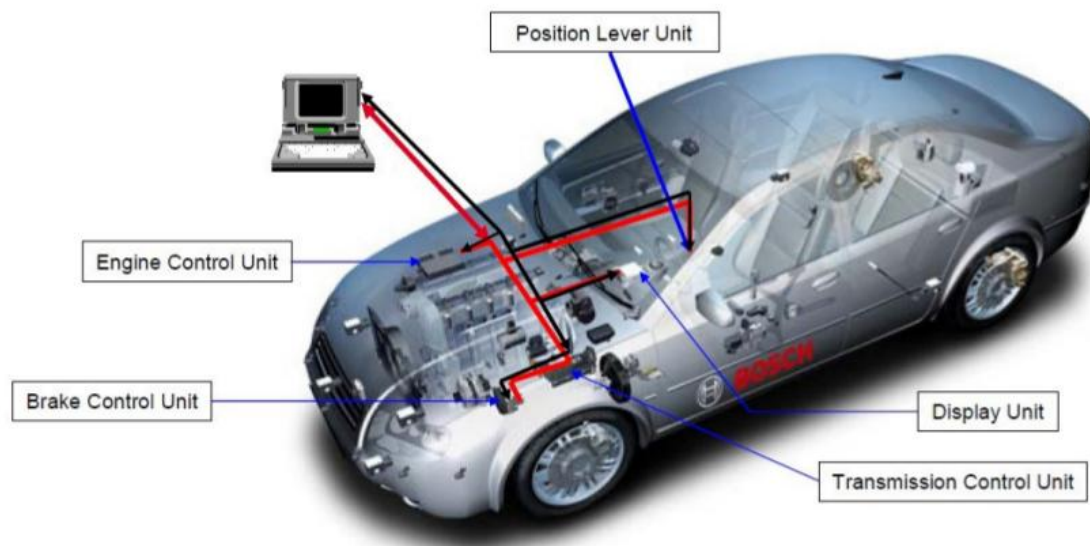
- All you need is the sitecode
 - We got that from memory
- Complete time for reading the memory and opening the lock is about 200 milliseconds
 - This can be longer if you need to try different addresses, due to supporting multiple door types
- Creates an entry in the audit report that shows the PP having been used to open the lock
 - But it doesn't alter any data on the lock or inhibit normal functioning



案例-4: 汽车ECU

❑ “Dude, WTF in my car?”, Blackhat 2013

Communication System in the Vehicle



案例-5: 监控摄像头

□ “海康威视“黑天鹅”惊魂两天”, 新华网



这些弱口令包括“123456”、“888888”等初始密码
“所有暴露在互联网环境下的设备都会面临黑客攻击的风险。”
海康威视称，早在去年3月，公司就
已经在官网上提醒用户修改初始密码。

案例-6: IP摄像头

❑ “Abusing the Internet of Things - BLACKOUTS. FREAKOUTS. AND STAKEOUTS”, Blackhat 2014



NetCam connects to local Wi-Fi

Traffic is secured using SSL **except sometimes it's not and your credentials are sent to a remote server in clear**

```

▶ Frame 331: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Ethernet II, Src:                               Dst:
▶ Internet Protocol Version 4, Src: 192.168.2.7 (192.168.2.7), Dst: 66.160.133.67 (66.160.133.67)
▼ Transmission Control Protocol, Src Port: 51121 (51121), Dst Port: brlp-3 (4104), Seq: 0, Len: 0
  Source port: 51121 (51121)
  Destination port: brlp-3 (4104)
  [Stream index: 1]
  Sequence number: 0 (relative sequence)
  Header length: 44 bytes
  ▶ Flags: 0x002 (SYN)
  Window size value: 65535
  [Calculated window size: 65535]
  ▶ Checksum: 0x398d [validation disabled]

```

```

0000
0010
0020
0030
0040

```

```

CX_UNAME=
CX_PASSWD=
current_version=1.1
os_name2=iphone2
#Sat Oct 12 19:37:42 PDT 2013
1=66.160.133.79\4104
#Sat Oct 12 19:37:42 PDT 2013
1=66.160.133.79\4104

```


案例-7: 婴儿监控器

❑ “Abusing the Internet of Things - BLACKOUTS. FREAKOUTS. AND STAKEOUTS”, Blackhat 2014



Baby monitor connects to local Wi-Fi

Connects to external SIP proxy to communicate with iOS app



Connects to monitor using local Wi-Fi to obtain authorization

Connects to external SIP proxy to communicate with monitor

smartUniqueID and serialNumber are basically the authentication tokens.

案例-8: 无人机

❑ “Knocking my neighbor’s kid’s drone offline”, Defcon 2015



```
telnet 192.168.42.1
# ardrone3_shutdown.sh
shutdown: Shutdown Dragon
shutdown: Asking Dragon to stop...
shutdown: Stopping users of eMMC
eMMC_release: Releasing eMMC...
MTP: stopping service
shutdown: Synchronise filesystems
eMMC_umount: Umounting eMMC...
Connection closed by foreign host.
```

案例-9: 吉普切诺基远程攻击

□ “Remote Exploitation of an Unaltered Passenger Vehicle”, Blackhat 2015



脆弱点

- ❑ 弱登陆认证 or 无登陆认证
- ❑ 固件未签名 or 外部固件
- ❑ 固件未加密 or 固件弱加密
- ❑ 秘钥未保护 or 秘钥弱保护
- ❑ 芯片测试接口未关闭
- ❑ 使用“自行临时设计”的密码协议
- ❑ 假定“设备处在安全内部wifi”

那么，

密码芯片能贡献点啥？

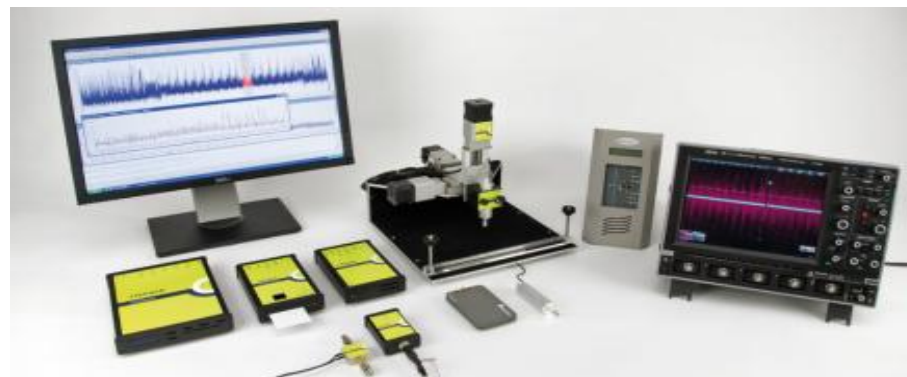
密码芯片

- 约2000年开始，开始在欧洲大量应用
- 中国2015年不再发行磁条卡
- 15年的攻击/防护技术研究
 - 秘钥生成
 - 秘钥保存
 - 加密、解密
 - 签名、验签
 - 安全存储

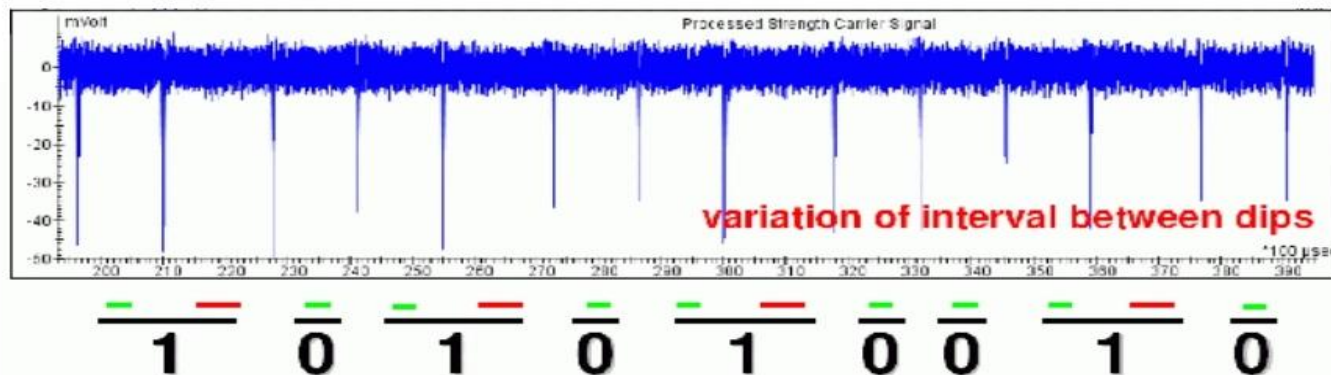


抗旁路攻击

旁路攻击设备



芯片密钥



抗故障攻击

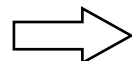
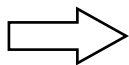
故障攻击

- 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



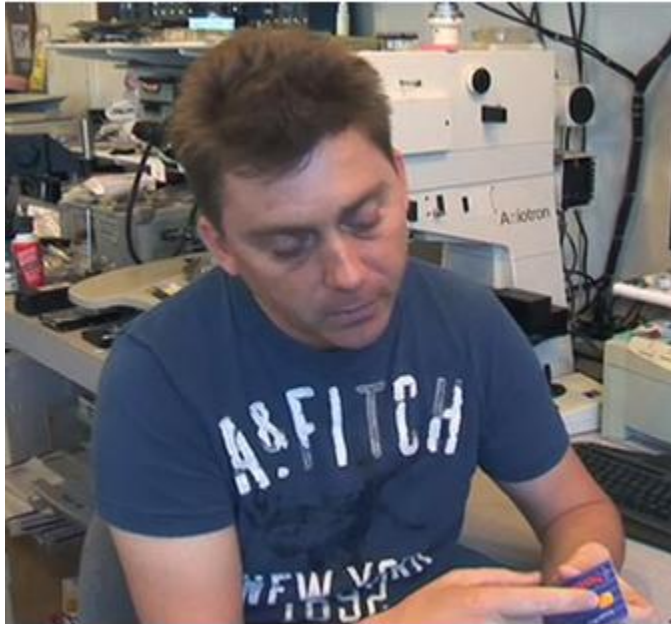
Riscure高精度激光
错误注入平台

input



error

抗侵入式攻击



The chip analysis studio of Christopher Tarnovsky

其他安全功能

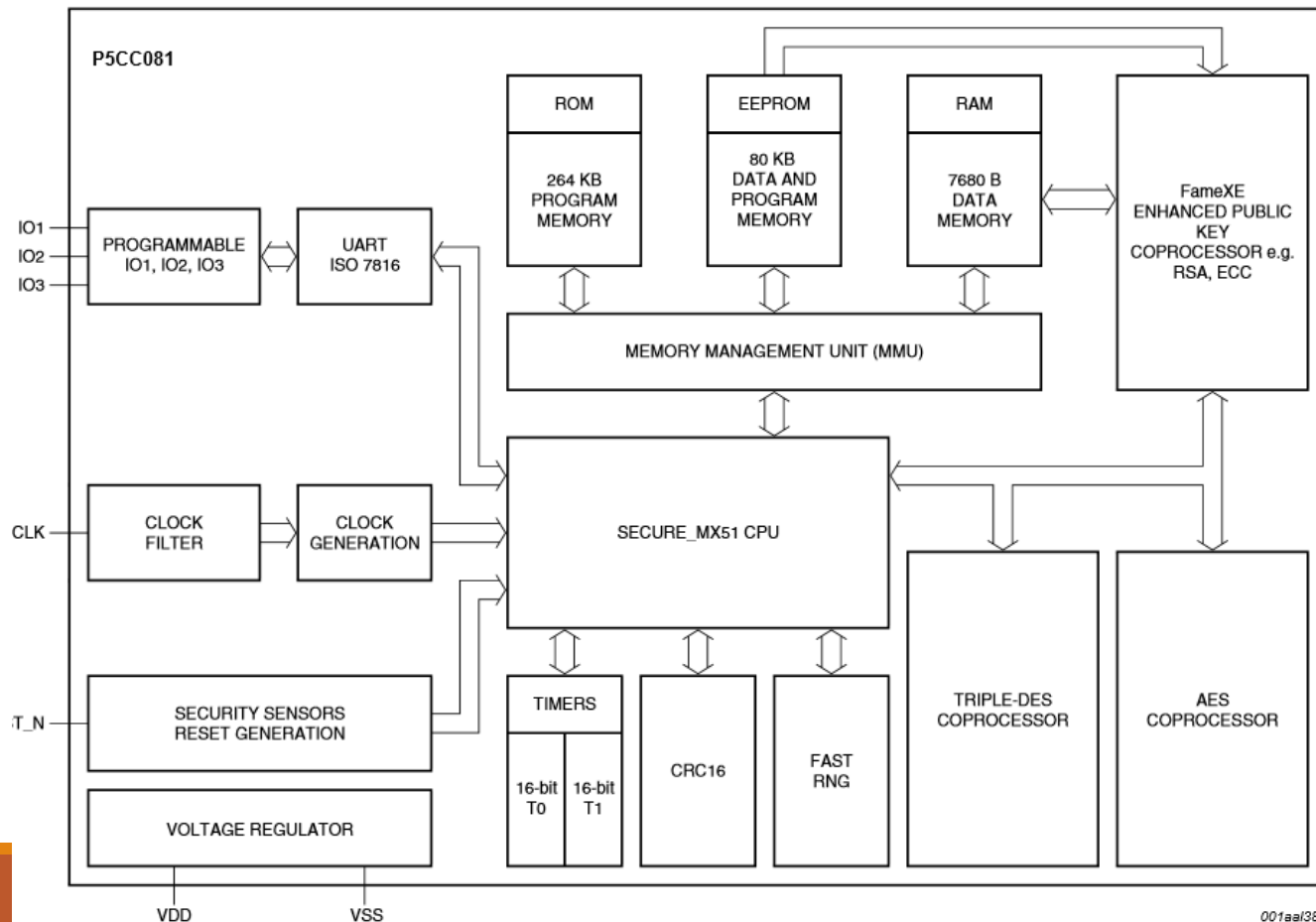
❑ 固件加密

❑ 总线加密

❑ 安全CPU

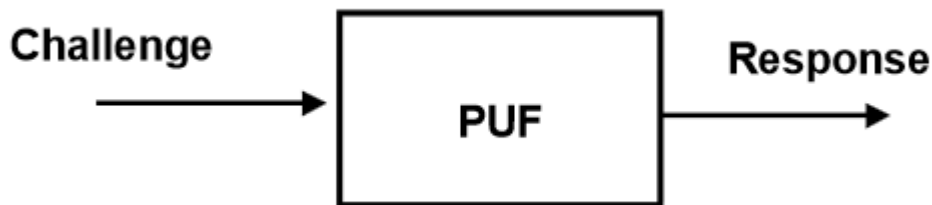
❑ 传感器

❑ 测试封口



PUF: 芯片指纹

- ❑ PUF: Physically Unclonable Function (物理不可克隆函数)
- ❑ 基本思想
 - 使用芯片生产过程中的随机性
 - 同样的设计，在不同的die上特征不同
 - 仅在上电时才产生



安全检测

❑ 国密、BCTC/EMV、Common Criteria、FIPS 140-2等

- 随机数发生器
- 密码算法（DES/RSA/ECC/SHA/SM2/SM3/SM4）
- 芯片抗物理攻击能力
- 嵌入式软件安全
- 芯片生命周期管理
- 配置管理
- ...

如果，

IoT设备都使用安全芯片.....

基于密码芯片的IoT

□ 基于密码协议的身份认证

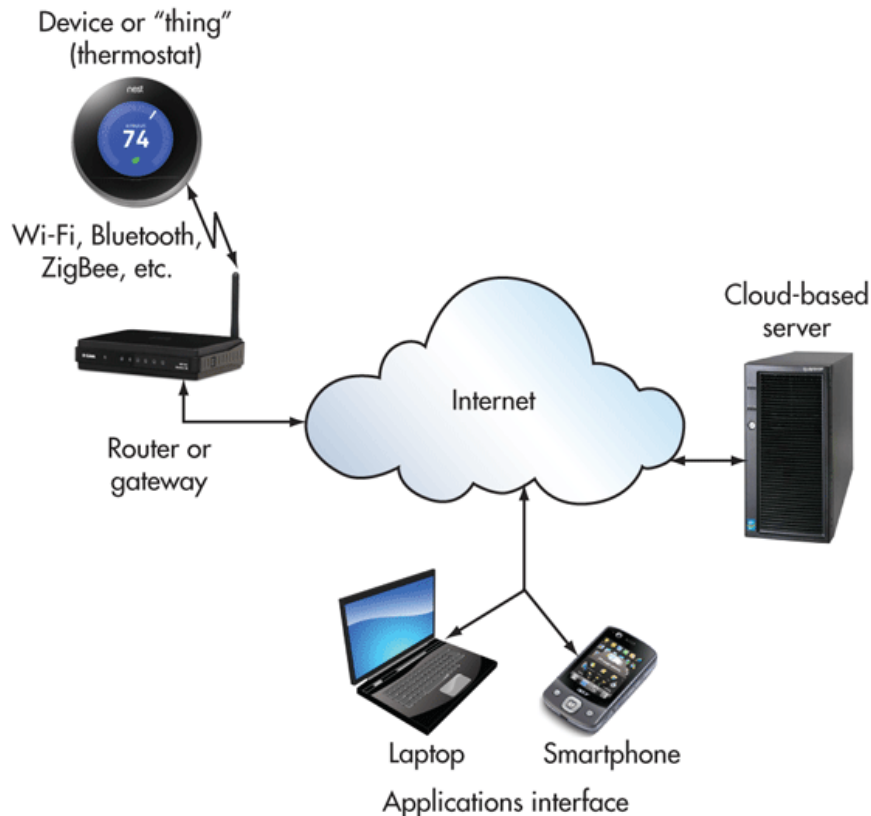
■ 基于PKI



■ 基于PUF



■ Password



基于密码芯片的IoT

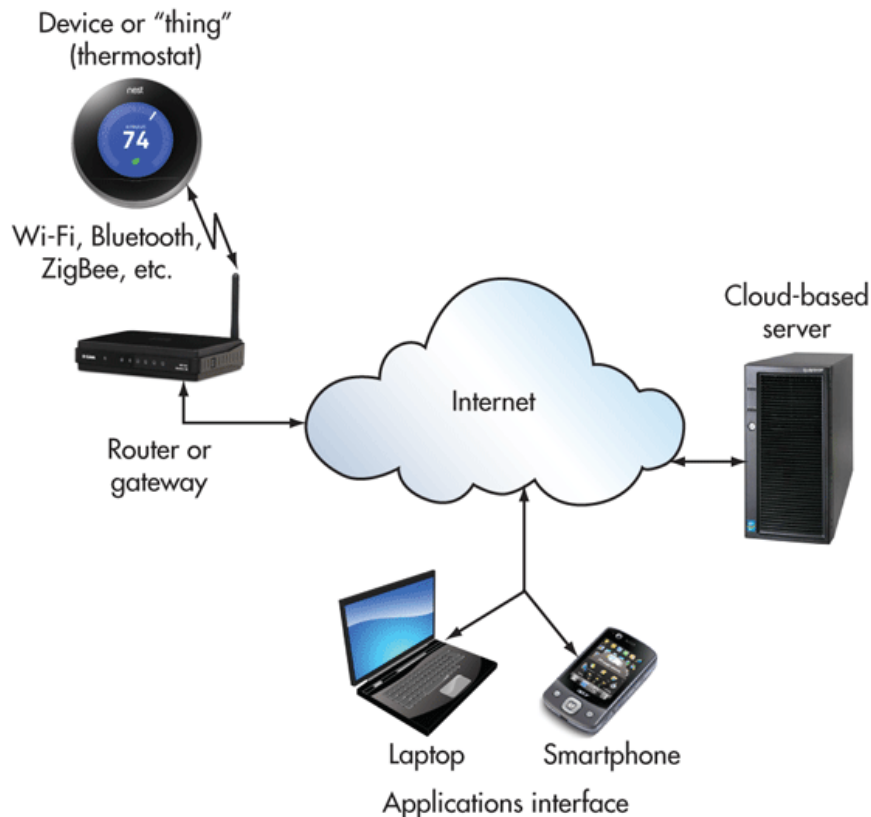
□ 端到端密钥协商

- 安全密钥协商

- 安全TLS

- 预置密码

- 明文密钥协商



基于密码芯片的IoT

安全固件

- 固件加密



- 固件签名



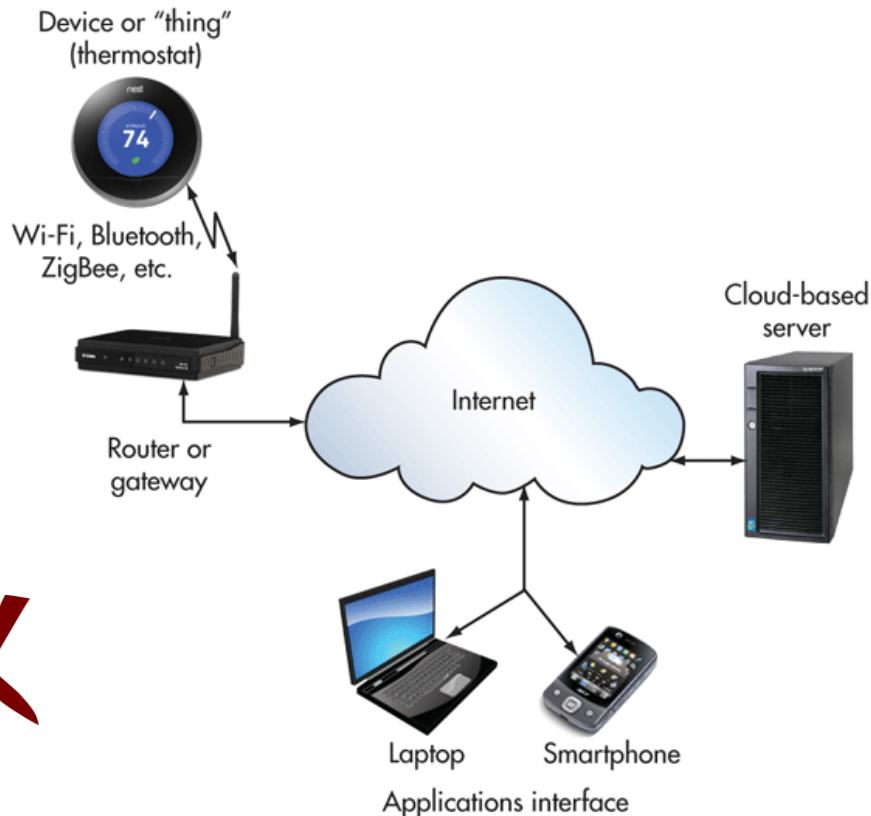
- 安全固件升级



- 灾难恢复



- 固件破解、反向、非法修改



基于密码芯片的IoT

□ 安全加解密运算

■ 高性能



■ 低能耗



■ 抗物理攻击



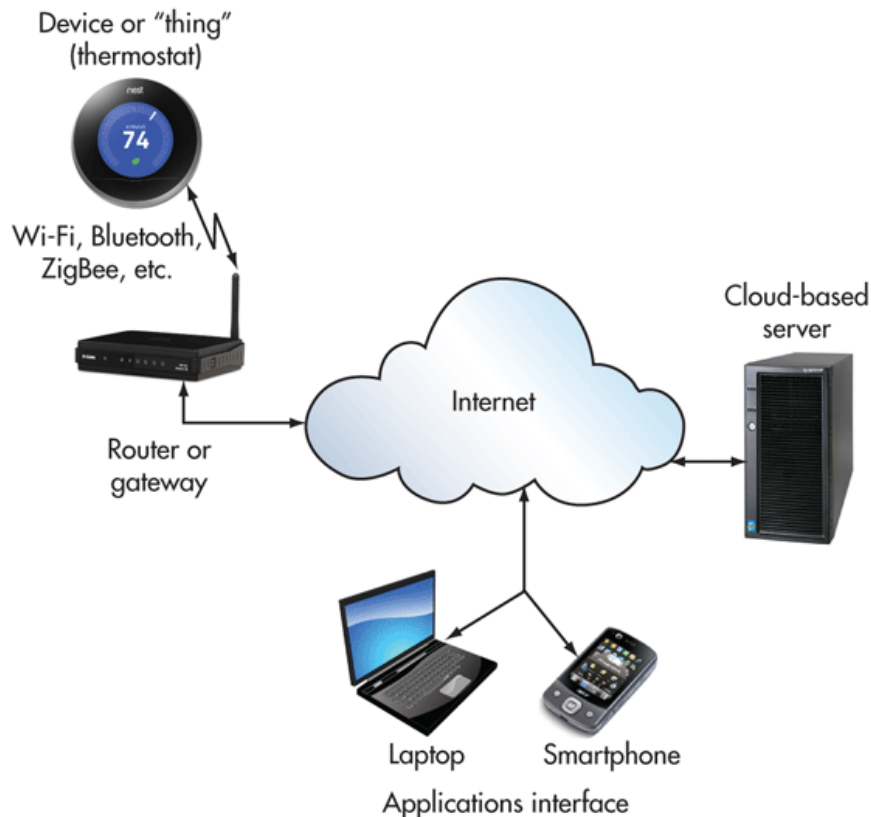
■ 数据加密保存



■ 加解密、签名软件漏洞



■ 物理攻击



基于密码芯片的IoT

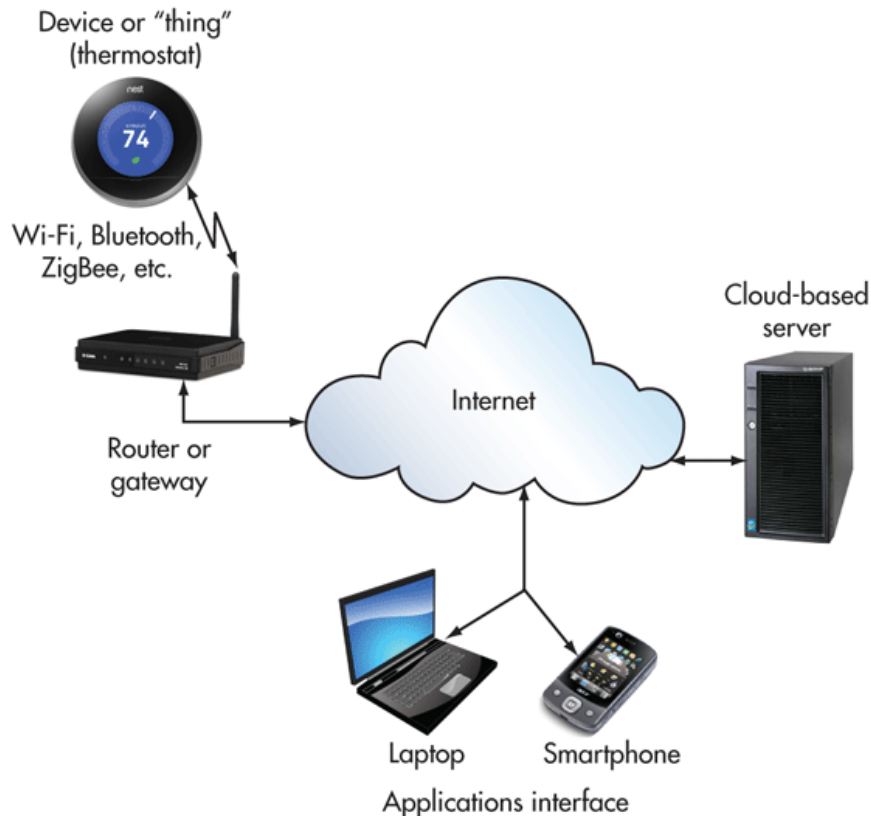
□ 安全组网 & 灾难恢复

- 基于硬件Root-of-Trust



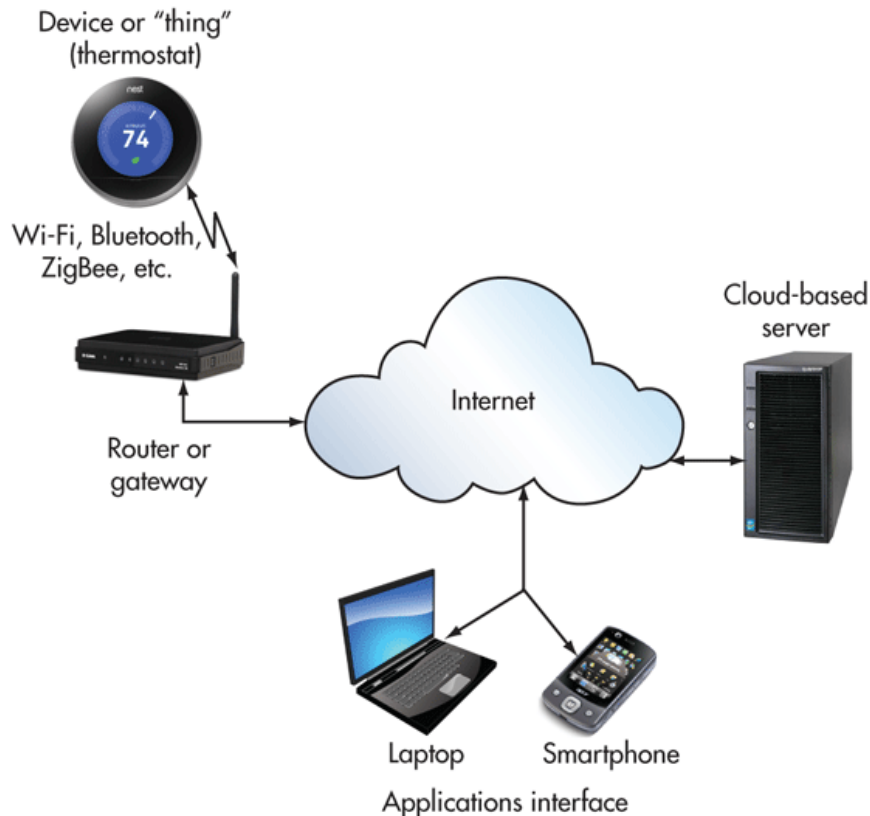
- 灾难恢复和自愈网

- 被破解，然后扔掉



基于密码芯片的IoT

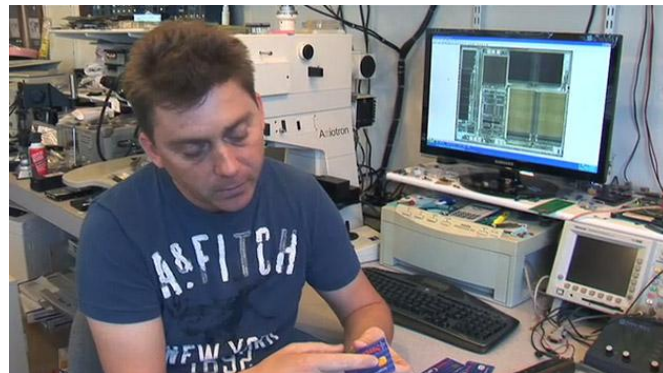
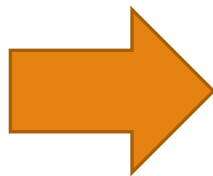
- ❑ 安全固件(加密/签名)
- ❑ 安全密钥存储
- ❑ 端到端加密
- ❑ 强用户认证
- ❑ 安全存储
- ❑ 设备唯一识别
- ❑ 灾难恢复



安全测评



终极目标





- This, Jen, is the Internet of things. -