CAICT 泰尔终端实验室
中国信息通信研究院 China Telecommunication Technology Labs-Terminals

信息安全部
Information Security

智能家居信息安全防护与检测

泰尔终端实验室 信息安全部
刘　陶
2017-03-29

交流提纲

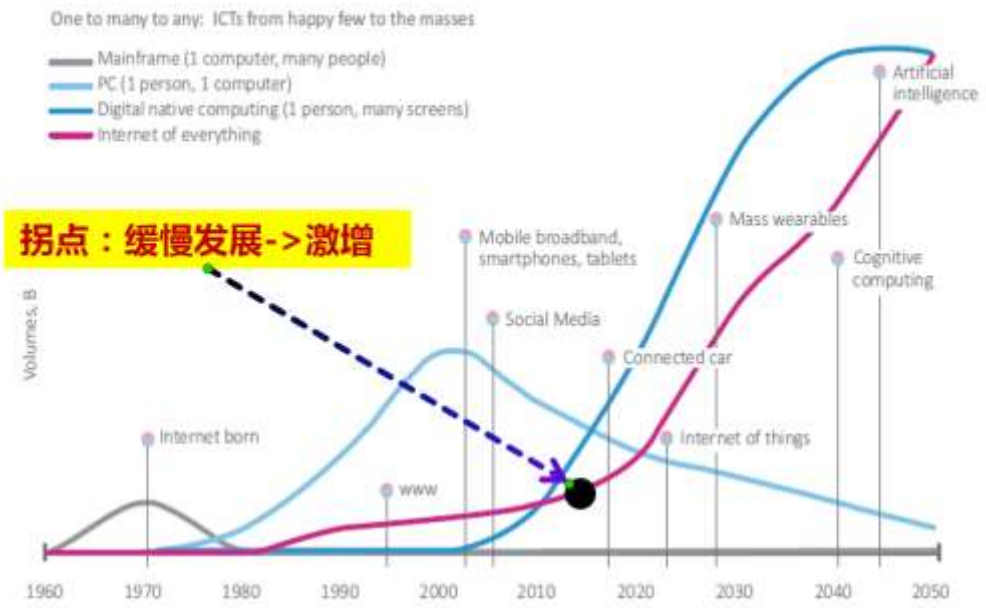
信息安全部
Information Security

- 一、智能家居安全威胁分析
- 二、智能家居架构及安全防护重点
- 三、智能家居安全检测体系
- 四、智能家居标准与检测认证思路

智能家居市场蓬勃发展，设备种类多样

信息安全部 Information Security

- 物联网市场正呈现指数级增长态势，万物互联已成为技术发展和产业应用的必然趋势。根据Gartner预测，2020年全球IoT设备数量将高达260亿件。
- 智能家居作为IoT典型代表之一，据国内机构预测，至2018年，我国智能家居市场规模将达1800亿人民币，而全球市场规模有望达4000亿元。



智能家居常见使用场景

分类	描述
安防	入侵报警、火灾监控、水电气监控、可视对话
娱乐	电视、游戏、音乐媒体
视频	视频监控、录像
通讯	呼救设备、多媒体通讯设备
计量	远程抄表、能耗提醒
监测	温度、湿度、光照度等环境监测
家电	空调、洗衣机、电饭煲、微波炉、烤箱等

智能家居安全威胁

信息安全部 Information Security

智能家居所面临的主要信息安全风险

隐私泄露

白帽验证可通过智能电视监视用户；黑客可利用云技术、大数据等技术分析智能家居产品用户行为和日常生活轨迹等。

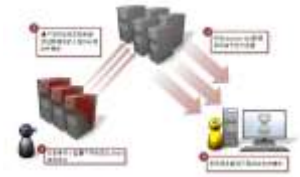
财产损失

黑客通过捕获空气中的蓝牙信号破解某智能门锁的密码；通过远程恶意操作，导致设备不可用。

人身攻击

白帽曾验证入侵智能插座的办法，包括开启加热装置和电熨斗；美国Trustwave安全公司还成功破解了日本Lixil智能马桶所使用的蓝牙通信链路，能通过蓝牙发起连接而任意操纵马桶盖的开启和关闭，自动喷水等。

网络攻击



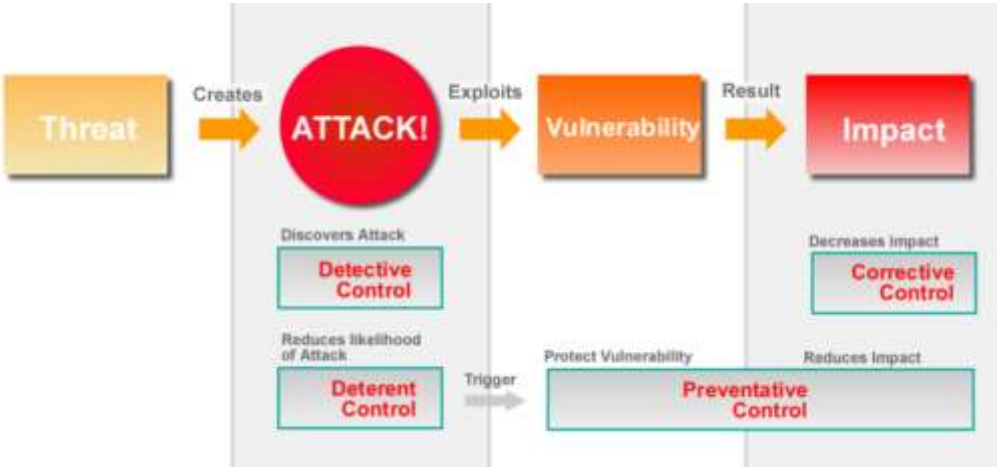
Mirai、Bashlite等新型病毒可感染联网的家电设备（如，路由网关、电视、多媒体中心等），控制的僵尸网络已成为**DDoS攻击领域的新生力量**。2016年底的美国东部网络瘫痪事件引发广泛关注。

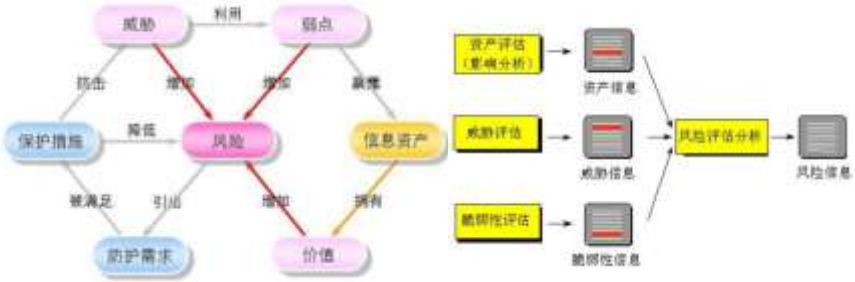
舆论扰乱

白帽曾遥控三星智能电视发布“白宫遭到攻击”的假新闻，除此之外，飞利浦、惠普等多个知名品牌智能电视均被曝光存在严重安全漏洞等。

智能家居安全缺陷

信息安全部
Information Security





- 根据ISO/IEC 13335 信息安全模型，系统缺陷是导致安全威胁的根本原因

智能家居系统安全缺陷

- 智能家居系统可能存在的主要安全缺陷
  - 硬件层面
  - 软件层面
  - 通信协议

芯片/OS/应用安全缺陷 → 终端设备软/硬件安全漏洞

访问控制缺乏/明文传输/协议安全缺陷 → 传输信道安全漏洞

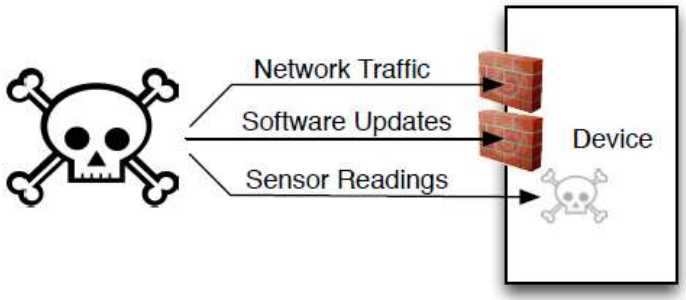
用户数据过度采集/云端服务安全缺陷/管理不完善 → 应用服务安全漏洞

硬件层面：信息传感器的结构特点面临新型威胁

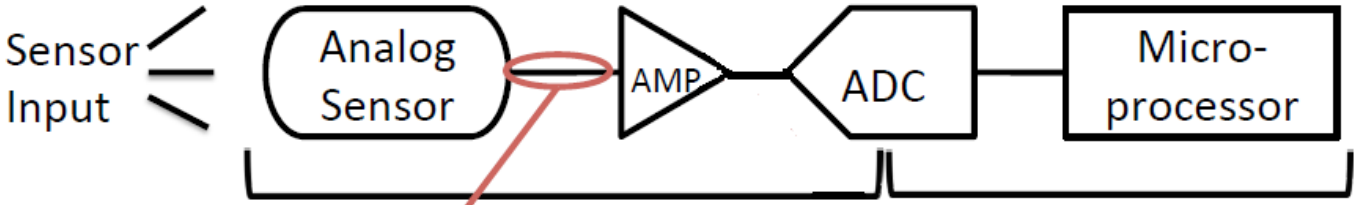
信息安全部 Information Security

智能家居终端核心硬件组成：

- MCU-处理器
- Sensor 等完成数据采集、处理、存储的芯片
- 射频芯片及相关模块

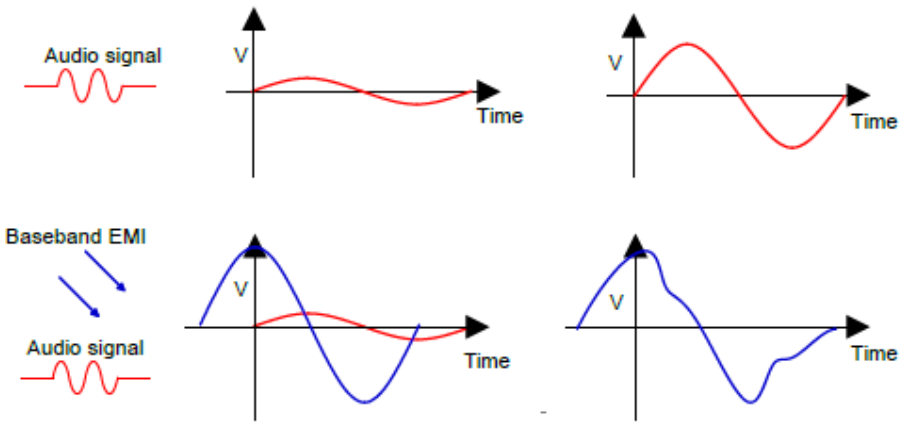


智能家居设备通常信任传感器的输入，访问控制的强度较网络流量和软件更新要弱



"Ghost Talk"

连接处相对暴露，为攻击信号（EMI）插入提供可能。EMI：Electro Magnetic Interference攻击是针对智能家居终端的一种攻击方式，分为基带EMI攻击和调制EMI攻击。



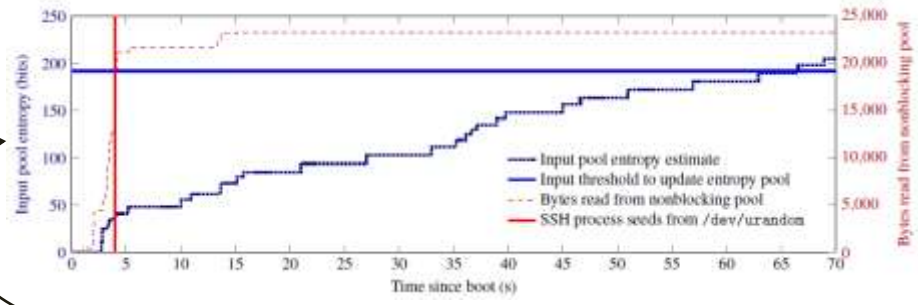
软件层面：OS欠缺对新产品特点的考虑而存在弱点

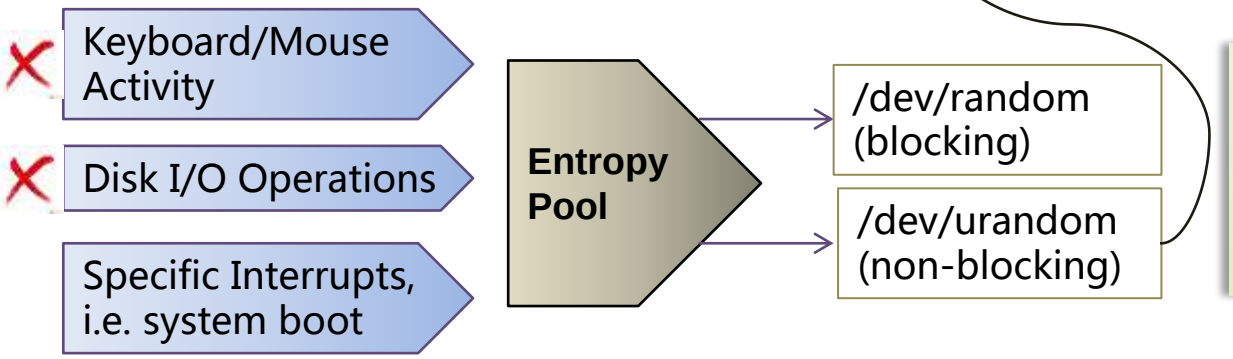
信息安全部 Information Security

很多智能家居终端OS基于Linux kernel开发，但Linux最初并不是针对这类终端设计，因此需优化调整，避免因为没有适配新型智能终端的特点而形成新的安全漏洞。

“at least 5.57% of TLS hosts and 9.60% of SSH hosts use the same keys as other hosts”——很多新型智能终端使用相同的加密密钥，其根本原因是这些终端OS内核产生密钥的随机数存在缺陷，与Linux随机数产生机制不适合新型智能终端特点密切相关。

Linux Urandom Boot-Time Entropy Hole





该漏洞近期已被修复，但由于IoT设备普遍更新周期较长，仍有很多系统存在该漏洞

通信协议漏洞被挖掘，数据传输面临窃听和伪造威胁

- ZigBee初始密钥明文传输
- 可以通过Sniff嗅探获取
- 最终导致攻击者能够接管PAN内所有ZigBee连接的智能设备

ZigBee是一种新兴的短距离无线通信技术。它提供了基于循环冗余校验（CRC）的数据包完整性检查功能，支持鉴权和认证，采用了AES-128的加密算法

智能家居信息安全隐患的影响因素

信息安全部 Information Security

① 网络扁平化发展，接入安全问题突出

接入点无处不在，网络边界不清晰，曾在终端防护中使用的隔离、切断等安全管控措施面临较大挑战，任一设备受到攻击感染，其传播速度将呈指数增长，影响范围不得而知。

② 数据大多存放云端，传输和存储安全面临挑战

当前云服务市场尚处于发展阶段，公有云安全防护能力参差不齐，网络服务、云应用中出现的安全问题即可导致智能家居用户终端信息安全问题。

③ 厂商联盟各自为营，缺乏统一标准

多架构体系---多应用协议---多业态渗透

海尔U+	ZigBee	家电厂商
美的	BT	互联网厂商
格力	WiFi	开发商

④ 行业安全产业化滞后，缺乏有效检测技术

交流提纲

信息安全部
Information Security

一、智能家居安全威胁分析

二、智能家居架构及安全防护重点

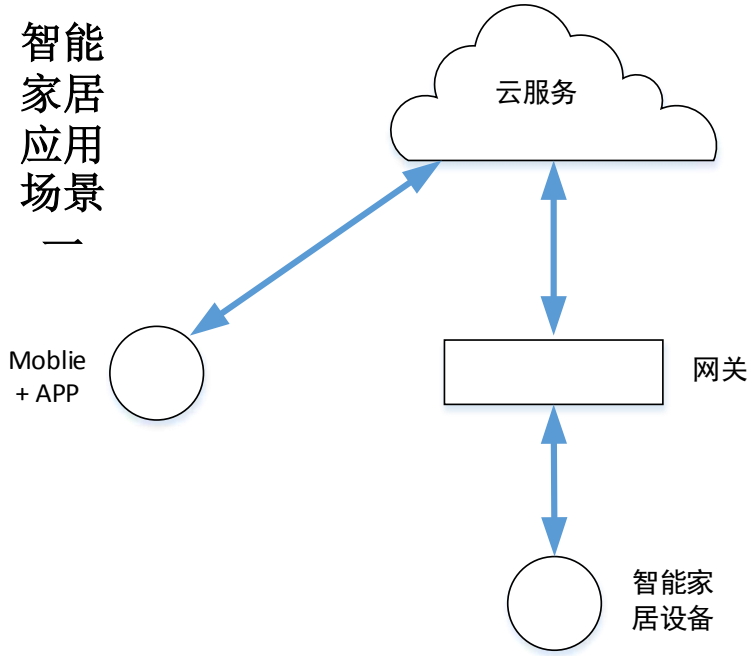
三、智能家居安全检测体系

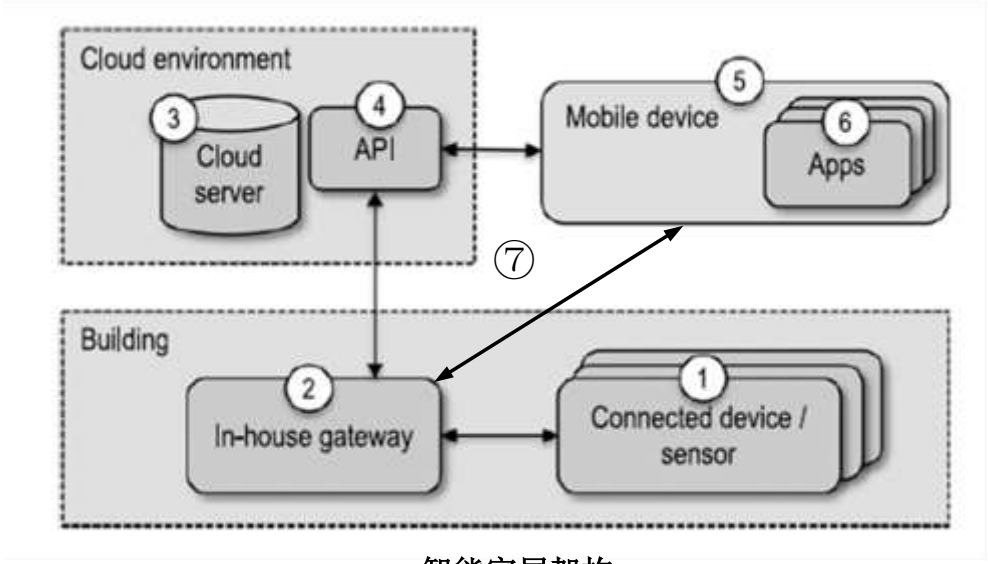
四、智能家居标准与检测认证思路

智能家居应用架构

信息安全部 Information Security

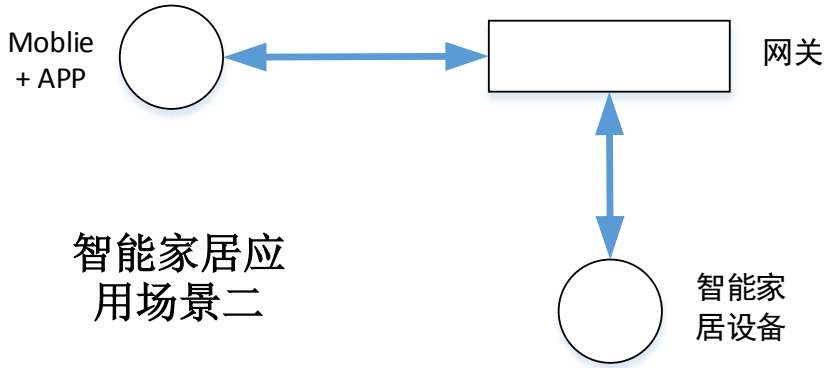
智能家居应用场景一





智能家居架构

智能家居应用场景二



智能家居系统安全需求：

① 智能家居终端设备安全

② 家庭网关&路由安全

③ 云端服务安全

④ 云端应用接口安全

⑤ 移动智能终端安全

⑥ 移动智能终端应用软件安全

⑦ 通信链路安全

③、④ 适用标准GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》

⑤、⑥ 适用标准YDT 2407-2013《移动终端安全能力技术要求》

关注智能家居终端设备安全

信息安全部
Information Security

智能家居终端

- 智能家居终端是连接到家庭网络的、协同提供智能家居服务的各种终端设备，包括：智能家居网关设备、控制设备、以及相关应用设备

智能家居应用设备

- 与智能家居网关设备相连，通过对接收指令的执行，实现智能家居应用的设备

智能家居网关设备

- 同时与公共通信网络、智能家居控制设备和应用终端相连的设备，为应用设备分配通讯地址，根据分配的通讯地址与智能家居应用设备通信，并完成控制设备与应用设备之间的信令转换，将转换后的信令发送至智能家居控制设备或应用设备

智能家居设备

- 根据接收的用户指令或预先配置的任务，执行智能家居控制逻辑，通过智能家居网关向智能家居应用设备发出指令，通过智能家居应用设备对指令的执行，实现智能家居应用。常见控制模式包括，场景控制、组合控制、关联控制、远程控制等

智能家居终端存在的弱点和相应威胁

信息安全部
Information Security

对象	主要安全威胁	脆弱点
硬件	1. 非授权的访问； 2. 功能失效、设备不可用； 3. 假冒设备； 4. 重放攻击、侧信道攻击；	1. 信号注入 2. 传输未加密 3. 访问控制缺失
固件	1. 非授权的访问； 2. 审计数据丢失； 3. 恶意代码攻击； 4. DDoS攻击、溢出攻击、口令猜测、密码分析	1. 缺乏身份认证机制 2. 访问控制缺失 3. 调试接口暴露 4. 审计漏洞
应用软件	1. 非授权访问； 2. 软件漏洞； 3. 恶意代码攻击；	1. 弱口令 2. 缺少身份认证机制 3. 调试接口暴露
外围接口	1. 非授权访问； 2. 审计失效；	1. 缺少访问控制机制 2. 调试接口暴露 3. 审计漏洞
通信	1. 通信数据泄露、篡改、丢失； 2. 传输中断、拦截、篡改、伪造； 3. 拒绝服务攻击，重放攻击，中间人攻击； 4. 虚假路由； 5. 通信协议漏洞	1. 采用明文传输 2. 通信协议存在漏洞 3. 安全协议存在漏洞
用户数据	1. 用户数据泄露	1. 终端过度手机 2. 传输、存储安全漏洞

*所列威胁均为由攻击者主动发起的威胁，不包括不可抗力，误操作等客观存在

智能家居终端设备安全防护需求

信息安全部 Information Security

智能家居终端设备安全能力框架

交流提纲

信息安全部
Information Security

一、智能家居安全威胁分析

二、智能家居架构及安全防护重点

三、智能家居安全检测体系

四、智能家居标准与检测认证思路

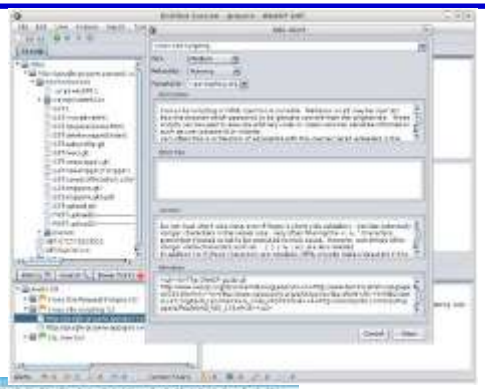
智能家居安全测试

- 深度渗透测试

◈ Web漏洞扫描

对固件、后台服务等web服务进行漏洞扫描，发现中、高等级脆弱点，尝试进行渗透测试。

→拖库、非法访问



◈ 通信安全测试

利用网络抓包、SSL中间人攻击等方法，对通信进行监控，对通信协议安全性、数据传输保密性和完整性进行测试。

→用户名密码泄漏、数据流地址泄漏、其他信息泄露

◈ 固件逆向分析

利用固件逆向和自动化分析工具，对固件进行逆向分析，发现其证书、密钥存储及业务实现所存在的逻辑漏洞。

→证书泄漏、密钥泄漏、代码泄漏。

◈ 应用安全性分析

利用App漏洞扫描、反编译等工具，对智能家居App进行安全性测试，发现存在的漏洞。

→密钥泄露、代码逻辑漏洞、业务逻辑泄露。

安全评估检测体系

信息安全部 Information Security

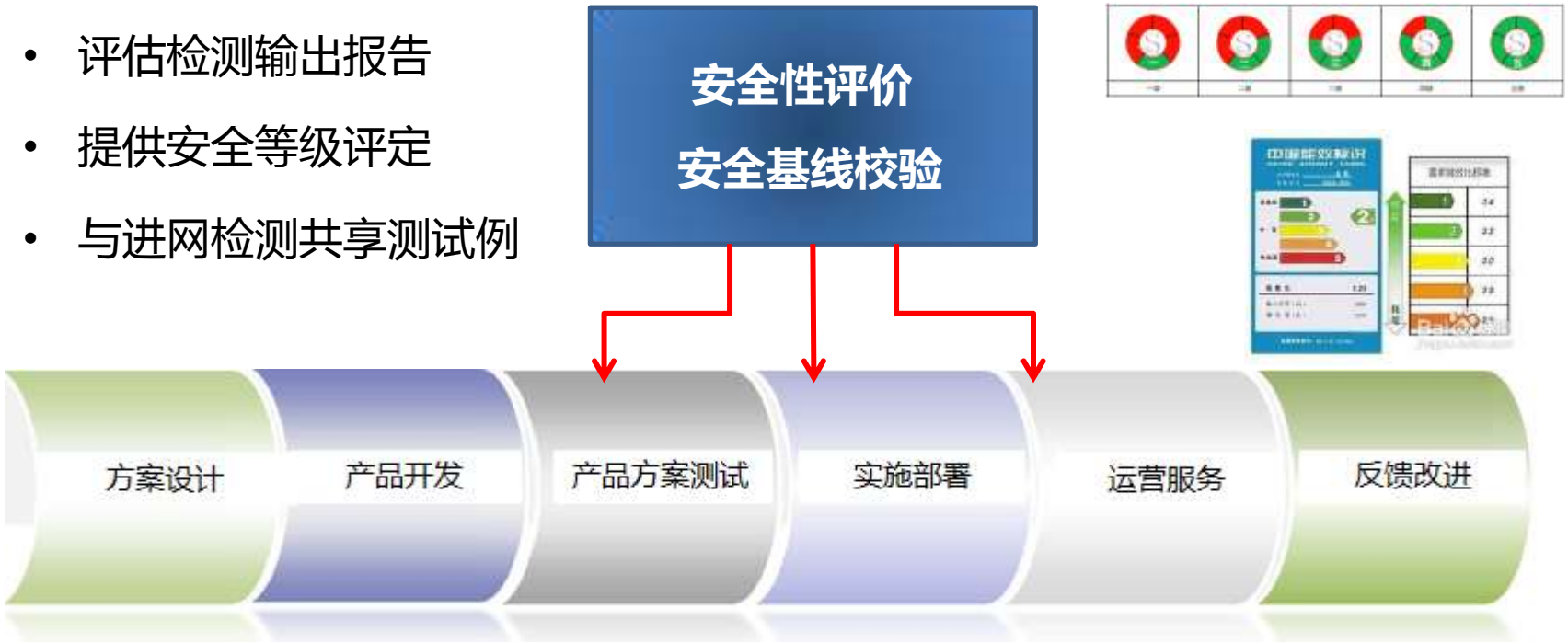
	安全性评价 黑盒检测	安全基线校验 白盒分析
评价目标	对智能家居的安全性进行黑盒检测	对智能家居所使用的安全机制的符合性进行评估
评价方式	漏洞扫描+渗透测试，包括以下渗透接口和扫描对象： • 云端服务器及WEB应用 • 通信协议WiFi/BT/ZigBee，自定义协议 • 手机APP/主控中心，智能家居终端（软件+硬件多层面）	安全基线包括： • 安全域隔离，e.g. TEE一致性检测 • 身份认证与访问控制，e.g. 定制FW • 应用安全， e.g. 签名的使用 • 数据安全，完整性保护及加密 • 监控与审计
能力要求	• 扫描工具 • 攻击实操 • 渗透脚本	• 定义《安全基线》规范 • 检测工具配套

评测对象和效果

信息安全部
Information Security

- “安全性评价”和“安全基线校验”服务相互独立
- 评估检测服务向传统家电厂商、新型家电厂商、互联网厂商提供

- 评估检测输出报告
- 提供安全等级评定
- 与进网检测共享测试例

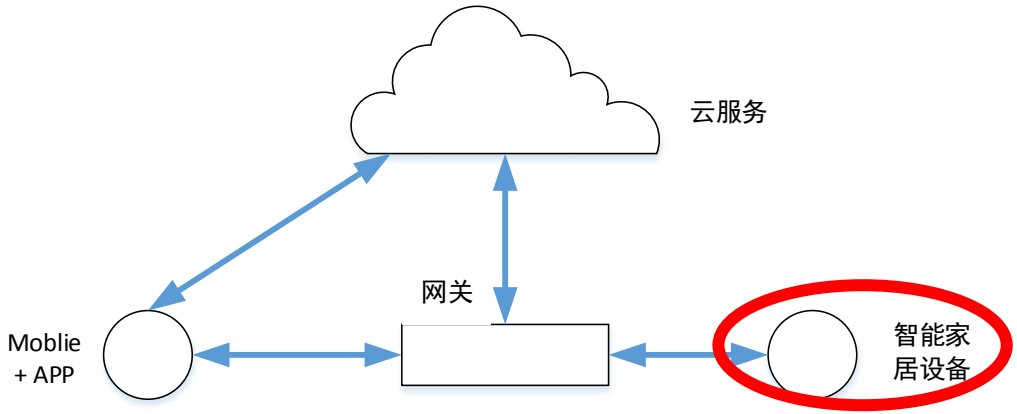


终端硬件检测

信息安全部
Information Security

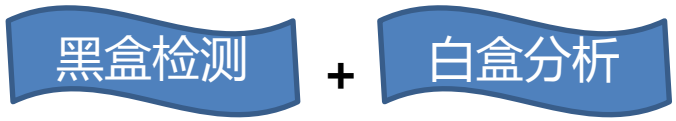
硬件安全测评方法

进行智能终端硬件侧信道攻击及故障注入攻击测试，并将黑盒测试与白盒测试结合，全面检测评估硬件产品安全



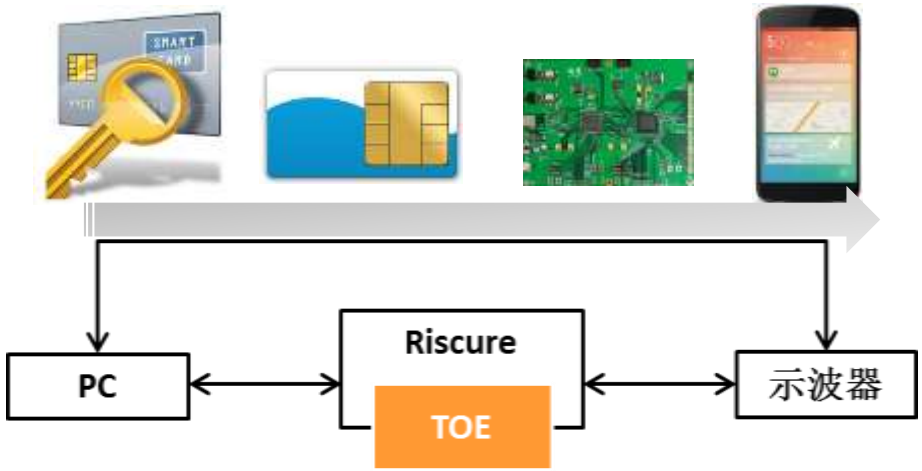
评估关键硬件

对关键硬件应用通过文档审查与实验验证相结合的方式进行评估



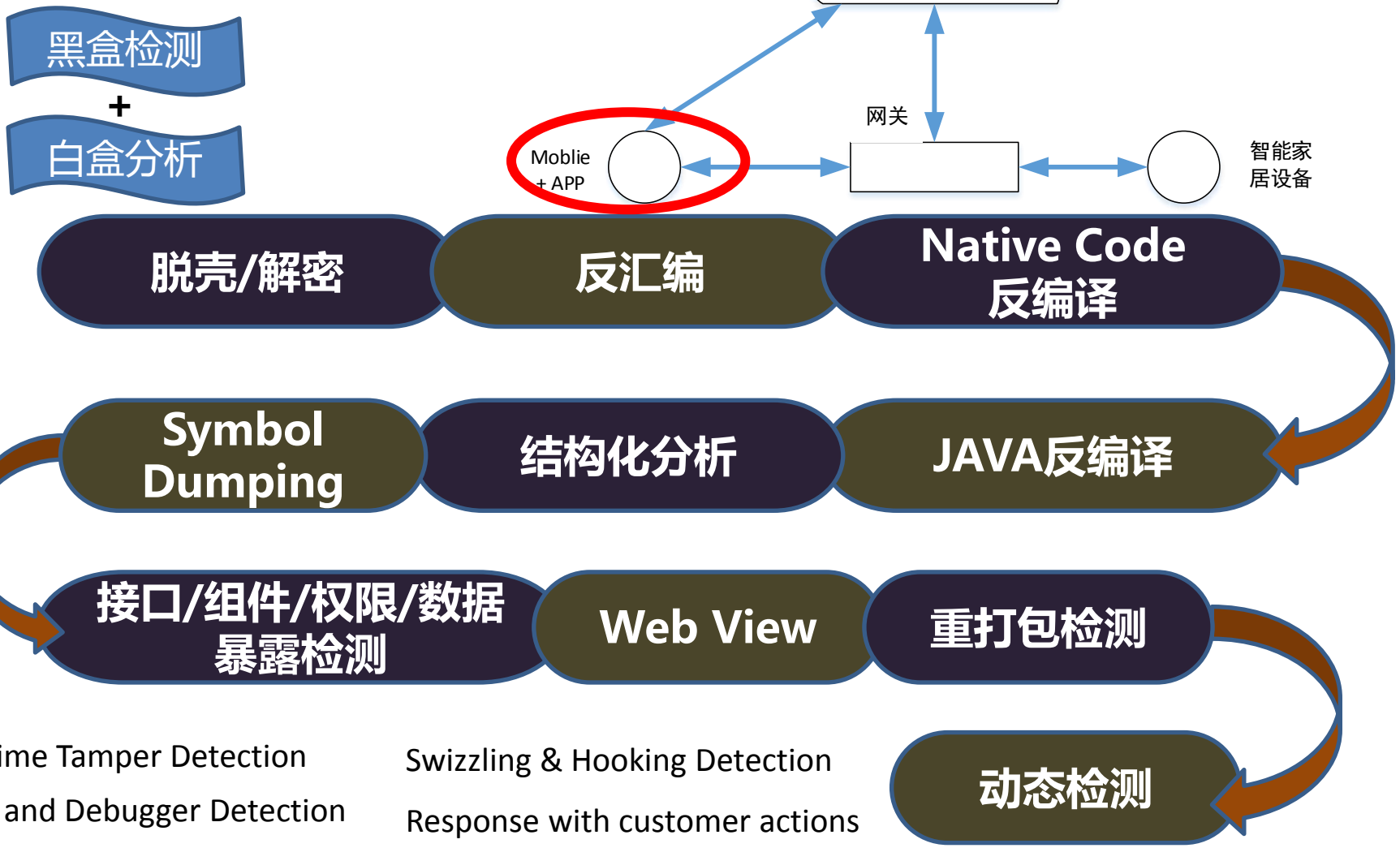
挖掘硬件漏洞

对测试设备Riscure Inspector进行二次开发，提升对包括智能家居在内的新型智能终端的硬件安全检测能力



手机APP审计

信息安全部
Information Security



Runtime Tamper Detection

Root and Debugger Detection

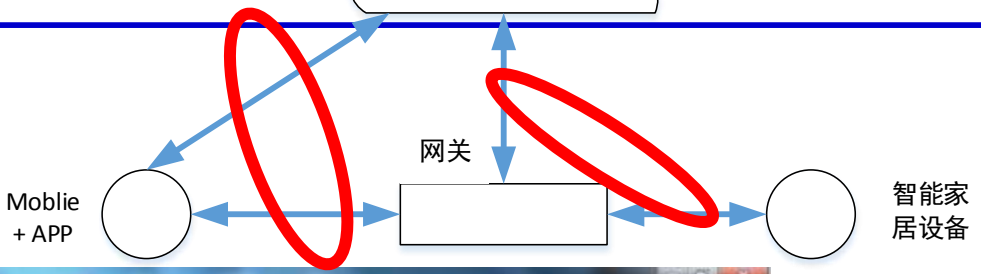
Swizzling & Hooking Detection

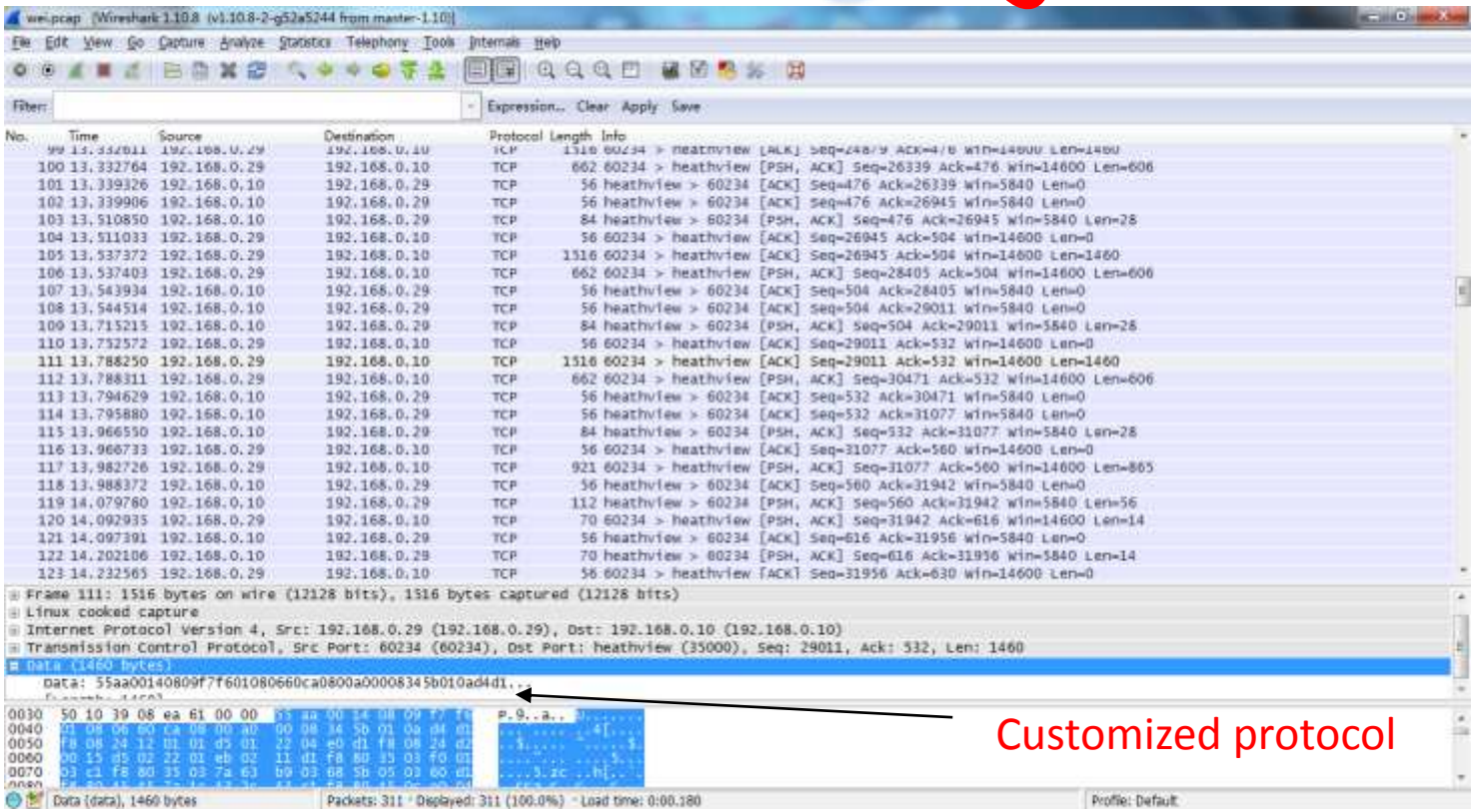
Response with customer actions

通信协议安全性分析

信息安全部 formation Security

发现通信协议中明文传输密钥，用户口令，缺少验证，指令合规性等多种安全性问题。





黑盒检测

多种检测工具：

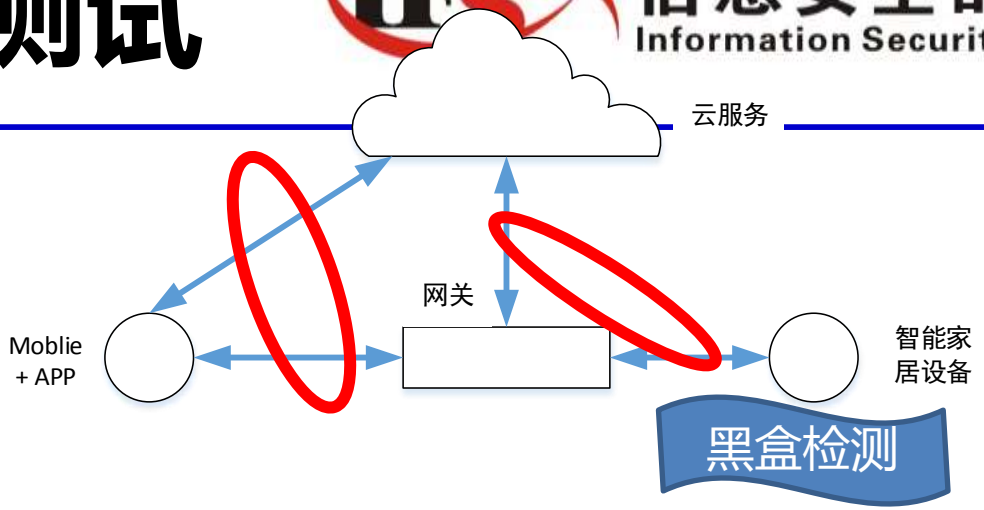
- MD8475A
- Wireshark
- Fiddler
- ……

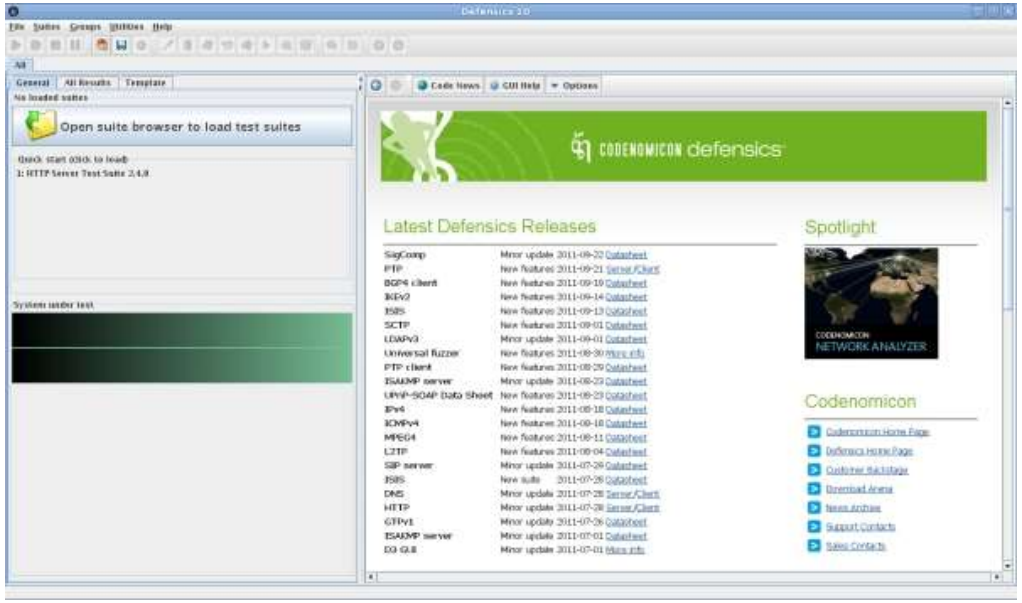
通信协议鲁棒性测试

信息安全部
Information Security

Codenomicon Defensics

集成多种测试包，内置大量测试实例，测试协议的健全性和安全性，旨在发现软件安全漏洞，管理和削弱安全威胁。它利用深度协议模型，智能的、精确的命中目标协议中易受攻击影响的部分，自动的生成具有广泛覆盖的Fuzz测试用例， 目前覆盖超过200 种协议和文件格式。



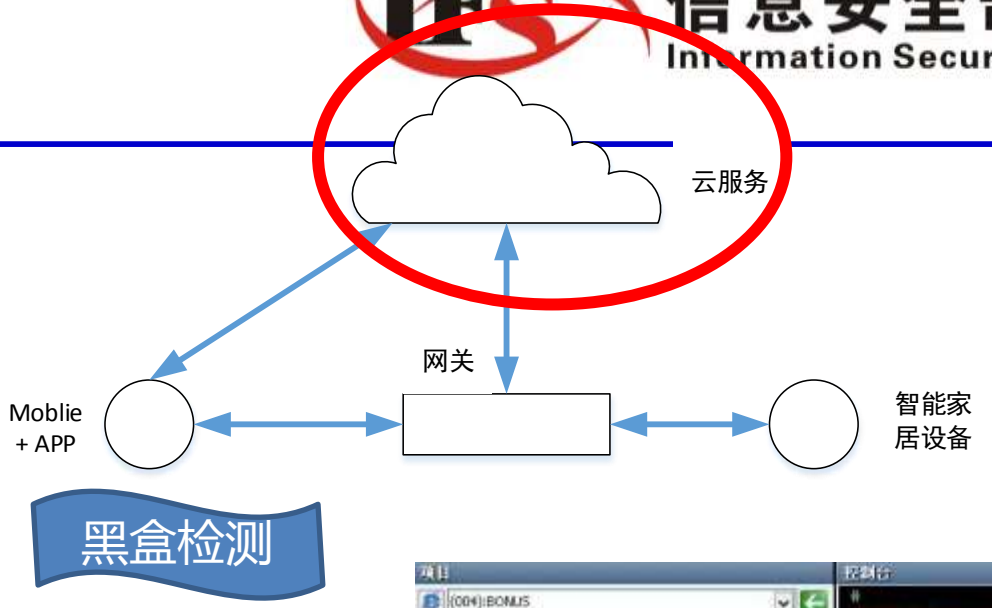


云端安全扫描

信息安全部
Information Security

WEB服务进行扫描，四大引擎：

1. 任务调度引擎负责处理任务的分发和管理
2. 数据分析引擎实现基础数据的采集及综合比较
3. 事件监测引擎对扫描引擎和整个管理平台的状态进行监测并记录，为告警及日志管理提供支持
4. 扫描引擎则采用了已经被市场广泛认可的业内领先的漏洞扫描引擎，以稳定提供精准且快速的漏洞发现



图一：渗透测试功能

交流提纲

信息安全部
Information Security

一、智能家居安全威胁分析

二、智能家居架构及安全防护重点

三、智能家居安全检测体系

四、智能家居标准与检测认证思路

智能家居相关技术规范与标准

CAICT 中国信息通信研究院 China Academy of Information and Communications Technology

智能家居目前还处于基于单个品牌构建解决方案的状态，厂商各自为战，缺少统一的接口和标准，无法做到互联互通。CCSA TC11 WG1已成立移动互联网+智慧家庭子工作组，重点研究智慧家庭领域中的系统架构、终端设备、平台、安全等方面的标准化工作。

国内智能家居平台/解决方案

- **互联网厂商**
  阿里物联平台、百度Inside、 京东微联、腾讯QQ物联…
- **家电厂商**
  海尔U+、美的M-Smart、苏宁私享家…
- **手机厂商**
  小米智能家居、华为Hilink…
- **电信运营商**
  中国电信悦me、中国移动魔百盒、中国联通智慧沃家…

国外智能家居平台/解决方案

- 苹果Homelink、三星Smart Home、Amazon、Google Nest、AT&T 、Verizon…

国际智能家居产业联盟

微软、英特尔、三星、高通等企业组成的OCF联盟是目前最受关注的物联网标准组织，正力图解决碎片化问题。先后兼并AllSeen、OIC等组织。另，谷歌、三星牵头的Thread联盟以及苹果Homekit等多个阵营，也在互联标准、云平台及开发组件上积极寻求突破

多架构体系---多应用协议---多业态渗透

海尔U+	ZigBee	家电厂商
美的	蓝牙	互联网厂商
格力	WiFi	手机厂商

	ZigBee	Z-Wave	AllSeen
Technical Foundation	IEEE 8.02.15.4	No International Standard	Technology Agreement of Software Layer
Founded-Union	ZigBee Alliance	Z-Wave Alliance	AllSeen Alliance
Use of band	2.4GHz	Sub 1G	Based on framework for all kinds of wireless communication technology, for example: Bluetooth, NFC...etc.
Transmission Distance	100m	50m	
Modulation Technology	BPSK, OQPSK	GFSK	
Node	65536	232	
Power Consumption	Idle: ~1 uA Rx: ~20 mA Tx: ~40 mA	Idle: ~1 uA Rx: ~20 mA Tx: ~40 mA	
IC Provider	TI, Freescale...etc.	Sigma Design	AllSeen Alliance

智能家居领域需要一个强大而开放的领导者，带领整个行业、企业，打通智能家居上中下游产业链，建立规范统一的行业、技术标准，共同建立、布局智能家居生态链，保障智能家居行业的健康、可持续发展。

CCSA TC11 智慧家庭子组
安全标准体系

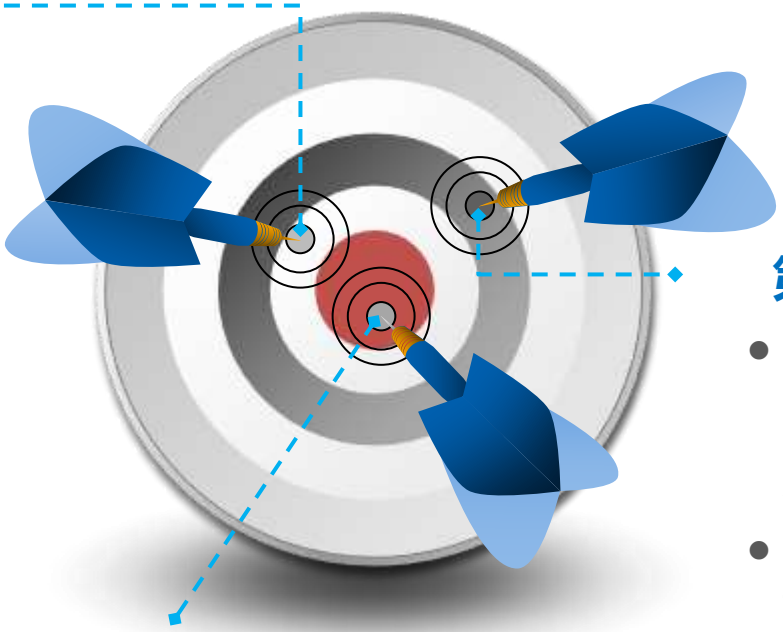
信息安全部 Information Security

推进检测认证的思路

CAICT 中国信息通信研究院
China Academy of Information and Communications Technology

国际、国内标准组织

- 跟踪国际国内相关标准，保持技术领先，建立国际交流与合作的平台
- 推进物联网终端安全相关技术和管理标准的制定和落实工作，加快标准的统筹与实施



第三方实验室

- 作为“国家物联网通信产品质量监督检验中心”，加强物联网终端的信息安全风险评估、安全检测及认证工作
- 发挥第三方实验室优势，为测试认证提供支撑，推动各类标准的迅速落地实施

行业协会、产业联盟

- CCSA行业协会成立智能家居子组，研究并制定相关技术标准，推进数据安全、隐私保护等体系建设
- 推动多种形式的产业联盟和资源共享平台，充分发挥产业界力量合力推进标准化，并加大物联网终端安全研究的力度

Q&A

信息安全部
Information Security