安全小课堂第140期【浅谈IoT系统的攻击与防御】

JSRC 京东安全应急响应中心 1周前

万物互联的时代正在来临，据不完全统计,全球物联网设备已达到70亿+，同时每年以20%左右的速度增长。
从智能家居、智能生活到智慧城市，IoT设备早已深入人们的生活，为大家提供更高品质的生活服务，如常见的路由器、摄像头、音箱、智能插座、温控器等。
黑客入侵，设备被控制，隐私数据被窃取等情况会严重影响我们的生活。本文从IoT系统风险、攻击手段、防御方法方面浅析相关安全建设，知己知彼，做好安全防御建设。

JSRC小课堂第140**期**，邀请到**Double哥（京东安全工程师，主要从事系统安全、IoT 方面的安全架构与实现）**就IoT系统的攻击与防御为大家进行分享，同时感谢白帽子们的精彩讨论。

IoT的场景下安全风险风险有哪些?

AI + IoT给社会提供了更多的智能应用方案，提高了社会生产效率，降低了社会成本，驱动着社会高速发展。

像计算机一样，IoT设备同样会受到攻击，黑客可能直接进行攻击，或者通过控制IoT设备的应用程序间接进行攻击，亦或直接在设备端进行入侵。黑客通过攻击 IoT 设备，来窃取数据、勒索企业，或者远控IoT设备执行大规模分布式拒绝服务 (DDoS) 攻击。

据某媒体报道，市场上的几款颇受欢迎的智能汽车报警系统存在重大安全缺陷，使得潜在的黑客能够跟踪车辆、打开车门，在某些情况下还能切断引擎。安全厂商通过安全测试进行验证，发现汽车警报系统确实存在被远程利用的风险，使潜在的攻击者能够劫持车辆并监视驾驶人员。

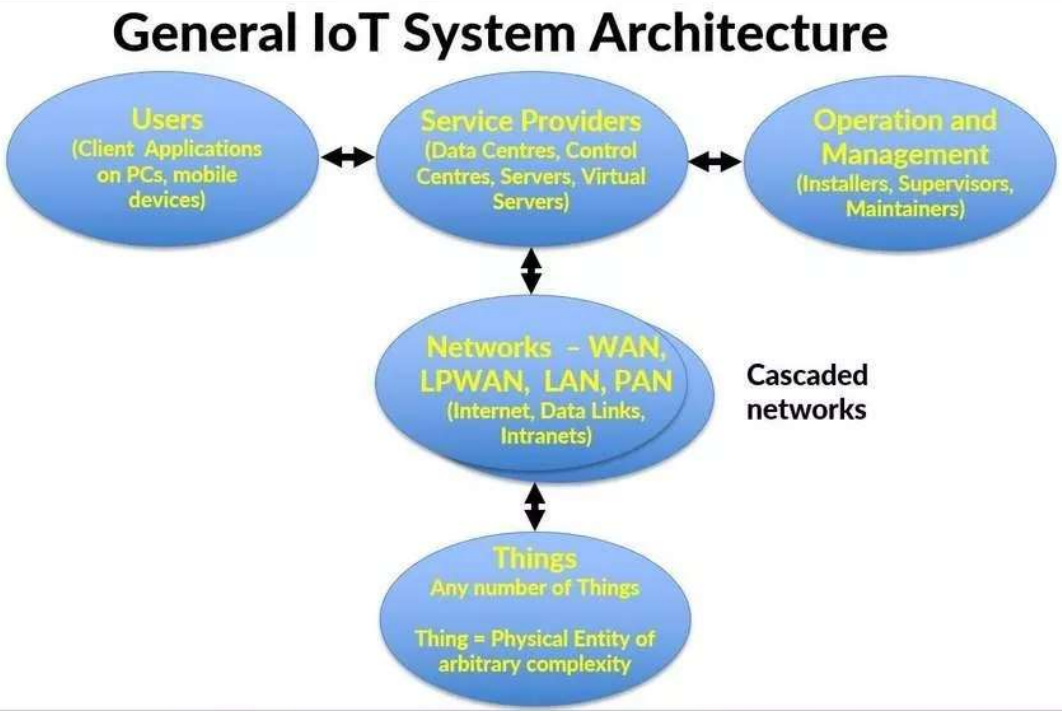
历史上一次大规模的分布式拒绝服务 (DDoS) 攻击导致互联网 DNS 服务供应商瘫痪，GitHub、Twitter、PayPal等多家公司网站不能正常访问。攻击的背后是一个庞大的僵尸网络，其中包括近20万个IoT设备。

想象一下，辛苦一天的“路人甲”，带着疲惫的身体跨入家门时，温暖的灯光伴随着温馨的音乐，空调调到合适温度、加湿器和空气净化器提前10分钟进入工作状态，洗澡水开始加热，小厨机器人正在烧制可口晚餐。

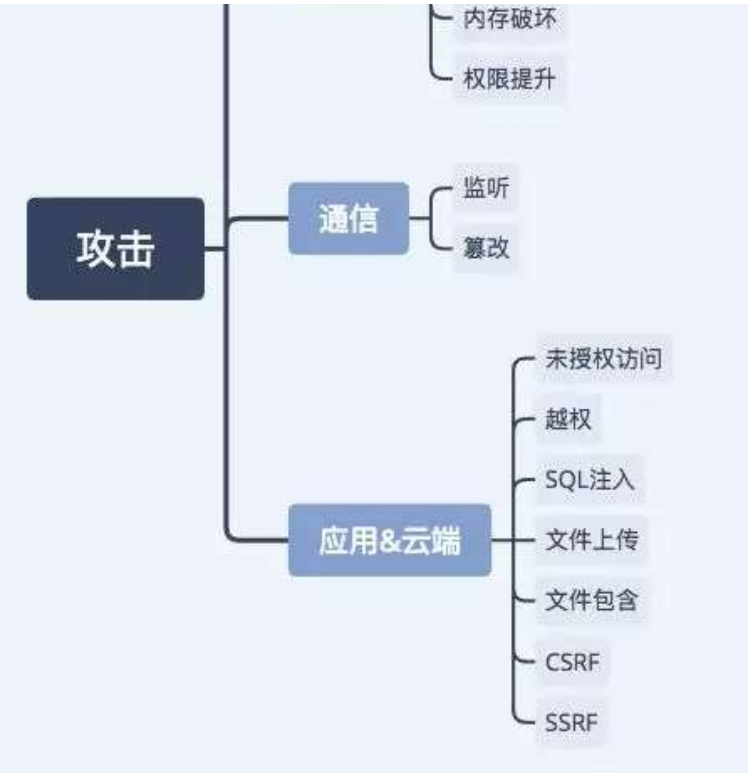
21世纪的我们幸福满满.... 然而这一刻有可能戛然而止，有个蒙面人在非法控制着一切.... 设备被劫持、被远程控制，个人隐私、个人数据被泄露....

IoT场景下的常见攻击手段有哪些?

那么黑阔这么厉害，危害和影响那么大，他们是如何做到的呢？是通过什么样的手段入侵 IoT 系统?



常用的 IoT系统架构如上图所示，通常分为设备端、应用端、云端和通信，在各层都有不同的入侵方法。



在设备端，可以通过Firemware、NVRAM挖掘出重要的信息，如系统口令、系统配置，直接拿下设备权限。或者通过修改 Fireware，篡改功能和配置，重新烧进设备。也可以通过主板上的调试接口，动态调试或观察运行日志，来分析系统薄弱点，在进行定向攻击。当然，如果运气好的话，也有可能通过这个接口直接访问设备，获取控制权限。

在应用端，我们可以Hook或篡改 APP 应用，向设备发送伪造的控制指令，获取设备的控制权限。

云端应用和传统的 Web 系统攻击方法是相同的，基本上都是OWASP Top 10， IoT 的云端非常常见的问题主要是越权、未授权访问等。

网络侧主要是中间人攻击，嗅探敏感信息，或篡改系统关键信息。

IoT场景下安全防御方法有哪些?

IoT系统在每个层次都必须采取有效的安全措施来阻止黑客，建立完整的安全体系以保障IoT系统的设备安全、系统安全、应用安全和数据安全。如硬件侧需要设计最小化系统，并且对硬件、软件进行度量，校验设备的真实性和完整性，确保处于可信的基础运行环境。

操作系统层面要进行系统加固，构建基础可信运行环境，监控和阻止攻击行为，防范漏洞利用方式入侵、提权，对于系统或应用产生的漏洞能够快速修复。

应用系统需要有可靠的验证身份体系，防范身份伪造的情况或冒用。涉及数据交换与通信，要确保传输数据的机密性和完整性，防范中间人攻击，窃取和篡改数据。

系统开发过程按照SDL进行实施，进行威胁建模、代码安全检查(白盒)、黑盒安全测试、上线安全审查、线上安全监测。

设备采集的日志数据，进行安全检测，运营人员对于产生的告警与事件，及时进行跟踪处理，及时发现安全威胁，推进强化系统安全建设。

IoT安全建设的“坑”有哪些?

建设IoT安全系统的同时要确保避免影响到用户体验，以及对于系统稳定性、可用性方面的影响。

这是JSRC小课堂陪伴你的

第3年107天

如果有你希望出现在安全小课堂内容暂时未出现

欢迎留言告诉我们

如果有所收获欢迎将它分享

让更多的人加入JSRC安全小课堂

交流

QQ开课群：464465695

留言：针对本期主题内容，你还有什么疑问吗？欢迎留言交流~

JSRC