WILEY IEEE

物联网安全与网络保障

[美]泰森·T.布鲁克斯（Tyson T.Brooks） 编著

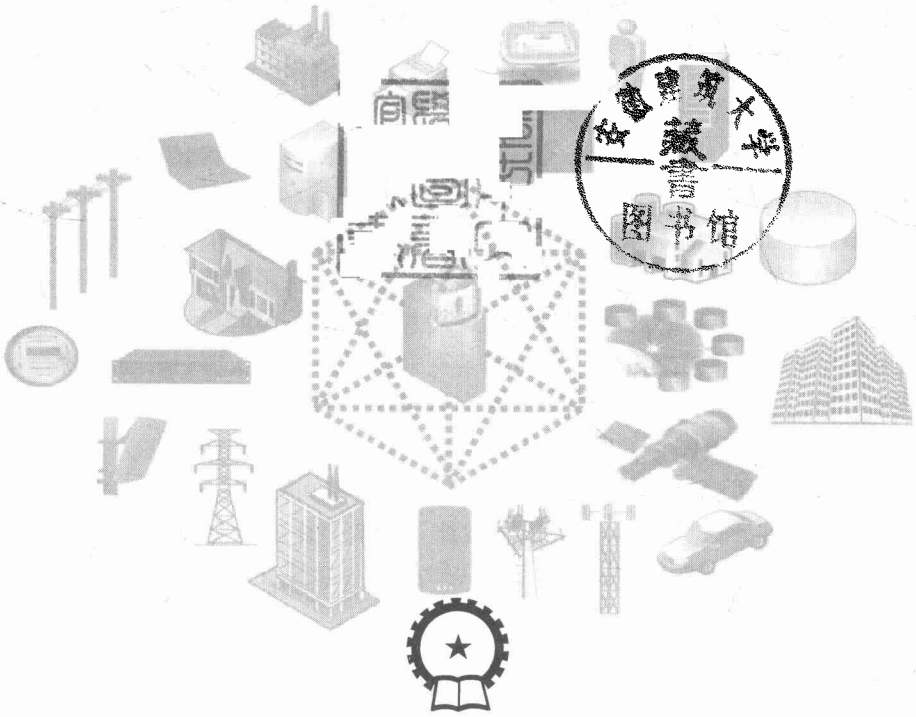
李永忠 俞小霞 等译

Cyber-Assurance for the Internet of Things

机械工业出版社
CHINA MACHINE PRESS

物联网安全与网络保障

[美] 泰森·T. 布鲁克斯（Tyson T. Brooks） 编著
李永忠 俞小霞 杜 淼 沈 成
吕 博 吴 勇 沈祥修 等译



机械工业出版社

图书在版编目（CIP）数据

物联网安全与网络保障/（美）泰森·T. 布鲁克斯（Tyson T. Brooks）编著；李永忠等译. —北京：机械工业出版社，2018.9

书名原文：Cyber – Assurance for the Internet of Things

ISBN 978-7-111-60726-7

Ⅰ.①物…　Ⅱ.①泰…②李…　Ⅲ.①互联网络 – 应用 – 安全技术②智能技术 – 应用 – 安全技术　Ⅳ.①TP393.4②TP18

中国版本图书馆 CIP 数据核字（2018）第 192579 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）

策划编辑：吕　潇　责任编辑：吕　潇

责任校对：郑　婕　封面设计：马精明

责任印制：张　博

北京华创印务有限公司印刷

2018 年 10 月第 1 版第 1 次印刷

169mm × 239mm · 25.5 印张 · 495 千字

0 001—2 000 册

标准书号：ISBN 978-7-111-60726-7

定价：129.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务　　网络服务

服务咨询热线：010 – 88361066　　机 工 官 网：www.cmpbook.com

读者购书热线：010 – 68326294　　机 工 官 博：weibo.com/cmp1952

010 – 88379203　　金　书　网：www.golden – book.com

封面无防伪标均为盗版　　教育服务网：www.cmpedu.com

本书提出了物联网网络保障的概念和方法，分析了物联网环境的网络保障需求，强调了物联网的关键信息保障问题，并确定了信息保障相关的安全问题。本书由工作在网络保障、信息保障、信息安全和物联网一线行业的从业人员和专家根据其研究成果撰写而成，内容涵盖了当前信息保障的问题、挑战和解决物联网保障所需的基本概念和先进技术，也包含了射频识别（RFID）网络、无线传感器网络、智能电网以及工业控制系统的监控与数据采集（SCADA）系统。

本书适合从事无线通信技术、信息安全体系结构和安全系统设计领域工作的研究人员和专业人员阅读，也适合参与信息保障和物联网网络技术的专家教授和学生作为参考。

译者序

随着计算机网络技术，尤其是物联网技术的飞速发展，为智慧智能行业提供了有效的物联网应用技术，现代化的社会已经离不开计算机和网络。物联网技术的推广使用和发展，在极大地方便了人们的工作和学习的同时，也带来了很多安全方面的难题。随着语音电话和数据网络的融合，特别是工业控制网络与公共数据网络的融合，连接网络系统服务的多样性的增加也推动了网络攻击活动的相应增长。针对物联网的攻击和个人隐私泄露等问题日益增多，入侵攻击而造成巨大损失的案例也不断出现。物联网的安全问题日益重要和迫切。本书提出了物联网网络保障的概念和方法，是目前比较新的一种网络安全理念。网络保障的概念和方法不同于目前网络安全的概念和方法，网络安全和信息安全强调的是对现有网络和信息系统的安全进行保护，其方法和技术是属于被动措施；而网络保障方法强调的是在网络分析和设计阶段采取的主动防护措施。所以，网络保障技术不是简单的网络与信息安全技术。本书首先分析了物联网环境的网络保障需求，强调物联网的关键信息保障问题，并确定了信息保障相关的安全问题。本书由工作在网络保障、信息保障、信息安全和物联网一线行业的从业人员和专家根据其研究成果撰写而成，内容涵盖了当前信息保障的问题、挑战和解决物联网保障所需的基本概念和先进技术，并审查了物联网基础设施、体系结构和物联网应用的未来发展趋势。书中涉及的其他主题包括物联网系统的信息保障防护、信息存储、信息处理或未经授权的访问以及修改机器对机器（M2M）的传输，也包含了射频识别（RFID）网络、无线传感器网络、智能电网和工业控制系统的监控与数据采集（SCADA）系统。本书还探讨了对物联网网络和信息进行检测、保护和防护采取信息保障措施的必要性，以确保其信息的可用性、完整性、可鉴别性、保密性和不可抵赖性。

作者从理论和实际应用的角度，对物联网的网络保障理论、应用、体系结构和信息安全等方面的研究现状和发展趋势进行了分析和探讨。帮助读者了解如何在物联网中设计和建立网络保障系统，能够使工程师和设计师接触到新的策略和新标准，促进网络保障的积极发展。本书内容涵盖了具有挑战性的新问题以及潜在的解决办法，鼓励广大从业者在这些领域进行探讨和辩论。

作者泰森·T. 布鲁克斯（Tyson T. Brooks）是美国雪城大学（Syracuse University）信息研究学院副教授，同时他也在美国雪城大学的信息与系统保障信任中心（CISAT）任职，是一位信息安全技术专家和实践者。布鲁克斯博士是《国际物联网与网络保障杂志（International Journal of Internet of Things and Cyber – Assurance）》的创始人和主编，是《企业架构杂志（Joural of Enterprise Architecture）》、《云计算与服务科学国际期刊（International Journal of Cloud Computing and Services Science）》和《国际信息与网络安全杂志（International Journal of Information and Network Security）》的副主编。物联网网络保障的概念和方法是由他提出并不断发展和实践完善的，本书是他对物联网安全与网络保障概念和方法的一个全面阐释和介绍，值得工作在无线通信技术、信息安全体系结构和安全系统设计领域的广大从业者学习和推广。

本书由江苏科技大学计算机学院李永忠主译，俞小霞、杜淼、沈成、吴勇、吕博、沈祥修、罗旋、贾慧、孙岚、张强强、顾磊等人参与了本书的翻译工作。其中甘肃建筑职业学院的俞小霞老师负责完成了本书校对工作。由于时间紧，翻译工作有不对之处，欢迎广大读者批评指正。

李永忠

2018 年 10 月

于江苏科技大学

原书序：有效的网络保障对物联网至关重要

Zeal Ziring
美国国家安全局，信息保障技术总监

我们的社会已经在很大程度上依赖于互联网，以各种各样的方式来访问和使用网络空间。互联网给人们带来了惊人的信息交换能力，可以进行信息交换、商业活动、教育和娱乐活动。但是，对于互联网的发展和成长，通常是通过人们的活动将虚拟世界和物质世界轻微地联系起来，网络数据包和协议的领域与田野、道路和建筑物的物理世界总是分开的。而物联网则使虚拟世界与物质世界越来越紧密地交织在一起成为了可能，它也可称之为网络物理系统（Cyber – Physical Systems，CPS）或其他名称。这种将虚拟世界和现实物理世界紧密联系起来的进程既能带来巨大的好处，同时也能带来巨大的风险，这是一个复杂的发展趋势，建立在技术进步的基础之上，以经济和社会发展为驱动力。它已经在顺利推进了，尽管到目前为止我们只感觉到轻微的影响。

随着物联网技术和功能的日益普及，并最终实现无处不在，物理世界的许多方面将在网络空间中变得更加明显。在某些情况下，网络空间的进程将影响或控制物理对象和环境。物理世界和虚拟世界的接触点将会激增。有很多人估计，在物联网发展的过程中，有多少连接的“物”会从物理环境中分散出来，这个数量会是 10 亿到 50 亿甚至 2000 亿。由于物理世界和虚拟世界之间的巨大融合，我们对互联网和相关技术的依赖也将增加。

已经有许多关于物联网技术的书籍和文章描述了推动物联网的技术以及我们将从中获得的巨大好处。但是这些好处是不确定的。随着物理世界越来越依赖于虚拟世界，目前局限于网络空间的安全威胁将会扩大和转化到物理世界。这本书的主题是关于理解这些风险：它们为什么会出现，它们如何不同于我们今天面临的网络风险，特别是如何解决这些风险。

1. 网络发展的历史

有许多讲述关于互联网历史的资料，主要集中在技术、人或其他因素上。看待互联网的一种方式是它如何从以前独立的系统和领域的融合中发展起来。这与

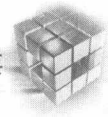
理解物联网及其网络保障的重要性有关，因为它代表了最大的融合。

从电话和无线电广播开始，军事和民用通信就截然不同了。从第二次世界大战开始，军事和民用通信使用不同的技术和不同的保护手段。军事通信通常是加密的，使用不同频段的协议和基础设施。自 1952 年创建以来，美国国家安全局（NSA）设计并编纂了包括军方在内的国家安全通信所必需的安全措施。从 20 世纪 90 年代中期到今天，20 多年来，军事和民用（包括商业）通信之间已经变得更加紧密：共同的技术、协议、基础设施和标准支撑了这两者。最初设想的用于维护国家安全的密码强度级别现在被用来保护战略情报和社交媒体。战术军事行动仍然使用专门的无线电设备，但也使用商业智能手机和蜂窝移动通信标准。从军事方面来说，融合主要是由商业产品提供的强大功能和工作能力驱动的；从商业方面来说，以往仅限于国家安全应用的安全机制是由于在网上进行业务的保证和隐私的需要而推动的。

另一个融合——语音电话和数据网络的融合——已经几乎完成。当然，语音电话网络是首先出现的，到了 20 世纪 60 年代计算开始发展时，国内和国际电话网络已经建立起来了。事实上，电话网络是如此庞大和可靠，早期的数字通信就是把它用作基础设施，将数字数据从串行线路转换成调制的音频信号，通过电话网络传输，然后在另一端再把它们转换成比特数据的。但是在 20 世纪 70 ~ 80 年代，电话网络本身变成了数字化的，同样的交换网络被用来承载语音呼叫和专用的数字链路（所谓的“租用线路”）。一些最早的广域数据交流，如电子公告板和新闻组，就采用这些技术。与此同时，大学和公司以及美国国防部（DoD）正在创建分组网络的基础设施。

到 20 世纪 80 年代初，互联网的许多关键技术已到位，互联网开始呈指数增长。但电话网络仍然围绕着静态中继线和电路交换而建立。从 20 世纪 90 年代到 21 世纪初期，分组交换和互联网协议的核心技术被整合到全球电话网络中，语音成为分组网络上的另一种数字通信业务。今天，全球网络结构完全是基于分组的，语音业务和数据业务之间的区别主要是针对蜂窝通信系统。但是以前独立的语音和数据网络的融合产生了安全方面的隐患，语音电话服务可能会受到数据网络的攻击，但现代网络中的网络保障技术可以帮助保护语音和数据服务。

另外还有一个趋势要特别指出，是与工业网络和公共数据网络的融合。工业系统的计算机控制始于 20 世纪 60 年代，采用直接数字控制（DDC）系统。第一个可编程序逻辑控制器（PLC）系统建于 1968 年。到 20 世纪 70 年代末，PLC 使用调制解调器、串行链路和专有协议进行连接。20 世纪 90 年代初，在互联网协议（TCP/IP）上出现了工业控制协议的互操作性和传输标准，但控制系统仍然通过专用链路或租用线路连接和管理。自 2000 年以来，通过互联网控制工业系统的领域发展迅速。这种融合的驱动因素是降低成本和提高操作灵活性，特别



是将工业控制和监控系统与业务系统集成在一起，这样做的好处是巨大的，但是让工业系统直接或间接地暴露给互联网来访问也会带来巨大的风险。控制系统的部件通常是为了可靠性、简单性和经济性而设计的，政府、学术界和商业实验室的反复测试已经发现了在整个行业中 10 多年来存在的诸多漏洞。将工业控制系统连接到互联网并将其与其他互联网系统集成的趋势有时被称为“工业互联网”，就好像它是一个单独的网络，其实事实并非如此。

随着上面所描述的融合历史的发展，针对计算机和数据网络的恶意活动也同时存在。这个历史记录在多本书和多篇论文中，但只有少数几个专题，讨论了威胁的增长。在互联网之前的年代，计算机和网络当然也会受到恶意行为的影响，但范围相对狭窄，一些早期的个人计算机（PC）病毒传播相当广泛，但仅限于一个非常狭窄的操作系统和应用程序范围。军事网络一般在国家行为层面上由参与者被动收集，但这是可以预料的，风险也是可以管理的——被动收集的风险可以通过有效的加密来管理。

在全球互联网的早期，从 1988 年的莫里斯蠕虫病毒（Morris Worm）开始，一直持续到 20 世纪 90 年代和 21 世纪初，出现了许多大规模的网络恶意攻击事件。虽然这些感染成为了头条新闻，但更复杂的恶意软件和间谍功能软件正在悄悄发展。另外，随着万维网（WWW）的发展，对网站的篡改攻击也相应增长。在这段时期的大部分时间里，互联网上存储和业务信息的价值都不高，许多恶意行为者的动机即“释放一种在世界范围内传播的计算机病毒，获得同行的好评”。在此期间，计算机和网络技术的主要供应商也开始更加重视安全。举个例子，在 1992 年，微软公司的旗舰产品是 Windows 3.1，它没有有效的安全性；到 2000 年，他们的旗舰产品 Windows 2000 包含了广泛的安全功能。

在最近的十年中，互联网领域的融合带动了经济、政府和社会发展的很大一部分。连接系统和服务的价值和多样性的增加也推动了恶意活动的相应增长和多样化。例如，互联网服务更多地用于银行业，紧随其后的是针对银行账户和交易的网络犯罪。同样，随着各国政府和各经济体对互联网的依赖程度越来越高，世界各国政府已加大了利用互联网作为收集情报和向对手施压的领域。包括美国在内的许多国家已将网络空间业务纳入其军事理论。

我们也看到了第一起通过互联网攻击工业控制网的事件，其影响已经超出了网络空间进入物理世界。早期的大多数攻击被认为是偶然的，但到 2008 年底，很明显一些网络攻击者故意针对电力公司进行攻击并勒索。2010 年，Stuxnet 震网病毒被发现，似乎是针对特定的工业设施，通过互联网和其他网络传播，并造成该设施的物理损坏（以及其他地方的服务中断）。

网络发展历史的明确信息是，攻击跟随价值。即我们放在互联网上的信息价值和依赖性越大，恶意攻击者、罪犯和敌对政权就越有动力在那里攻击。我们正

处于网络最大融合的早期阶段，而且我们对保障的需求相当巨大且迫切。

2. 物联网的广度和多样性

物联网的融合是一个非常广泛的现象，涵盖了几乎所有行业、技术标准和地理范围。它既包括连接的“物”，也包括了与它们交互的各种数据分析、管理和基础设施服务。数据和交互是我们期望获得好处的基础，如一辆有互联网连接的汽车可能有助于驾驶员前往他们的目的地，并且当大多数汽车都通过一条路时，分析和主动管理软件将有助于一座城市有效地保持交通畅通。一些创新公司正在设计新的数据分析模型，并在住房、交通、制造业、医疗保健、公共安全、能源、零售等领域进行数据分析。

物联网的标准格局是比较复杂的，在许多领域，标准还在不断涌现或演变。标准对于物联网是必不可少的，因为它们促进了互操作性、稳定性和创新性。有许多领域的标准将是必不可少的，但其中四个与物联网安全特别相关。

1）蜂窝通信——无线电频谱是一种有限的、宝贵的资源。随着越来越多的设备连接入互联网，管理所有这些资源的可用性将是至关重要的。

2）个人局域网（PAN）——可穿戴设备和附近设备之间距离非常短的数据交换标准仍在发展，以支持我们所需的所有功能和保障。

3）安全性和密码学——大多数现有的安全协议、认证方案和其他标准都是为台式计算机和企业服务器设计的。未来将需要新标准来为大量小型受限设备提供基本的安全服务，这些服务包括身份和认证管理、授权以及数据保护等。物联网将在配置、效率和规模方面提出新的要求。

4）感知和数据管理——物联网的最大好处在于对物理世界的感知方面，将这些感知数据公开给网络空间进行分析和融合。所以，也需要标准来表示和管理大量的传感器数据。

物联网设备将使用各种连接互联网的方式。有些设备只有在被别的设备激活时才能被访问，比如射频识别（RFID）标签阅读器。还有其他设备会进行定期的交互，提供数据或接受命令，否则是静默的（例如植入式医疗器械、气象传感器）。许多设备将允许连续的连接来传送数据或允许远程实体对象施加实时控制（例如智能电视、变电站监控），还有一些设备将作为本地网关，支持本地交互并为其他设备提供互联网连接在其范围内（例如智能汽车、公共汽车或火车）。

综上所述，物联网将给我们带来巨大的好处，但这些好处大多取决于某种形式的信任，我们只有在物联网设备和支持服务的运作中对其有足够的信任，才能赋予它们对物理系统和环境的控制权。我们需要有信心，相信从传感器提供的数据是准确的，以便依靠它们做个人、商业甚至是军事决策。建立和维护必要的信任在很多方面都是具有挑战性的。即使对于狭窄的传统计算机，通常也不可能有

完整而全面的信任。相反，我们需要建立可以提供特定类型信任的系统。我们需要在个人设备、设备群体、用户、服务和基础设施多个层面对物联网系统进行信任管理和相关保证。

3. 关于物联网的网络保障是什么？为什么它很重要？

在最高层次上，物联网的保障就像对网络空间其他元素的保障一样。但是，受物联网规模的限制，以及保障失败的潜在影响，意味着目前实现保障的战略是不够的。

基本保障属性是：

1）真实性——保证声称拥有身份的实体拥有使用它的权利。分配和认证身份对物联网将是具有挑战性的。

2）完整性——保证信息仅由有权这样做的实体才能创建、修改和删除。

3）保密性——确保只有具备必要权利的实体才可访问或可读信息。

4）可用性——保证信息或服务在所有条件下都可用或可访问。

5）不可抵赖性——保证一项活动可以无可辩驳地绑定到一个负责任的实体上。

这些保证是基本的。通过使用和组合它们，系统可以提供更高的定制属性，例如隐私、合法性或可恢复性。所有这些对于物联网设备的安全运行及其将要支持的服务来说都是非常重要的。

除了设备直接面临安全风险外，物联网将对其所依附的传统系统和网络的风险状况产生深远的影响。将各种各样的物联网设备连接到传统网络上将扩大这些网络的受攻击面。为了支持这些设备，传统网络将不得不支持更广泛的协议和数据格式，这也为可利用的漏洞增加了新的潜在威胁。最后，许多物联网采用案例桥接弥补传统的信任边界，或者要求系统所有者建立新的信任关系，因此建立对物联网设备和系统的保障，对于管理这些风险也是至关重要的。

实现传统网络的基本保障属性已被证明是极其困难的——最近的安全事件向我们表明，我们现有的技术措施和做法不足以防止网络攻击的不利影响。在物联网系统中实现基本属性保障将更加困难。为什么？首先，物联网的规模和多样性将需要跨越范围很广的方法和标准。设备功能是多种而异构的，如计算速度、数据存储和通信带宽。对于连接的设备，这些功能中的一些功能将从小型标签和传感器到智能车辆和建筑物，在六个数量级或更多的范围内变化。

支持连接设备和服务的另一个挑战是安全需求的多样性。有些设备将需要非常严格的安全权限。例如，植入的医疗设备将具有非常高的完整性要求，并且应该仅向患者和授权医生发送数据；相反，气象传感器则可以向任何请求者提供数据。设备的寿命也将是一个挑战，所以要确保一些物联网设备具有长效性。有些设备将具有频繁接受安全更新的能力和相应的传输带宽，但有些设备却不需要。

例如，某些类型的传感器不得不运行多年，并且不能期望在工作期间接收任何软件更新或信任节点的更新，这意味着这些设备内置的安全机制需要非常简单和健壮。

最后，基于保证物联网设备数据和访问的法律、政策和实践相对不成熟，物联网将面临很多保障挑战。考虑一个智能建筑——应该授权哪些参与方读取建筑系统的传感器数据？是建筑物的所有者、租户、还是当地的消防部门，亦或是维修工（如水管工或电工）？每个利益相关者对于访问建筑物数据的一部分或调整建筑物的运行方面都有很好的理由。但是技术控制、法律判例和接受的做法都并没有为支持他们做好准备。

物联网将让我们体会到信息技术的灵活性和强大的力量感，从单人可穿戴设备到零售店，再到公路系统，感知、理解、管理和优化物理世界的许多方面，我们依靠物联网来为我们做这些事情，如果我们有一定的必要保障，就可以享受相应的利益。以下是基于网络安全的基本属性，但是已被调整为可以为物联网系统的设计者和制造者可以采纳的属性：

1）保证收集的数据是有效的（即报告的值是被检测的值）。

2）确保访问收集到的数据受到适当的限制。

3）保证设备的控制权仅由授权方执行，并可追究这些执行方的责任。

4）确保适用的法律、法规和政策得到执行。

5）确保物联网系统和其他网络系统之间的互动可以被监控和控制。

6）确保当单个设备或组件更新或替换时，整体安全属性继续保持不变。

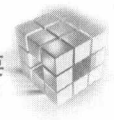
物联网最重要的安全属性将是系统属性，由硬件和软件、服务提供商、数据聚合中间件以及演示系统提供，限定并依赖于多层的保证。

4. 示例

下面的示例验证了四种不同的物联网场景的保障挑战。

示例 1——连接到互联网的医疗可植入设备可以提供更快捷的健康问题检测，更精细的反映和监测整体健康。由于设备本身在尺寸，功耗和连接性方面受到严重限制，使用这样的设备有直接的风险，即对其进行网络攻击可能直接威胁用户的健康和生命安全。例如改变设备报告数据的攻击可能会造成这样的威胁，因为医疗可能是以此数据为基础的。收集到的数据也有很强的隐私问题。数据访问的保障将是复杂的，因为有多个利益相关者：病人、医生、医院、急救员、保险公司、设备制造商等。此外，医疗设备和健康数据也受到复杂的监管制度的制约，这些制度仍适应于网络威胁。

示例 2——连接到互联网的汽车将支持从简单地避免碰撞，到驾驶和保养，以及到完全自主操作的各种使用情况。运输安全和效率有很大的潜在收益，这样一个复杂的系统也会有一个复杂的授权模型，对于驾驶员、机械师、制造商、公



路系统和网络基础设施都有不同的权限。有些操作将受到严格的实时限制，而另一些涉及与全球互联网的通信。车辆与智能高速公路系统之间的相互作用仍在定义，但意味着非常密切的信任关系。最近来自研究人员的漏洞演示表明，目前的汽车远程信息处理系统不能有效地执行信任边界，这将不得不改变信任关系。最后，连接网络的汽车将连接到各种各样的其他网络，如在业主的家中，在维护设施店，以及在高速公路上。每辆车和这些网络之间需要有非常具体和有限的信任关系。

示例 3——智能建筑将包含各种传感器、执行器和控制系统，用于多种用途：照明、安全、加热和冷却、入口控制等。这些系统中的很多都是为了提高建筑物的成本效益而设置的，或者是为了更好地吸引用户。收集到的数据会有一些隐私或保密问题。但主要风险将是基于控制的：建筑物内的控制系统的滥用可能使其不适宜居住甚至损坏。控制完整性和授权将成为智能建筑的关键保障，但如上所述，这类建筑的授权用户将是庞大而多样的。除了连接到互联网之外，许多楼宇自动化技术还使用无线网络，使用 Wi-Fi，ZigBee 和蓝牙等标准。这些可以使建筑物的网络暴露于任何接近的人。

示例 4——传感器网络提供了监测不同环境和场所的物理条件的潜力。例如，海洋传感器网络可能由传感器浮标、通信继电器以及其他浮动和锚定元件组成。网络组件将是广泛分布的，工作条件恶劣，连通性不确定。这些组件可能会受到功率的限制，预计将在存储式电源上长期运行。从这些传感器收集的数据可能是公开的，其完整性可能对于海洋导航和天气预报至关重要。来自传感器网络的数据将与分析系统中的其他数据来源进行融合，在分析系统中可能会有更多的价值来吸引威胁行为者。这意味着需要管理传感器网络和分析系统之间的信任，以防止传感器向上传播的危害。

这四个例子显示了几个共同的元素。第一，完整性是大多数物联网用例的关键问题，它包括报告数据的完整性和控制的完整性；第二，许多为各种物联网领域生产部件的供应商历史上都不必担心其产品的网络保障，直到现在他们的产品才面临这样的威胁；第三，在这些示例中，没有简单的模型或信任关系的通用模型。每一个示例都包括各种不同的角色和权利的利益相关者。最后，这些示例中所有连接的设备都不能独立运行，它们都与其他基础设施和系统相互作用，从这些系统中承受风险并同时给这些系统带来风险。

5. 物联网的网络保障要素

研究人员、学术界人士、专业人士和科学工作者还有很多工作要做，以创造一个可靠的和可信赖的物联网环境。研究已经在进行中，需要继续下去。标准机构和财团已经承担了将安全建设纳入所需标准的挑战。下一步是为更广泛的社区、制造商、服务提供商、数据整合商的产品提供保障，并为用户提供需求。我

们还不知道物联网需要的所有保证和安全功能，但我们知道的这些都将是至关重要的。这部分知识，以及在构建过程中的学习，一直是通向当今互联网环境的各种主要发展的特征。我们可以在构建的过程中学习，但我们必须在每一步中构建要点。下面列出了一些要点，并在本书的各章中进行了更充分的探讨。基本的安全属性、基本原理，必须设计到物联网的设备、基础设施和后端分析系统中。安全性设计必须反映物联网的要求和约束，必须使高层保障成为端到端的保障。

本书第 1 章和第 2 章探讨设计物联网的一般保障，提供物联网设备和服务的身份认证以及管理与这些身份认证相关的凭证、属性和授权。对于支持诸如隐私和访问控制之类的高级别保障属性至关重要。物联网设备必须能够安全地集成到现有的网络服务和企业 IT 环境中——这就要求物联网设备本身具有一定的安全特性，并且企业网络系统处理信任域的方式也将发生重大变化，第 3 章探讨了这个非常具有挑战性的领域。建立和维护物联网系统的保障将取决于信任管理服务，信任管理服务将不得不从单个设备扩展到第 4 章和第 5 章所述的高级数据分析服务。第 6 章回顾了可穿戴计算的隐私和安全问题。第 7 章重点介绍了工业控制系统的漏洞问题。第 8 章讲述利用大数据技术来增强物联网的安全的方法，这本身只是提高网络保障所需的多种措施之一。保障不是一次可以建立，然后就可以被遗忘的事情，它必须积极管理、测量和维护。第 9 章探讨了安全评估机制的更普遍的挑战。第 10 章研究网络保障在未来人工智能方面的应用。第 11 章探讨了物联网对网络物理系统的威胁。

为了确保构成物联网的设备和系统中必须包含必要的保障要素，有必要提高对挑战和可能解决方案的认识。本书是朝这个方向迈出的一步。通过提出棘手的问题，并提出可能的解决方案，将鼓励讨论和辩论，让工程师和设计人员接触到新的策略和新的标准，促进网络保障的积极发展。有了这些保障，我们将能够充分利用物联网的潜在好处。

原书前言

物联网已经导致了相对不成熟技术的广泛部署。然而，物联网技术的程序设计者、网络设计者和技术实施者在确保所提供适当的安全级别时也面临着许多重大的挑战。由于采用物联网的创新技术将更多地集中在无线技术上，因此在部署无线基础设施时必须考虑许多复杂的事项。如果没有充分的预见性，使用它们可能是不明智的。研究人员和商业机构预测，到2020年将有500亿台设备连接到互联网，2025年对物联网应用的潜在经济影响（包括消费者剩余价值）将高达每年11.1万亿美元。物联网网络将变得非常流行，因为它们可以在很少的设备基础设施上快速部署。这些网络也适合短期用户群体的环境。物联网的可能应用几乎是无限的，世界各地的组织都很快地意识到了它的潜力。

无线设备和技术的大量使用，使物联网的运营变得十分复杂。同时，数据传输和数据存储处理速度的明显加快，也加快了物联网系统的数据集中的步伐，而快速移动的接入点必然带来信息安全策略迅速而不断的变化。在这样一个高度复杂和不断变化的环境下，企业必须重视信息安全工具和技术的使用，以期在这种新的环境下战胜网络攻击。未来的物联网平台将不得不在非常恶劣的环境中运行，存在着严重的高级持续攻击威胁（APT），将会影响正在处理的信息的安全性。这些APT攻击对于正在处理的数据的安全性造成威胁，包括物联网的安全性、信息安全性和物理安全性。对这些APT攻击采取适当的对策来确保主动应对网络的攻击是必要的。采取的主要措施包括采用不同的技术防御措施，加强物联网网络和设备的安全性设计，并对这些网络和设备进行研究和生产。

本书提出了物联网网络保障方法的概念，网络保障技术是多样性的，这些技术承担着找出有可能被网络攻击者成功地用于可利用漏洞缺陷的任务。此外，本书还将帮助信息安全、信息保障以及物联网行业从业者建立对如何设计和构建物联网网络保障的认识。本书的目标读者是那些在无线技术、信息系统理论、系统工程、信息安全体系结构和安全系统设计领域工作的研究人员、专业人员和学生以及参与物联网相关网络保障工作的大学教授和研究人员。

第1章：提供了一种通过设计系统来设计物联网的安全方法以及通过建立硬件和软件组件来最小化人为错误和漏洞引入的程序和过程。

第 2 章：提供了一种通过嵌入式传感器自动保护物联网网络和设备的概念，该传感器识别网络攻击，并在继续处理数据之前减轻对设备和网络的任何威胁。

第 3 章：讨论了一套安全更新物联网设备的统一方法的潜在集合，通过基于其加密处理能力、可用存储以及如何实现网络连接的功能，对物联网设备进行分类，可以应用于任何形式或功能的设备更新。

第 4 章：解释了无线自组织网 Ad Hoc 网络和传感器网络中的漏洞，并结合各自的设计指标和分析，阐明了信任管理方案的设计属性。

第 5 章：讨论信任边界的两个方面：一个被授权认可的物联网设备在接受到网络的信任边界时如何影响安全态势，以及一个未经授权认可的物联网设备在与网络信任边界内的设备交互时如何影响安全态势。

第 6 章：回顾了 Fitbit 可穿戴设备实验及其与可穿戴物联网设备的隐私/安全问题的关系。

第 7 章：涉及物联网传感器设备应用的特定领域，消费环境中的反馈环路，突出自动控制理论、控制系统工程、信息技术、数据科学、技术标准等领域的漏洞。

第 8 章：回顾了复杂事件处理和大数据这两大计算的发展趋势，提出了增强物联网安全的来源和相关机遇。

第 9 章：确定了一个框架，该框架可以简化和聚合云计算 - 物联网中的安全关键设备（例如嵌入式设备、标签、执行器、智能对象）的功能。

第 10 章：论述了确保物联网网络保障的人工智能方法。

第 11 章：评估给定的网络物理系统，以帮助推导出一组输入要求，并为物联网的威胁检测和评估提供自动化的方法。

Tyson T. Brooks

缩略语

3D	Three – Dimensional	三维立体
6LoWPAN	IPv6 Over Low Power Wireless Personal Area Network	基于 IPv6 的低功率无线个域网
AE	Action Engine	活动引擎
AES	Advanced Encryption Standard	高级加密标准
AFRL	Air Force Research Laboratory	空军研究实验室
AI	Artificial Intelligence	人工智能
AIoT	Advanced Internet of Things	高级物联网
ANSI	American National Standards Institute	美国国家标准协会
AONS	Advanced Object Naming Service	高级对象命名服务
AP	Access Point	无线接入点
API	Application Programmatic Interface	应用程序接口
APT	Advanced Persistent Threats	APT 高级持久攻击
ARM	Advanced RISC Machines	高级精简指令集计算机
ASI	AIoT Standard Interface	高级物联网标准接口
AV	Autonomous Vehicles	自主车辆
BS	Bachelor of Science	理学学士
BVCC	Boosted Power Supply Voltage	升压电源电压
BYOD	Bring Your Own Device	带上自己的设备
C2	Command – and – Control	命令与控制
CA	Certificate Authority	证书授权
CAD	Computer – Aided Design	计算机辅助设计
CAN	Controller Area Network	控制器局域网
CAR	Computer – Assisted Reasoning	计算机辅助推理
CC	Cloud Computing	云计算
CCP	Custom Cryptographic Processor	自定义密码处理器
CCS	Calculus of Communicating Systems	通信系统的演算
ERP	Enterprise Resource Planning	企业资源规划
ES	Embedded Systems	嵌入式系统
ETL	Extracted, Transformed, and Loaded	提取、转换和加载
FAA	Federal Aviation Administration	美国联邦航空管理局
FGTM	Front – End – Loaded Grounded Theory Method	前端加载接地理论方法
FPGA	Field – Programmable Gate Array	现场可编程门阵列
FRiMA	Faster Risk Malicious Assessment	风险快速评估
FTPS	Fire, Theft Prevention System	防火防盗系统
GPS	Global Positioning System	全球定位系统