

IoT安全的To B与To C

王滨 海康威视CSO





IoT设备包括哪些？

IoT 2019

工业智能机器人
家用路由器
摄像头
心脏起搏器
自动驾驶汽车
智能家居
心脏起搏器
手环
各种传感器
智能音箱
智能窗帘



公众眼中的IoT安全

IFT 2019

央视曝光大量家庭摄像头遭破解，防止隐私泄露做到这几点很重要

11月5日
2018年 11月26日 13:25

众所周知，随着智能电子设备的快速发展，一些新兴的黑科技产品逐渐进入普通家庭的生活。例如家用摄像头，因其能够远程监控的优点，被许多家庭都安装了智能摄像头。即便出门在外，也可以用手机随时查看家中的一举一动。这对于照顾老人、小孩、宠物以及防止家贼方便。

细思极恐，当你的车辆被黑客远程控制

2018-05-23 11:03:27

今年3月美国爆发一起窃案，犯罪分子通过远程控制车辆，阻止车主去银行取款。



搜狐健康 > 健康养生 > 健康新闻

黑客控制心脏起搏器杀人？安全专家称可以实现

正文 数据新闻(7人参与) 2018-05-23 11:03:27

科技前沿 > 安全 > 网络安全

原标题：黑客控制心脏起搏器杀人？安全专家称可以实现

【北京5月23日电】(记者 孟祥 刘博) 最近有报道称，黑客能够通过控制心脏起搏器，远程控制人于心脏起搏器植入患者的心脏起搏器，在特定的场景中，黑客

中国网·中国

滚动

女孩萌萌时戴运动手环 全程被监测 盘点谁要被偷窥的尴尬场面(图)

2018-05-27 15:00

来源：网络(作者：空位) | 1

滚动新闻 > 新闻

亚马逊旗下智能音箱存在漏洞可被变成黑客的监控工具

2018-05-23 11:03:27 来源：网络(作者：空位) | 1

正版软件商城

买正版软件就上APSCO软件



立即购买

【北京5月23日电】亚马逊公司最近公布其旗下的人工智能语音助手Alexa存在严重的安全漏洞，黑客可以通过远程控制Alexa设备，将其变成黑客的监控工具。亚马逊公司表示，黑客可以通过远程控制Alexa设备，将其变成黑客的监控工具。亚马逊公司表示，黑客可以通过远程控制Alexa设备，将其变成黑客的监控工具。





安全研究人员眼中的IoT安全

IFT 2019

黑客只要三步就能操作你的网络摄像头!

2017-01-03 16:27

1 先查到了

2 至于如何搞定

3 后面这些就是

4 其实我们每

5 全球几百万摄像头在

6 输入默认的账号密码, 最少百分之80的是没改密码的!

ZoomEye

http://www.sonu.com/a/123283355_266823

- 弱口令
- 暴露在互联网上
- 漏洞

http://www.sonu.com/a/123283355_266823



IoT安全的ToB&ToC

IT 2019

ToB : 弱口令、漏洞、暴露在互联网上

ToC : 弱口令、漏洞





ToC—设备可以不暴露在互联网上

FIIT 2019





ToB—设备大量暴露在互联网上

FIIT 2019

- 本身为了应用的需要暴露在互联网上
- 设置不当导致设备暴露在互联网上





IoT设备安全永远的痛--弱口令

IT 2019

用户：**安全意识淡薄，亟待提高**

厂商：**早先的产品存在密码硬编码/未使用更加健全的口令机制**

国家信息安全标准委员会 (TC260)

《信息安全技术-智能联网设备口令保护指南》





IoT设备安全无法回避的问题—漏洞

IFT 2019





ToC安全该怎么做？

IT 2019

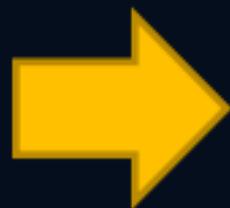




ToB安全该怎么做？

IT 2019

- 设备需要开放多种端口
- 用户安全意识普遍不高
- 系统网络环境复杂多样
- 纵深防御很难有效实施
- 历史累积问题堆积如山



- 厂商提供更高产品安全要求
- 为用户提供轻管理的安全防护方案





IoT设备漏洞的几点呼吁

IoT 2019

- 目前业界遵循的90天的漏洞披露策略对于无有效升级途径的物联网设备并不适用；
- POC的检测更推荐采用版本检测的方式；
- 用户设置周期性固件更新计划任务，弱口令一定要避免；
- 厂商加强设备的安全设计、开发、测试和应急响应；
- 行业主管机构必须要有强制的检查和通报机制



REEBUF | FIT

THANKS