21世纪高等学校规划教材 | 物联网

物联网安全教程

张 凯 主编

清华大学出版社

物联网安全教程

张 凯 主编

清华大学出版社
北京

内容简介

本书是物联网安全课程的教材，内容包括信息安全概述、信息加密技术、物理安全威胁与防范、计算机网络安全、信息安全标准体系、信息安全管理、物联网安全、物联网感知层安全、物联网网络层安全、物联网应用层安全、物联网安全技术应用、练习题和参考答案等。本书可作为高等院校物联网工程专业或计算机专业物联网方向物联网安全课程的教材或教学参考书，亦可作为物联网安全方面的学者和爱好者的参考书。

图书在版编目(CIP)数据

物联网安全教程/张凯主编. —北京：清华大学出版社，2014
21世纪高等学校规划教材·物联网
ISBN 978-7-302-33500-9

Ⅰ. ①物… Ⅱ. ①张… Ⅲ. ①互联网络－安全技术－高等学校－教材 ②智能技术－安全技术－高等学校－教材 Ⅳ. ①TP393.4 ②TP18

中国版本图书馆CIP数据核字(2013)第189091号

责任编辑：闫红梅　赵晓宁
封面设计：傅瑞学
责任校对：梁　毅
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：26.5　　**字　数**：662千字
版　　次：2014年1月第1版　　**印　次**：2014年1月第1次印刷
印　　数：1～2000
定　　价：44.50元

产品编号：050132-01

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程”（简称“质量工程”），通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上。精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合 21 世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻性。教材由个人申报或各校推荐（通过所在高校的“编委会”成员推荐），经“编委会”认真评审，最后由清华大学出版

社审定出版。

目前，针对计算机类和电子信息类相关专业成立了两个“编委会”，即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括：

(1) 21 世纪高等学校规划教材·计算机应用——高等学校各类专业，特别是非计算机专业的计算机应用类教材。

(2) 21 世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21 世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21 世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21 世纪高等学校规划教材·信息管理与信息系统。

(6) 21 世纪高等学校规划教材·财经管理与应用。

(7) 21 世纪高等学校规划教材·电子商务。

(8) 21 世纪高等学校规划教材·物联网。

清华大学出版社经过三十多年的努力，在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌，为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格，这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

联系人：魏江江

E-mail：weijj@tup.tsinghua.edu.cn

前言

物联网工程是一个新的本科专业，国内很多大学刚刚开办。“物联网安全”是物联网工程专业本科生的一门专业课，该课程教学面临的问题较大，主要包括两个方面：一是教学体系尚未形成，教学内容、教学目标和知识点要求不是很清晰；二是教材建设薄弱，目前市面上物联网专业的教材相对较少，物联网安全的教材更少，实际教学与教材建设差距很大。编者在编写这本教材时，就这两个问题做了一些探索和尝试。

本书包括两大部分，共11章。第一部分　信息安全基础方面的理论和原理。内容涉及第1章　信息安全概述，第2章　信息加密技术，第3章　物理安全威胁与防范，第4章　计算机网络安全，第5章　信息安全标准体系，第6章　信息安全管理。第二部分　物联网安全体系，感知层、网络层和应用层安全的理论、原理和方法，以及物联网安全技术应用案例。内容涉及第7章　物联网安全，第8章　物联网感知层安全，第9章　物联网网络层安全，第10章　物联网应用层安全，第11章　物联网安全技术应用。

本书由张凯教授策划、主编、审核、修改和定稿。张治博士编写了第8章，万少华博士编写了第2章2.1节的部分内容，其他章节由张凯编写。研究生张雯婷做了大量的资料整理工作，并编制了练习（课后练习和期末模拟考试卷），刘爱芳老师对全书进行了文字校对。在此，对所有参加本书工作的人员和关心本书的学者表示衷心的感谢。

本书在编写过程中，参考和引用了大量国内外著作、学术论文、硕士/博士论文、研究报告和网站文献的内容。由于篇幅有限，本书仅仅在结尾处列举了主要参考文献。应该特别说明的是，由于物联网安全是一个新的领域，目前这方面的教材很少，也不成熟。编者希望在编写这部教材时，不仅要介绍信息安全的基本理论和方法，也要将近年最新的研究成果“原汁原味”地介绍给读者。由于编者水平有限，有些学术论文的内容介绍属直接引用，在书中引用时大多都加注了原作者和出处的说明，编者也未对其内容做较大修改，以保持原作者的风格，以便读者掌握其新的理论和技术思想。还有一种情况就是，某一个主题的研究有几个作者和文献，编者编写时引用了几个作者的观点和资料，为了文字通顺流畅和主题突出，这时的引用和注释可能不够准确。另外，本书也参考了互联网上一些专业人员的经验和心得以及部分网站的相关资料。如果有作者发现其成果被引用而未注明，请联系编者（电子邮件：zhangkai@znufe.edu.cn），我们将在再版时补上。在此，编者向所有被参考和引用的作者和网站表示由衷的感谢，你们的辛勤劳动为本书提供了丰富的资料。

本教材编写的教学内容安排是36～51学时。对于学时较多的学校，可讲授全书的内容。对于课时只有36学时的学校，可安排第11章自学；第2章信息加密技术是教学难点，教师可删减教学内容，以降低学习难度；第5和第6章介绍了大量信息安全方面的标准，教师可酌情删减其内容，以介绍主要思想为主。本书是对“物联网安全”课程和教材的一种探

索。尽管编者付出了巨大努力，因能力有限，本书难免存在一些错误，望读者对此提出宝贵意见。

目前，清华大学出版社的数字化教学平台已经运行，本书的课件将在出版时上传，读者可从中下载。另外，如果授课教师有什么具体或特殊要求，包括期末考试题电子稿、实验大纲和背景资料等，请直接与编者联系，我们将尽量满足您的要求。

编　者

2013 年 8 月

目 录

第1章 信息安全概述

本章将介绍信息安全基本概念、安全体系、历史和现状，以及信息安全法规。要求学生对信息安全有一个基本了解。

1.1 信息安全基本概念

本节将介绍信息安全基本概念、安全属性和内容。

1.1.1 信息安全概述

信息安全本身包括的范围很大，大到国家军事、政治等机密安全，小到如防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证和数据加密等），直至安全系统，其中任何一个安全漏洞都可以威胁全局安全。信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

1. 信息安全的定义

目前，信息安全没有统一的定义，不同学者和部门有不同的定义。

有人认为，在技术层次上，信息安全的含义就是保证在客观上杜绝对信息安全属性的安全威胁，使得信息的主人在主观上对其信息的本源性放心。

还有人认为，信息安全是指秘密信息在生产、传输、使用、存储过程中不被泄露或破坏。信息安全所面临的威胁主要包括：利用网络的开放性，采取病毒和黑客入侵等手段渗入计算机系统，进行干扰、篡改、窃取或破坏；利用在计算机 CPU 芯片或在操作系统、数据库管理系统、应用程序中预先安置从事情报收集、受控激发破坏的程序来破坏系统或收集和发送敏感信息；利用计算机及其外围设备电磁泄漏，拦截各种情报资料等。

美国国家安全电信和信息系统安全委员会（NSTISSC）对信息安全给出的定义是对信息、系统以及使用、存储和传输信息的硬件的保护。但是要保护信息及其相关系统，诸如政策、人事、培训和教育以及技术等手段都是必要的。

目前，国内外有关方面的论述大致分为两类：一类是指具体的信息技术系统的安全；而另一类则是指某一特定信息体系的安全。但有人认为这两种定义均过于狭窄，信息安全

定义应该为：一个国家的社会信息化状态不受外来的威胁与侵害，一个国家的信息技术体系不受外来的威胁与侵害。原因是：信息安全首先应该是一个国家宏观的社会信息化状态是否处于自主控制之下，是否稳定的问题，其次才是信息技术安全的问题。

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。信息安全主要包括5个方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。

其根本目的就是使内部信息不受外部威胁，因此信息通常要加密。为保障信息安全，要求有信息源认证、访问控制，不能有非法软件驻留，不能有非法操作。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

2. 信息安全的威胁

信息安全的威胁来自方方面面，不可一一罗列。但这些威胁根据其性质，基本上可以归结为以下几个方面：

(1) 信息泄露。保护的信息被泄露或透露给某个非授权的实体。

(2) 破坏信息的完整性。数据被非授权地进行增删、修改或破坏而受到损失。

(3) 拒绝服务。信息使用者对信息或其他资源的合法访问被无条件地阻止。

(4) 非法使用(非授权访问)。某一资源被某个非授权的人，或以非授权的方式使用。

(5) 窃听。用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如对通信线路中传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄漏截取有用信息等。

(6) 业务流分析。通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

(7) 假冒。通过欺骗通信系统(或用户)达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。我们平常所说的黑客大多采用的就是假冒攻击。

(8) 旁路控制。攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。例如，攻击者通过各种攻击手段发现原本应保密，但是却又暴露出来的一些系统“特性”，利用这些“特性”，攻击者可以绕过防线守卫者，侵入系统的内部。

(9) 授权侵犯。被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的，也称作“内部攻击”。

(10) 抵赖。这是一种来自用户的攻击，涵盖范围比较广泛，如否认自己曾经发布过的某条消息、伪造一份对方来信等。

(11) 计算机病毒。这是一种在计算机系统运行过程中能够实现传染和侵害功能的程序，行为类似病毒，故称作计算机病毒。

(12) 信息安全法律法规不完善。由于当前约束操作信息行为的法律法规还很不完善，存在很多漏洞，很多人打法律的擦边球，这就给信息窃取、信息破坏者以可乘之机。

3. 信息安全的重要性

我国的改革开放带来了各方面信息量的急剧增加，并要求大容量、高效率地传输这些信息。为了适应这一形势，通信技术发生了前所未有的爆炸性发展。目前，除有线通信外，短波、超短波、微波和卫星等无线电通信也正在越来越广泛地应用。与此同时，国外敌对势力为了窃取我国的政治、军事、经济、科学技术等方面的秘密信息，运用侦察台、侦察船、侦察机、卫星等手段，形成固定与移动、远距离与近距离、空中与地面相结合的立体侦察网，截取我国通信传输中的信息。

21世纪，很多事情已经托付给计算机来完成，敏感信息正经过脆弱的通信线路在计算机系统之间传送，专用信息在计算机内存储或在计算机之间传送，电子银行业务使财务账目可通过通信线路查阅，执法部门从计算机中了解罪犯的前科，医生们用计算机管理病历，所有这一切，最重要的问题是不能在对非法(非授权)获取(访问)不加防范的条件下传输信息。传输信息的方式很多，有局域计算机网、互联网和分布式数据库，有蜂窝式无线、分组交换式无线、卫星电视会议、电子邮件及其他各种传输技术。信息在存储、处理和交换过程中都存在泄密或被截收、窃听、篡改和伪造的可能性。

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。但是，对于不同的部门和行业来说，其对信息安全的要求和重点却是有区别的。

1.1.2 信息安全属性和内容

1. 信息安全的属性

所有的信息安全技术都是为了达到一定的安全目标，其核心包括保密性、完整性、可用性、可控性和不可抵赖性5个安全目标。

1) 信息保密性

信息保密性是指系统中有密级要求的信息只能经过特定的方式传输给特定的对象，确保合法用户对该信息的合法访问和使用，阻止非授权的主体阅读信息。它是信息安全一诞生就具有的特性，也是信息安全主要的研究内容之一。更通俗地讲，就是说未授权的用户不能够获取敏感信息。对纸质文档信息，只需要保护好文件，不被非授权者接触即可。而对计算机及网络环境中的信息，不仅要制止非授权者对信息的阅读，还要阻止授权者将其访问的信息传递给非授权者，以致信息被泄露。

2) 信息完整性

信息完整性主要是指系统保证信息在存储和传输的过程中保持不被非法存取、偷窃、篡改、删除等，以及不因意外事件的发生而使信息丢失。完整性要求信息在存储或传输的过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性，防止信息被未经授权的篡改，保护信息保持原始的状态，使信息保持其真实性。如果这些信息被蓄意地修改、

插入和删除等，形成虚假信息将带来严重的后果。

3）信息可用性

信息可用性是指授权主体在需要信息时能及时得到服务的能力。可用性是在信息安全保护阶段对信息安全提出的新要求，也是在网络化空间中必须满足的一项信息安全要求。

4）信息可控性

信息可控性是指系统对信息的传播及其内容具有可控制能力的特性，是对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统。

5）信息不可抵赖性

信息不可抵赖性也称为不可否认性，是指在网络环境中，信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为。信息交换的双方对信息的传递与接收都具有不可抵赖的特性，即发出信息的一方不可抵赖曾经发出某种信息，接收方不可抵赖曾经收到某种信息，且不可以对信息做出任意非法操作，并能按照发出方的要求提供回执。

信息安全的保密性、完整性和可用性主要强调对非授权主体的控制。而对授权主体的不正当行为如何控制呢？信息安全的可控性和不可否认性恰恰是通过对授权主体的控制，实现对保密性、完整性和可用性的有效补充，主要强调授权用户只能在授权范围内进行合法的访问，并对其行为进行监督和审查。除了上述的信息安全五特性外，还有信息安全的可审计性、可鉴别性等。信息安全的可审计性是指信息系统的行为人不能否认自己的信息处理行为。与不可否认性的信息交换过程中行为可认定性相比，可审计性的含义更宽泛一些。信息安全的可鉴别性是指信息的接收者能对信息的发送者的身份进行判定。它也是一个与不可否认性相关的概念。

2. 信息安全的内容

1）从结构层次看

信息安全内涵从安全结构层次划分，包括物理安全、安全控制和安全服务三个方面。物理安全是系统安全的基本保障，是信息安全的基础。安全控制是指控制和管理存储、传输信息的操作与进程，是在网络信息处理层次上对信息进行初步的安全保护。安全服务是指在应用层对信息的保密性、完整性、真实性等进行保护和鉴别，防止受到各种攻击和威胁。

2）从内容方面看

信息安全内涵从其主要内容划分，包括物理安全、网络安全、系统安全、信息安全和管理安全5个方面。物理安全既包括计算机网络设备、设施、环境等存在的安全威胁，也包括在物理介质层次上的存储和传输存在的安全问题。网络安全包括结点安全、运行安全和线路安全。系统安全包括硬件安全和软件安全。信息安全是指系统中存储、传输和交换信息的保密性。管理安全包括用户的同一性检查、使用权限检查和建立运行日志等内容。

1.2 信息安全体系

本节将介绍信息安全体系结构、信息安全管理体系、信息安全测评认证体系和信息安全研究体系。