

智能家居产品的安全隐患及应对措施

姚碧
智能卡与安全事业部



英飞凌产品面向智能卡安全与嵌入式系统安全

智能卡方案

支付



- 智能卡支付
- 可穿戴支付

政府证照



- 电子护照
- 电子身份证
- 健保卡
- 电子驾照

交通票务



- 交通
- 票务

嵌入式安全方案

移动安全



- 嵌入式安全模块 eSE
- 移动通讯

工业与设施安全



- 车联安全
- 工业安全
- 运算、设施安全
- USB 令牌

互联设备安全



- 智能家居
- 配件设备认证
- 物联网设备
- 付费电视



目录

1

智能家居简介

2

风险分析

3

对策

4

展望未来

物联网趋势影响所有市场



智能化推动了利润的提升

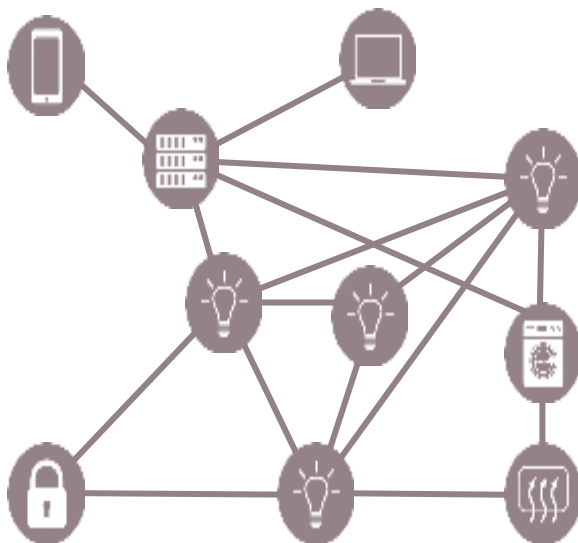


1 新的功能和服务

2 节能减排，提升效率

3 提高灵活性和定制化

智能家居设备的主要特性



- 这些特性均基于网络及网络中存储的数据

- 记录并分析数据
- 监测及报警
- 实时监控
- 远程控制
- 自动计划
- 节能
- 远程更新
- 出

目录

1

智能家居简介

2

风险分析

3

对策

4

展望未来

针对物联网的攻击日益增多



Software Cannot Protect Software: An Argument for Dedicated Hardware in Security and a Categorization of the Trustworthiness of Information

Matthew Judge, Paul Williams, Yong Kim, and Barry Mullins

Air Force Institute of Technology
2950 Hobson Way

Wright Patterson AFB OH 45433, USA

{matthew.judge,paul.williams,yong.kim,barry.mullins}@afit.edu



花火网 > 智能家居 > 新闻 > 正文

联网智能家居未设防护 黑客可轻松破解

2015-08-27 10:07:04 来源：互联网 编辑：小事

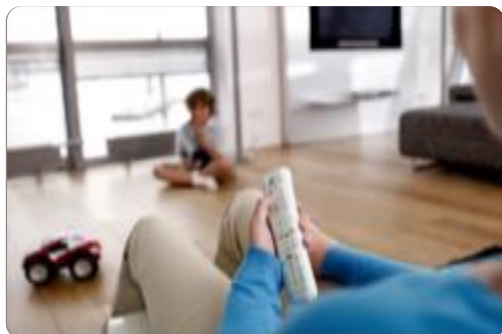
智能科技走进我们的生活，给我们的生活带来诸多乐趣，背后却也暗藏了许多信息危险。这些智能硬件都与互联网相连，只要有互联网就让黑客们有机可乘，据说他们甚至可以轻松破解大部分智能家电。

智能家居应用安全风险



产品安全风险

- 家电设备可能被操控全天候24x7运作，这可能导致产品过热和经济损失
- 电器设备的使用周期可能变短
- 产品向后台服务器端上传虚假数据，干扰服务器端的数据分析与决策



家庭安全风险

- 家庭成员的作息时间表可能被小偷收集
- 个人数据可能被盗用
- 网络监控摄像头存储的数据可能被篡改

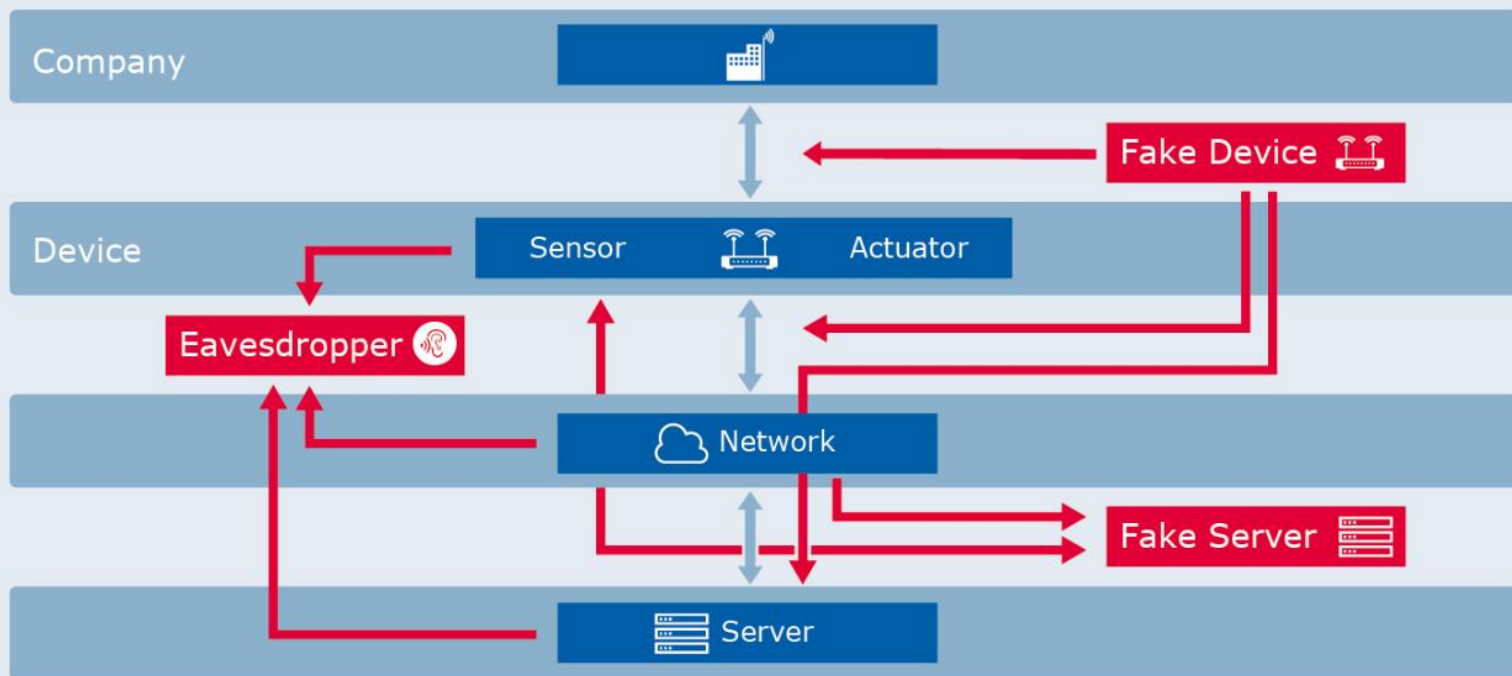


社会公共安全风险

- 时基操纵可能导致技术和社会问题
- 能源基建被操控

物联网系统中的每一层都可能受到攻击

物联网面临的安全威胁

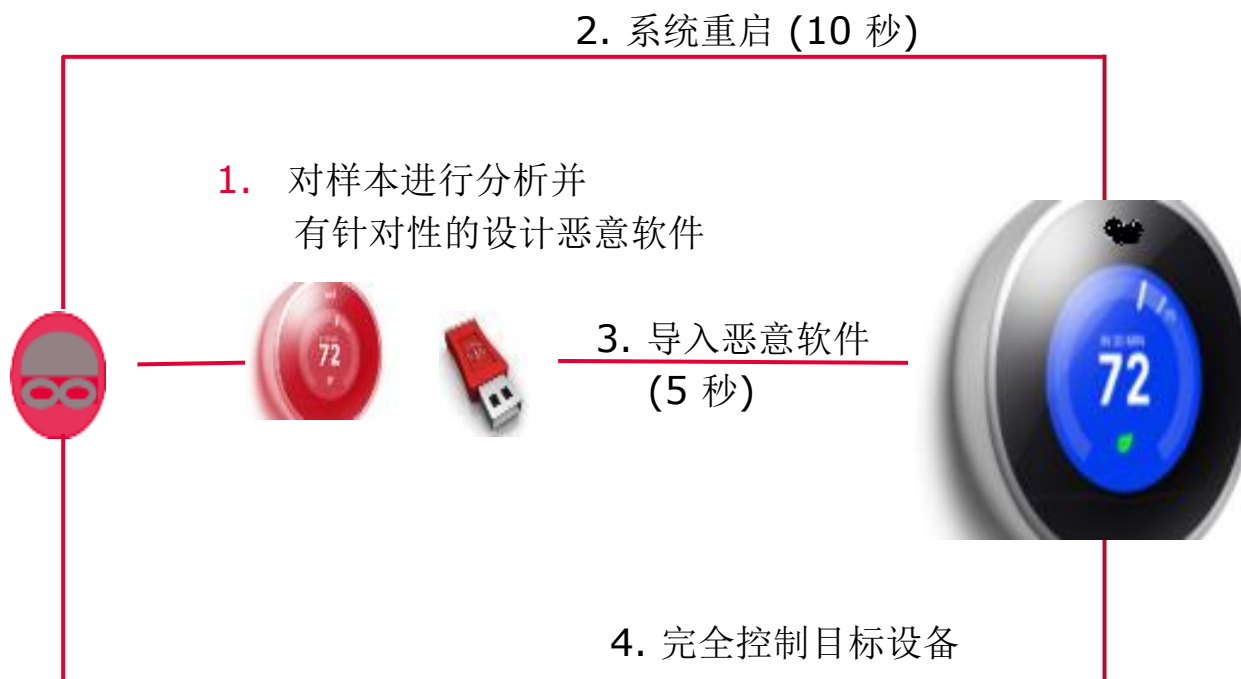


窃听数据或指令的**侦听者**可能泄漏关于基础设施运行的信息。

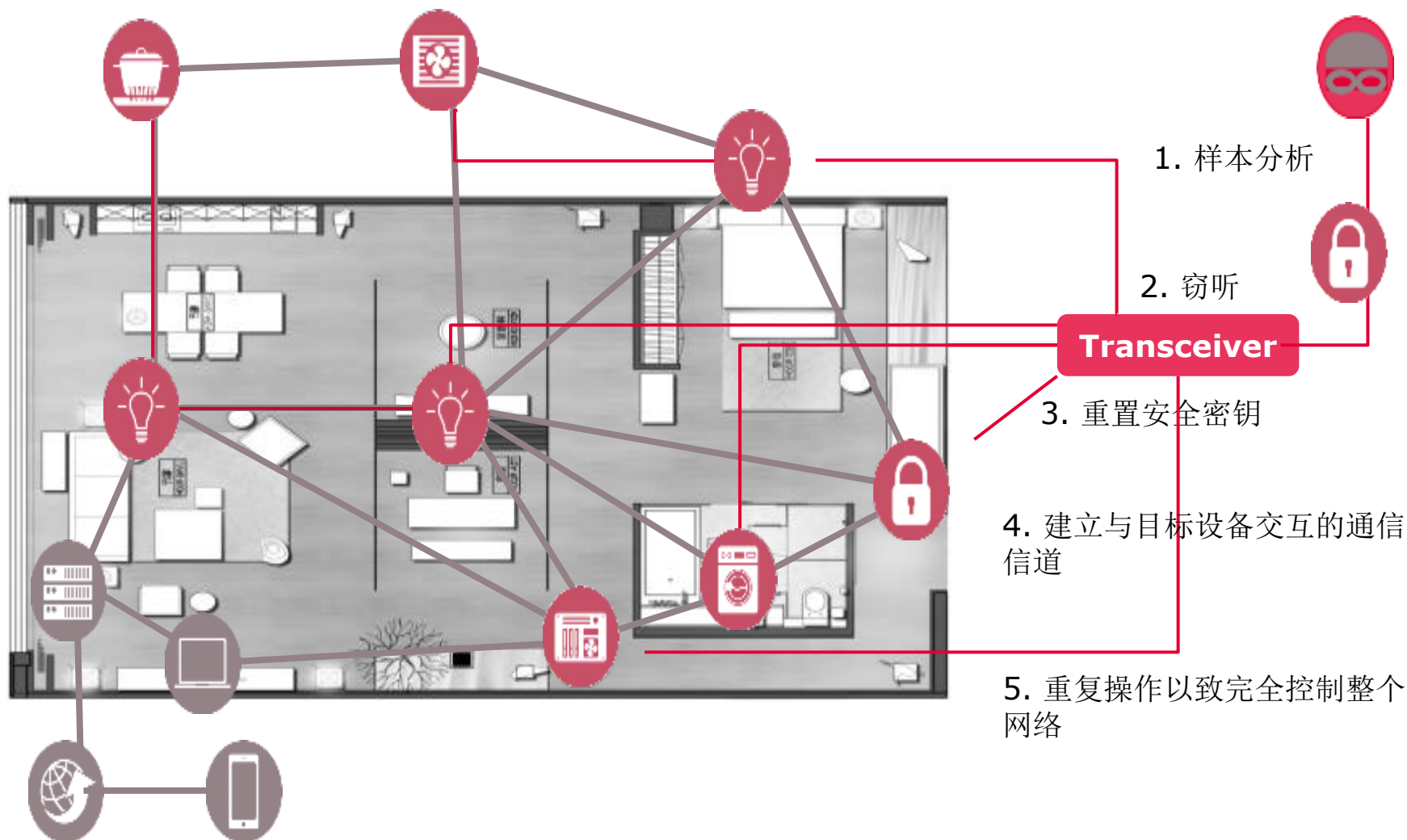
注入伪造测量数据的**问题设备**可以扰乱控制过程，使之做出危险或不当反应，或者可能被用于掩盖物理攻击

发送错误指令的**问题服务器**可能被用于触发非计划事件，将重要信息数据发送给非法接受方，诸如此类。

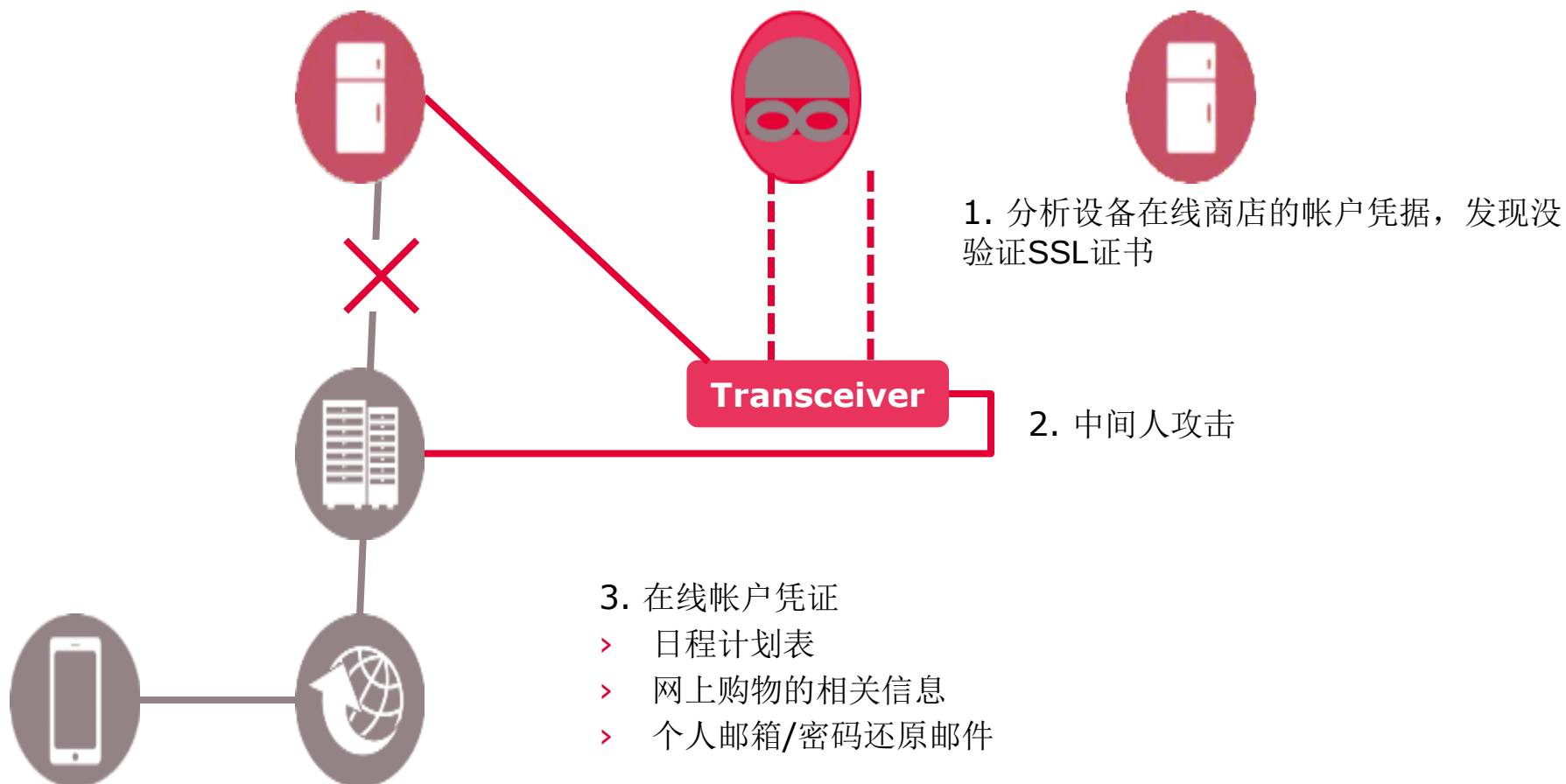
恒温器攻击案例



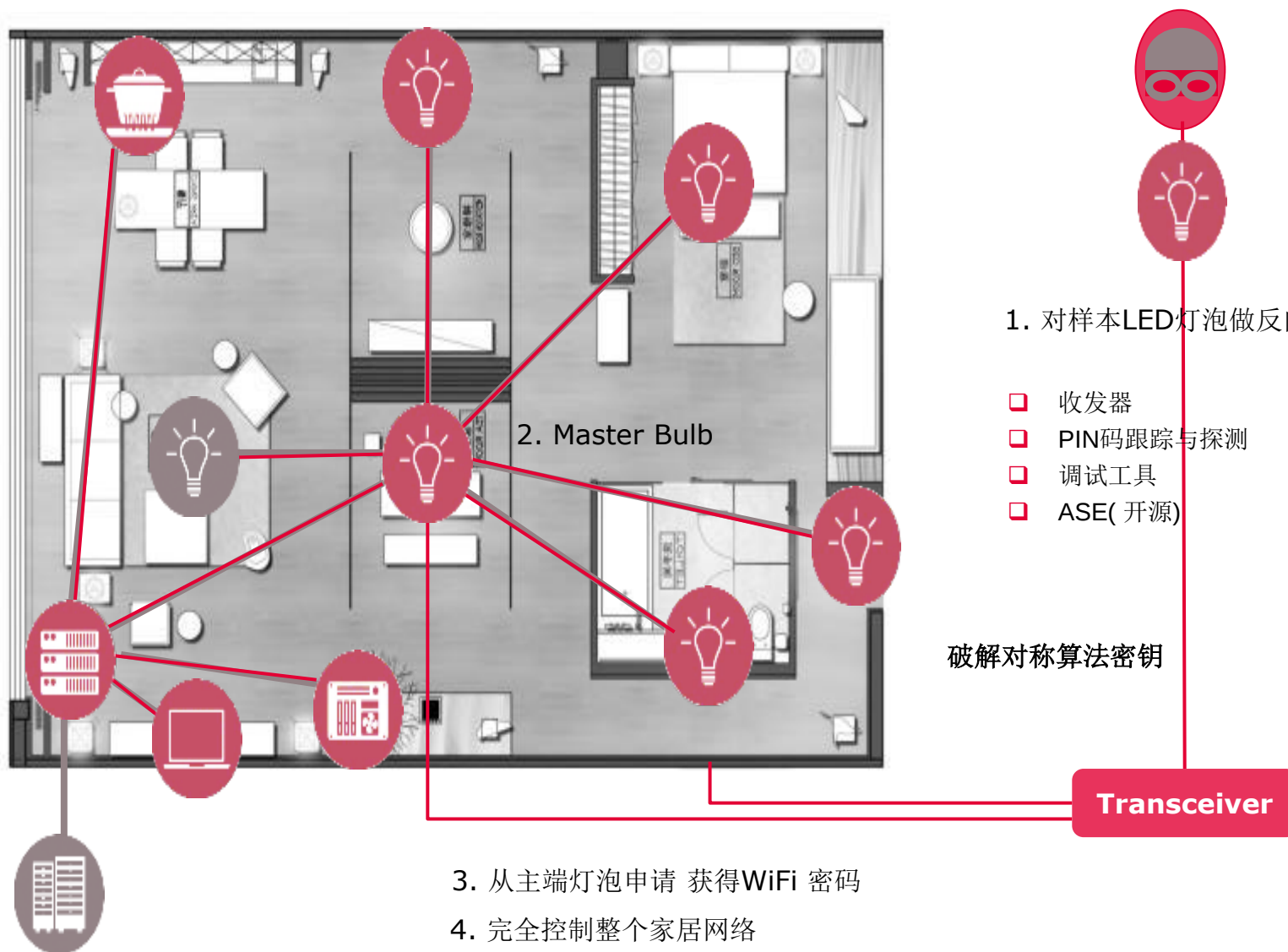
智慧锁攻击案例



家用电器攻击案例



智能灯具攻击案例



目录

1

智能家居简介

2

风险分析

3

对策

4

展望未来

物联网安全防护

常见安全防护措施



审计



密钥建立和管理



加密卸载



生命周期管理



平台完整性验证



认证



存储数据保护



安全通信

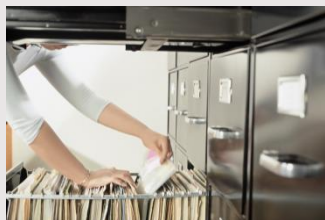


启动过程保护



安全软件/固件更新

物联网安全的实现方式



没有安全

所的内容开放给所有人



基于软件实现的安全

防御恶意指令与基础的软件攻击



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

可读性

软件代码易于访问与读取

硬件芯片保护自身代码不被读取

可复制

软件代码易于被复制并在黑客间分享

安全的硬件中的代码无法轻易的被复制，即便通过反向工程

可分析

借助标准工具软件代码易于分析与理解

安全的硬件基于专用的设计以及非标准的代码，所以不易于被分析与理解

信任根

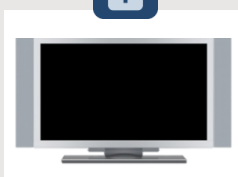
软件无法做到可信任的根，恢复受攻击的系统是几乎不可能的

安全的硬件可以为系统提供可信任根，实现监测、系统恢复与安全更新

智能家居同样需要各种不同级别的安全措施



家用电脑



智能电视



智能手机平板
适配器



游戏机



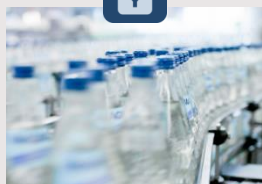
智能电源插座



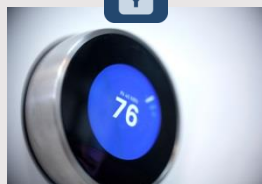
安全网关路由



智能表具



净水器



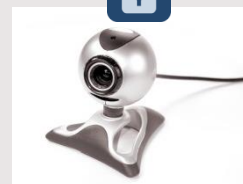
温控器



健康监控



数字门锁



IP 摄像头



物联网智能家居：英飞凌产品及方案

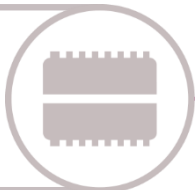
先进的感知能力

- › 麦克风（警报控制）
- › 3D霍尔传感器（智能电表）/霍尔开关（位置）
- › 雷达（导航），压力传感器（燃气表）



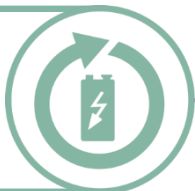
多功能控制

- › XMC™ 微处理器（控制，通讯及传感器管理）



高效率电源管理

- › IGBT, 驱动, DC/DC: FETs, IPMs, PoLs; AC/DC（冰箱，洗衣机或空调SMPS控制模块）

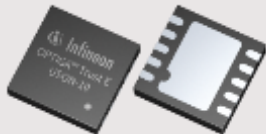


可信安全保护

- › OPTIGA™ Trust（设备认证）
- › OPTIGA™ TPM（服务器和网关间加密通信）



OPTIGA系列针对物联网提供根信任解决方案

	OPTIGA™ Trust B	OPTIGA™ Trust	OPTIGA™ Trust E/X	OPTIGA™ Trust P	OPTIGA™ TPM
					
安全等级	+	+	+++	基于 EAL 5+	EAL 4+
设计复杂度	易	易	易	中等	中等
主要应用	认证	认证	支持PKI认证	通用可编程	TPM标准
交钥匙型方案	✓	✓	✓	可编程	✓

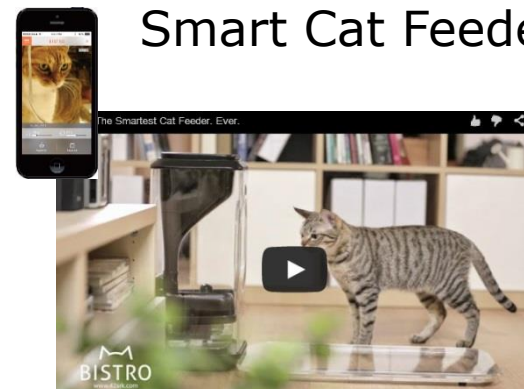
安全性及复杂度

OPTIGA™ Trust在产品设计中的创新应用

i-FlashDrive



Smart Cat Feeder



技術規格

NextDrive Plug 無線擴充座使用 LinkNext Technologies 物聯網技術，結合世界一級大廠元件，包含 ARM Cortex A9 1Ghz CPU、Broadcom Wi-Fi 與 Bluetooth 模組、及 Infineon 加密晶片。做為物聯網中的智慧網關 (IOT Gateway)，NextDrive Plug 能透過 Wi-Fi 為手機和平板電腦連結多種 USB 裝置，帶來強大的擴充力。

ARM CORTEX A9 1GHz CPU

BROADCOM Wi-Fi AND BLUETOOTH MODULE

INFINEON AUTHENTICATION CHIP

INPUT 100V~240V OUTPUT 5V 2A POWER MODULE

OPTIGA™ TPM为谷歌智能家庭网关OnHub提供安全

Infineon Brings Certified Security to Computing and Emerging IoT Applications: OPTIGA™ TPM 2.0 First to Receive Common Criteria Certification

Sep 25, 2015 | Technology Media

Munich, Germany – September 25, 2015 – Certified security solutions from Infineon Technologies AG (FSE: IFX / OTCQX: IFNNY) enable protection of data, devices and networks in both mainstream computing and the emerging Internet of Things (IoT). The leader in Trusted Computing today announced that

device to comply with international

› [German Federal Office for Inform](#)

certification is an independent third

With Common Criteria certification

personal computers be equipped with

11889:2015) also addresses the security

hardware provides robust protection

connected industrial and automotive



智慧家居互联安全开放实验室

美的携手行业巨头成立智慧家居互联安全开放实验室

2016-11-24 17:20:59 来源: 网易家居

▲ 举报

分享到:       

 0

11月24日,“智慧家居互联安全开放实验室”在北京揭牌成立,该实验室由美的智慧家居科技有限公司(以下简称“美的智慧”)、中国电子技术标准化研究院(以下简称“电子标准院”)、华为消费者BG(以下简称“华为”)、英飞凌科技(中国)有限公司(以下简称“英飞凌”)、腾讯科技(北京)有限公司(以下简称“腾讯”)五家单位联合发起。发布会当天,美的智慧、电子标准院、华为、英飞凌、腾讯的领导共同为实验室揭牌。



中国电子技术标准化研究院
China Electronics Standardization Institute



Tencent 腾讯

英飞凌安全芯片为美的智能WiFi模块提供安全

英飞凌携手美的为安全智能家电提供智能WiFi模块

中电网 2017-03-10 16:04:26 美的 智能家电 物联网  阅读(117)  评论(0)

声明：本文由入驻搜狐公众平台的作者撰写，除搜狐官方账号外，观点仅代表作者本人，不代表搜狐立场。

[举报](#)

智能家电中的程序漏洞可能让您的的人身安全处于危险之中。黑客们会找出联网智能家电中的漏洞，给家庭用户带来风险：他们可以偷窥个人密码，对您的居家生活了如指掌，甚至远程操控家用电器。英飞凌科技股份有限公司（FSE: IFX / OTCQX: IFNNY）今天携手美的智慧家居开发出了新一代智能WiFi模块，可有效保护数据传输，当智能家电启动时对其进行身份验证，当其联网或互相之间传输数据时确保信息的安全。



目录

1

智能家居简介

2

风险分析

3

对策

4

展望未来

智能家居安全可能的未来发展

› 额外功能

- 扩展安全特性
- 扩展加密算法

› 与智能家居系统紧密集成

- 所有智能家居系统均实现硬件信任根标准
 - 同如今的信息技术和支付系统一样

› 对更强大的安全性的外部要求与日俱增

- 条例、保险，等等

› 持续的攻防角力

总结



智能家居前景光明



要保护我们的价值，必须实现强大的智能家居安全



可灵活扩展的硬件根信任能保障智能家居的安全



英飞凌：保障物联网安全的首选合作伙伴

英飞凌安全控制器全球出货量逾**200亿**

2014年发行的每**10**张支付卡中有**4**张采用英飞凌安全芯片

全球**61**个国家，共**75%**人口的政府证照由英飞凌芯片驱动

英飞凌是移动**M2M**通信的先驱和绝对领袖

每两台商务便携式电脑中有一台配备英飞凌提供的可信平台模块（**TPM**）





Part of your life. Part of tomorrow.

