新形势下物联网终端安全发展趋势

刘陶 | 2017-08-31 11:56

新形势 物联网 安全 发展趋势

【数据猿导读】随着智能硬件技术的兴起，近年来物联网市场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年全球物联网设备数量将高达260亿件。与此同时，物联网安全事件呈爆发增长态势，安全威胁不断恶化。

随着智能硬件技术的兴起，近年来物联网市场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年全球物联网设备数量将高达260亿件。与此同时，物联网安全事件呈爆发增长态势，安全威胁不断恶化。多国开始从战略、标准、监管等各层面提升对物联网安全的重视等级。2016年年底，美国国国土安全部发布了“保障物联网安全的战略原则”，国土安全高级官员公开表示“物联网安全已演变成为国土安全问题”。与此同时，欧盟也宣布加快物联网安全规范的制定步伐。2016年世界物联网博览会信息安全高峰论坛上，中国工程院何德全院士指出，物联网是我国信息产业发展难得的机遇，相对互联网，物联网是一个更加复杂、更加多样、更大跨度的系统，要充分考虑其安全问题。

1. 物联网终端安全威胁发展趋势

(1) 针对物联网设备的攻击威胁将呈指数级增长

根据Gartner预测，从现在开始到2018年，超过半数物联网设备制造商将由于薄弱的验证实践方案而无法保障产品安全。物联网设备目前在制造过程中仍然很少考虑到安全性需求，而且由于其存在于网络环境中，因此一旦出现恶意入侵，其很可能造成网络受损及数据泄露，甚至给用户带来直接的财产损失或人身伤害。

(2)海量物联网终端将逐渐成为DDoS攻击主要来源

物联网设备已成为僵尸网络的主要载体，已可形成超高容量的DDoS攻击源，目前这些大规模僵尸网络已经不需要利用反弹/放大技术，即可对银行、电信、政府等大型系统进行攻击。物联网 DDoS攻击的规模、频度、复杂性、影响和损失正快速增长。2016年年底，由Mirai病毒引发的物联网DDoS攻击事件显示国家层面关键基础设施也逐渐成为重点攻击目标之一。

(3)贴近用户的物联网终端将成为隐私泄露的重要渠道

精品栏目

[2017/07/27] 大数据24小时 More>
[2017/07/24-28] 大数据周周看 More>
[2017/07/24-28] 大数据投融资 More>
[2017/07/24-28] 大咖周语录 More>
[2017/07/24-28] 大数据周聘汇 More>
[2017/07/24-28] 每周一本书 More>
[2016/08-10] 大数据活动公告 More>

专家推荐 More >


涂子沛

傅志华

马亮

苏萌

崔晓波

韩涵

车品觉

刘雷鸣

董飞

郭炜

张涵诚

陈运文

人物专访 More >

活动推荐 More >

ACS 2017中国汽车CIO峰会10 2017-10-25
2017金融科技价值—数据驱动 2017-10-19

由于大多数物联网设备是7×24小时实时不断地产生数据，在物联网系统中，设备之间的通信可以不需要人的参与，一些带有用户隐私信息的数据很容易被攻击者非法获取。攻击者可以通过入侵联网家用设备获取用户是否在家或生活规律等敏感信息，严重者可直接给用户带来严重财产和人身安全威胁。

2. 物联网终端体系架构及安全风险分析

目前物联网系统在信息安全防护方面能力分布并不均匀，呈现"重平台、轻终端"的态势。后台业务管理平台与云计算或传统服务器系统区别并不大，一般在设计之初就考虑了信息安全问题，防护措施也有相应规范标准，而感知层各类终端由于数量众多或资源技术能力的限制，防护能力普遍较弱，成为物联网系统信息安全的薄弱环节。物联网系统面临的主要安全风险可分为以下几类：

(1)软件漏洞。许多物联网终端设备在出厂的时候，其装载的软件就已经"过期"，或即将过期。即使有些设备出厂的时候装载的是最新版本软件，但由于未及时更新，也可能在未来出现漏洞。因此，除非拥有持续的软件更新机制，物联网终端设备存在的软件漏洞风险极高。

(2)不安全的通信。由于目前许多安全防护功能都是为更加通用的计算设备设计的，由于计算资源或系统类别的限制很难在物联网上实现，但是物联网上许多安全缺陷已经被发现。例如，采用缺乏加密的通信机制，许多物联网设备都是部分或全部明文传输;缺乏成熟的授权或认证机制，许多物联网都未对代码或配置项变更进行权限限制，一些恶意敏感操作或数据未授权访问都非常容易发生;缺乏网络隔离，一些家庭内网络很少进行网络分段隔离或防火墙设置，使得物联网设备极易遭受同网段病毒感染、恶意访问或操控。

(3)数据泄露。物联网系统泄露用户隐私数据的风险较高。主要存在云端、物联网终端设备本身两个来源的泄露风险。一方面，云端服务平台可能遭受外部攻击或内部泄密，或者由于云服务用户弱密码认证等原因，均有可能导致用户敏感数据泄露;另一方面，设备与设备之间也存在数据泄露渠道，在同一网段或相邻网段的设备可能会查看到其他设备的信息，比如屋主名字，精确的地理位置信息，甚至消费者购买的东西等。

(4)恶意软件感染。恶意软件可能会影响物联网设备的操作，获取未授权的访问，或者实施攻击。例如引发大规模DDoS 攻击的Mirai、BASHLITE、Lizkebab、Torlus、Gafgyt等。除了被用于拒绝服务攻击，被这些病毒感染的物联网设备还可用于窥探他人隐私，勒索所劫持设备，或者被利用作为攻击物联网设备所连接的网络渗透的入口。

(5)服务中断。可用性或连接的丢失可能会影响物联网设备的功能特性，一些情况下还可能降级安全性，例如楼宇警报系统，如果连接中断的话，即会直接影响整体的安全性。

3. 物联网终端安全防护及监管建议

物联网安全问题已受到产业链各方的广泛关注。针对目前物联网发展所面临的安全问题，我们应做好顶层设计，产业链各方应采取措施积极应对。

(1)通过标准、最佳实践引导产业链厂商提高物联网产品自身安全性。

应倡导物联网产业链各环节厂商针对自身特点采用最佳安全实践方案，提高设备自身安全防护水平，提供更加安全的物联网应用服务。同时应积极加快标准制定，为设备制造商提供开发过程中的最佳实践指引。另一方面，物联网设备安全很大程度上还取决于供应链安全，通过法律、规范、标准明确从制造商到零售商应如何采取措施进行安全防护，保证物联网产品整个生命周期的安全，这也是需要考虑的重点问题之一。

(2)通过检测认证、实时监测、定期评估等手段提高物联网应用的安全防护能力。

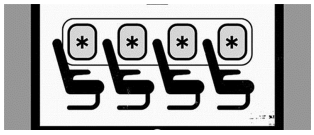
一方面，企业应积极利用安全框架来检测各物联网设备类型的风险，并对其加以有效控制。如应建立完善的入侵检测防护机制，检测恶意节点行为，对异常入侵行为进行及时拦截和纠正，从而避免

或降低各类攻击的负面影响。另一方面，应积极引入第三方测试、评估、认证机制，对物联网产品、应用、服务，进行可信赖的、权威的、有依据的安全保障，其中终端固件应为安全测试评估的重点内容之一，由于物联网自身特点，芯片内部的软件与控制它的应用一样重要。它们都需要进行安全和质量测试。再一方面，国家层面的态势感知和预警响应平台也是需重点考虑的目标之一。可以预测未来几年内数以亿计的物联网设备将会覆盖各类行业应用，跟踪何种设备置于何处，提前预知漏洞/攻击可能的影响面和范围对于国家关键基础设施安全也至关重要。

来源：人民邮电报

相关文章

刷新


数据安全：科学家采用多种手段保护研究数据


报告显示，人工智能对物联网的重要性超过了大数据分析


大数据周周看：亚马逊推出基于AI的云安全服务，投资达20.8亿...

我要评论

我想要评论.....

提交评论

ok

北京丨数据堂 大数据架构师&大数据分析
北京丨聚合数据 业务拓展经理&JAVA工程
北京丨慧米数据 三个职位
湖南丨银杏数据科技有限公司 数据工程师
北京丨中献电子技术开发中心 大数据分析

大家都在搜

陕西 百度 python 医疗
大数据 人工智能 融资
机器学习 互联网+ 数据挖掘
电商 追随 物联网 北京
创业 小米 阿里巴巴
云计算 营销 大数据
互联网 科技部 金融
机器人 数据分析 春节
漏洞 中国 投资
大数据应用