物联网关键技术分析及安全策略

杨 勇
（江西省邮电规划设计院有限公司，江西 南昌 330002）

摘 要：在现代无线电通信世界中，物联网的产生与发展正引领着一场新型的数字工业革命。无论是智能电视、传感器与智能手机，还是汽车、显示器等控制设备，均可以在连接互联网的情况下实现技术与应用方面的创新进步。本文以物联网关键技术与安全为探讨主题，分析物联网的概念与关键技术，从模块化的硬件和软件组件、带宽提速以及漏洞管理等方面阐述应对安全问题的有效策略。

关键词：物联网；关键技术；安全策略
中图分类号：TP391.4　　**文献标识码**：A　　**文章编号**：1004-7344(2021)12-0257-02

0 引言

在全世界范围内，越来越多的物联网设备投入到各行业领域的使用中，以无人操控设备、IP 支持设备为代表的事物对网络与无线通信技术加以灵活运用，实现设备小型化，在大数据分析与电池技术的支持极大地拓宽了应用发展领域。尽管物联网的广泛应用为人们的工作生活带来较大便利，但其也面临不可忽视的安全缺陷问题，科学处理安全隐患是技术发展需要关注的重点课题。

1 物联网技术概述

1.1 物联网定义

从简单定义的角度上来看，物联网属于一个系统，其不仅包含多样化的连接设备，还含有具有相互通信功能的各种网络，借助于相应的技术手段实现二者的有效连接。本质意义上，其也是一个架构框架，以现有的网络基础设施为基础，形成物理世界，然后集成计算机系统，达到相互交换数据的目的。在架构方面，有国际电信组织对物联网的体系结构进行明确规范，详细划定出感知层、网络层与应用层，但若对其内部构成进行详细划分，还可以划定接入层与中间件层。

1.2 物联网的关键技术

在整个物联网技术体系内，关键技术主要包括以下几部分：

(1)射频识别技术。借助无线电波，将个人身份或指定对象内容进行无线传输，是射频识别技术的主要原理。这种系统采用序列号形式，不仅可以将日常设备与物品连接到互联网，还可以将其与大型数据库、网络相连。作为一种高效的物品识别系统，其一方面体现出良好的成本效益，另一方面技术原理也十分简单，确保有关事物的相关数据信息得到妥善的收集与处理。

(2)传感器技术。在信息收集方面，传感器具有重要作用。对于 IoT 而言，软件起到大脑的功效，而传感器则代表着关键的神经系统，其主要负责收集、处理连续的数据流。除了 RFID，要想实现对环境变化的精准记录，还需注意到对事物物理状态变化情况予以检测的实践能力，以事物所处环境为基础，利用传感器进行数据收集，并产生有价值的数据信息，有利于人们增强对环境的全方面认识[1]。

(3)智能嵌入技术。利用事物自身的智能嵌入式，向网络边缘分配处理能力，一方面能够使网络弹性大幅增加，另一方面可以有效拓宽数据处理功能发展的可能性。与此同时，这也在一定程度上代表着将独立决定能力附加到网络边缘的设备，以及相关事物上。在面对来自外部环境的刺激作用时，其反应能力、处理能力均显著增强。

(4)小型化与纳米技术。将交互、连接能力赋予越来越小的事物，是发展小型化与纳米技术的主要特点，近年来，许多现实应用领域均逐步加快对纳米技术的应用，常见的包括农业工业、生物技术等，除此以外，还涉及生物医学与军事领域。依托于对小型化与纳米技术的充分利用，带来更多多元化的高级发展解决方案，器件的开发尺寸也实现了一到几百纳米的有效跨越。

2 物联网安全问题与应对策略

2.1 模块化的硬件和软件组件

在连接设备时，物联网需要重点考虑到其功能性、供应商的复杂性。无论是生产日期、技术接口，还是软件版本与比特率，不同设备之间均可能存在较大差异，在功能设计方面，对应的也是完全不同的对象。由此可见，协议的设计需满足处于不同工作状态下各种设备的运作需求。通过分析与观察当前计算机与网络安全的相关策略可以发现，其对于物联网的发展特点并不完全吻合。为了有效应对安全问题，可以研究模块化的硬件和软件组件为着手点，实现对互联网连接设备各个模块、部件的有效把控。一方面在攻击者试图对物联网设备供应链进行破坏时，起到有效的预防与警示作用，另一方面防止出现其他漏洞，或被植入恶意代码。针对企业环境的具体情况，完成设备的部署工作。对于企

业来说，可以向自己的网段隔离此类设备，将嵌入式系统与微内核结合使用，或是引入虚拟机管理程序的相关技术，在后续的运行管理过程中，一旦有安全漏洞问题的发生，能够在短时间内实现系统隔离[2]。

2.2 带宽提速

近年来，各种各样的社交网络平台得到快速发展，形成点对点的应用模式，随之而来的则是大幅激增的网络流量。在未来的发展阶段内，互联网上必然会连接越来越多的应用设备，因此网络流量的增长幅度也会逐年升高，整个社会环境不断增加对互联网的应用需求，也会使业务面前的连续性风险愈发显著，对于关键性的应用程序而言，若获得的带宽难以满足自身的运行需求，便无法向消费者或使用者提供良好的应用体验，这种问题的存在不仅会削弱生产链的生产能力，也会影响企业的盈利能力[3]。

要切实提升网络服务的高效性、实用性，企业应对带宽提速问题予以重点关注，一方面结合自身的经营需求适当增加带宽，另一方面实现对流量的有效监控与管理，这样可以降低业务面临连续性中断的潜在风险率，还能够对潜在的损失起到一定的缓解与预防作用。尤其是在规划设计开发项目时，需将容量规划放在首要位置上，组织人员应对网络流量的增长速度进行实时观察，确保整个系统运行的带宽要求得到满足。

2.3 漏洞管理

当前大部分社会企业均处于物联网技术环境中，在实际经营管理期间，如何快速修补处理 IoT 设备漏洞是面临的重大挑战。通过观察分析大部分 IoT 设备的应用情况来看，要向将现有漏洞进行高效修补，关键需要更新固件。因而任务的实时完成必然存在复杂的流程工序。例如，企业若需要更新升级打印机的固件，必须与 IT 部门进行沟通与协调，但由于其与桌面系统、服务器不同，因此部门无法将补丁快速地投入应用。由此可见，定制固件的升级更新不仅十分复杂，还需要耗费更多的精力与时间[4]。

在 IoT 设备的首次应用阶段，企业需要对其提供的默认凭据予以处理，这也是实际作业中面临的关键问题。一般情况下，诸如打印机、无线接入点等设备的应用，涉及已知的管理员 ID 与密码，与此同时，设备内可能会提供专门的 Web 服务器，借助远程连接的方式，管理员可以直接登录并管理设备。这样的应用形式虽然为设备的使用与管理提供了较大方便，但也为攻击者带来了可乘之机。为了避免攻击者掌握 IoT 设备，企业需要做好一系列的调试工作，完成新开发环境的优化与创建，完善设置各类器件的初始配置，然后进行精准测试。通过扫描，确保设备系统潜在的各类漏洞问题被有效地识别出来，第一时间验证登录信息，以便在向生产环境移入设备前，存在问题的设备系统被及时关闭。部分设备在首次使用时，会提示执行强制更改密码的信息，对于制造商来说，在提供此类设备时，可以附加相应的管理措施，即确保不会持久存在默认凭据。企业也应组件专门的工作团队，核查设备处于良好的运行状态下，再正式投入正式的生产使用中。加大安全控制力度，做好定期测试工作，严密监控对设备的任何操作与处理应用，尤其是密码的更改。在整个使用过程中，如若发现存在操作漏洞问题，应结合实际情况对问题原因进行合理分析，并采取针对性措施解决漏洞问题[5]。

2.4 预防服务中断

物联网在各行业领域的深入应用对 IoT 设备的使用性能提出高要求，一方面其需要具有坚固耐用的特点，另一方面则应对违规的物理篡改具备显著的抵抗能力。在面临攻击后，需要做到自主恢复，借助合理的降级处理等自我保护方式，达到可接受的处理级别，最大限度保障自身的安全性能。在整个过程中，并不需要人为的操作或参与。在对多类型的攻击与威胁进行处理时，尽管可以依托于现有的认知安全解决方案，但要避免出现服务中断现象，还应做好灵活化的把控，IoT 部署的管理人员需要将设备系统的应用优势充分发挥处理，对可能出现的异常情况进行可视化的应对与管控。

物联网存在的缺陷与安全问题是不容忽视的，对于企业而言，严重的安全问题不仅会带来经济损失，还会导致服务被中断、专有信息被盗、客户信息被泄露等诸多问题。设计发展物联网，核心原则是安全性得到保障。正确连接技术的选择、物联网节点地址的识别与验证，以及网络安全的维护，均是企业在物联网生态系统应用发展中面临的关键课题。

2.5 更新防御系统

无论是设备软件，还是正在使用的固件组件，均应保持定期更新的良好应用状态。尤其是在修补 IoT 设备与传感器时，往往需要面临分散化、不受控制、难度高的过程与环境，还涉及庞大的作业规模。总结分析以往的软件更新经验可以发现，在第一个版本更新改进过程中，尽管已经有效解决了所有已知的漏洞问题，在后续的使用阶段内，也会逐渐不断地暴露出新的漏洞问题。即使用设备的时间越长，面临的攻击风险也会大幅增加。因此定期重复更新防御系统，是高效及时解决并应对安全问题的必要措施。

3 结语

对于现代企业而言，重视对物联网关键技术的应用、有效解决安全问题，不仅是提高自身核心竞争力的有效手段，也是贴合时代发展趋势的必要途径。企业可以利用第三方专业知识，评估并识别安全风险，充分发挥物联网技术优势。

参考文献

[1] 余文科，程媛，李芳，等.物联网技术发展分析与建议[J].物联网学报，2020，4(4)：105-109.
[2] 付磊.Web 关键技术对物联网体系架构的影响探析[J].中国信息化，2020(12)：48-49.
[3] 王安之.物联网设备资源管理平台关键技术研究[D].南京：南京邮电大学，2020.
[4] 佟冬.计算机视角下的物联网关键性技术运用分析[J].通讯世界，2019，26(12)：48-49.
[5] 车巍.基于物联网的机电设备实时监测与诊断系统探讨[J].科学技术创新，2019(35)：76-77.

收稿日期：2021-02-01

作者简介：杨 勇(1978—)，男，汉族，江西南昌人，工程师，本科，研究方向为 5G 通信技术和物联网关键技术分析及安全策略。