高等学校计算机专业规划教材
国家自然科学基金资助项目教材

信息通信技术供应链安全

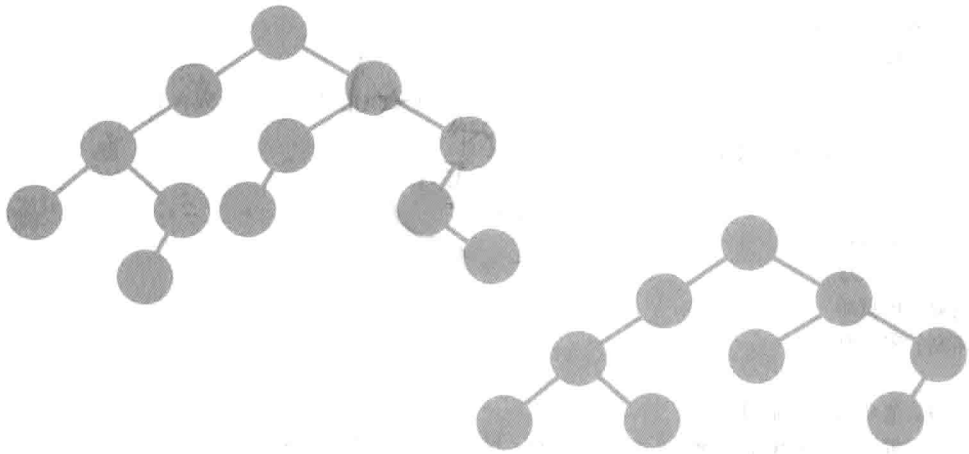
吴世忠 江常青 彭勇 陈冬青 陆天波 编著

清华大学出版社

高等学校计算机专业规划教材

信息通信技术供应链安全

吴世忠 江常青 彭勇 陈冬青 陆天波 编著



清华大学出版社
北京

内 容 简 介

本书主要介绍与信息通信技术供应链相关的主题，全书共10章，可分为四大部分，首先介绍信息通信技术供应链相关概念及其面临的安全威胁；然后阐述信息通信技术供应链的安全战略与实践、安全模型与标准规范；接着详细讨论了硬件供应链与软件供应链的安全风险与应对，采办与外包的安全理论及实践；最后分析了我国当前面临的信息通信技术供应链的安全风险，提出了保障我国信息通信技术供应链安全的对策和建议。

本书内容丰富，专业性强，讲解深入透彻，所研究的领域较为前沿，可以作为高等院校信息安全、软件工程、计算机、通信等专业的教学参考书，也可供我国信息技术供应链安全决策者、研究人员及其他相关人员参考。

图书在版编目（CIP）数据

信息通信技术供应链安全/吴世忠等编著. --北京：清华大学出版社，2014
高等学校计算机专业规划教材
ISBN 978-7-302-36418-4

Ⅰ. ①信… Ⅱ. ①吴… Ⅲ. ①通信技术－信息产业－供应链管理－研究 Ⅳ. ①F49

中国版本图书馆CIP数据核字(2014)第098544号

责任编辑：龙启铭
封面设计：何凤霞
责任校对：焦丽丽
责任印制：宋　林

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 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：18.5　　**字　　数**：428千字
版　　次：2014年8月第1版　　**印　　次**：2014年8月第1次印刷
印　　数：1～2000
定　　价：39.00元

产品编号：057562-01

前言

信息通信技术供应链是电力、石油石化、核能、航空、铁路、公路、水利、医疗等国家关键基础设施的生命线，对国家安全和国民经济至关重要。随着云计算、物联网、移动互联网的快速普及和广泛应用，一方面信息通信技术已成为现代供应链中不可或缺的组成部分，现代供应链在很大程度上依赖信息通信技术来实现其功能和作用；另一方面信息通信技术本身就是一套完整的供应链，除了关注传统供应链物流层面的安全威胁，更加强调设计、制造、安装、维护、升级等环节的安全风险，以及计算机和通信网络的安全性。显而易见，作为供应链基石的信息通信技术供应链如果不安全，那么所有其他供应链实质上也不安全。

信息通信技术在全世界范围内的发展日新月异，从信息通信技术供应链自身来看，由于其涉及的软硬件漏洞和攻击面日益增加，使得信息通信技术中固有的脆弱性也将随之进入到供应链系统，所以只要有供应链的地方，原则上都有受到破坏的可能；从外部环境来看，目前漏洞挖掘和系统渗透等攻击技术不断智能化，APT 等攻击方法不断创新，攻击人员能力明显提升，使得针对信息通信技术供应链的攻击事件屡见不鲜，而这些事件呈现危害范围广、后果严重、损失巨大等特点。因此，对信息通信技术供应链安全问题的研究已成为当前信息安全工作的重中之重。

信息通信技术供应链的独特性给全世界带来了很多新的安全挑战，而且对该类供应链的攻击将直接威胁国家关键基础设施的安全。因此，确保信息通信技术供应链的安全应作为强化国家信息安全保障的一项基础性工作。面对日益复杂的供应链，全世界，尤其是技术发达、网络化程度高的国家，已逐步开始将信息通信技术供应链安全列入其国家信息安全战略部署并加以实施。其中，美国在其国家网络安全综合计划中将“全球供应链安全”作为第 11 个任务，2012 年又发布全球供应链安全国家战略，通过建立完善的信息产品进出口安全审查机制等一系列措施来保障信息通信技术供应链安全。

与发达国家相比，我国对信息通信技术供应链安全的研究及实践尚处起步阶段，而且亟待完善信息产品安全审查体系等相关措施。因此，开展对国内外信息通信技术供应链安全态势、信息通信技术供应链涉及的具体领域、其他国家的战略和措施等进行系统性研究，有利于提高我国信息通信技术供应链安全保障能力，这也正是撰写本书的出发点。本书运用归纳总结、

逻辑推理与案例研究相结合的方式，对信息通信技术供应链安全威胁、世界各国相关战略、安全模型、相关标准、硬件供应链、软件供应链、采办安全和外包安全等进行研究，并针对我国信息通信技术供应链安全问题提出了探索性的建议。经过三年的调研与撰写，作者编写了本书，以供广大读者学习参考。

本书内容翔实、丰富、专业性强。全书共分为10章，基本内容分为四部分。第一部分包括绪论和信息通信技术供应链面临的威胁两章。绪论主要介绍了信息通信技术供应链相关概念，信息通信技术供应链面临的威胁具体阐述了相关的信息威胁、系统威胁和网络威胁。第二部分是信息通信技术供应链安全态势研究及分析，包含国外供应链安全战略、信息通信技术供应链安全模型和信息通信技术供应链安全标准共三章。从宏观层面讲述了部分发达国家信息通信技术供应链安全战略与实践、主要的供应链安全模型以及目前存在的供应链安全标准等。第三部分是信息通信技术供应链的产品及服务安全。在信息通信技术产品层面，包含硬件供应链安全和软件供应链安全两部分，介绍了硬件和软件供应链安全问题并提出了应对措施；在信息通信技术服务层面，包括采办安全和外包安全，主要阐述了采办和外包的相关理论模型和实践。第四部分针对我国信息通信技术供应链安全面临的严峻形势，专门阐述了我国信息通信技术供应链发展现状，分析了我国当前面临的信息通信技术供应链风险，并根据我国的国情提出了降低供应链风险、保障信息通信技术供应链安全的对策和建议。另外还专门对华为与中兴的案例进行了分析与总结，最后对信息通信技术供应链新技术领域的应用进行了探索研究。

本书的撰写和出版，得到了中国信息安全测评中心的支持和相关实验室的积极配合，得到了国家自然科学基金项目(项目编号：61170273)和中国民航信息通信技术科研基地开放基金项目(项目编号：CAAC-ITRB-201201)的支持。在本书出版之际，由衷感谢国家信息安全各主管部门和社会各界专家和学者的支持、推荐和鼓励。还要感谢北京邮电大学的赵玲玲、许兵、郭晓博、姚普欣、杜士贤、张信媛给予的极大帮助。

本书编写过程中参阅和研究了许多资料，包括相关领域的国内外著名专家、学者的经典著作和研究论文，主要参考文献已列于每章之后，在此对这些作者表示感谢。

限于作者水平，书中欠妥和纰漏之处在所难免，敬请读者和同行批评指正，联系方式：chendq@itsec.gov.cn，lutb@bupt.edu.cn。

作　者

2014年5月

目录

第1章 绪 论

1.1 供应链概念

“供应链”(Supply Chain)的概念产生于20世纪80年代初期。20世纪90年代后期以来,“供应链”成为非常热门的词汇。1963年美国成立的物流管理协会(Council of Logistics Management, CLM),是全球物流和供应链管理领域个人参与的最有影响的行业组织。2005年1月1日,该协会正式更名为美国供应链管理专业协会(Council of Supply Chain Management Professionals, CSCMP),域名也从 www.clml.org 更名为 www.cscmp.org,这标志着全球物流进入供应链时代。当年,该协会的物流突出贡献奖得主马丁·克里斯托弗有一句名言:“在21世纪,市场竞争将是供应链和供应链的竞争,而不是企业和企业的竞争。”畅销书《世界是平的》曾将供应链列为碾平世界的第七大动力,并以沃尔玛为例详细阐述了供应链的巨大威力[TF2006]。

关于“供应链”一词,存在各种各样的解释。美国供应链管理专业协会2006年10月更新的《供应链与物流术语》的定义是:供应链始于未加工的原材料,终于使用产品的最终用户,供应链将许多企业联结在一起。从原材料的采购到成品送到用户手中的物流过程中实体和信息的交换。所有卖主、服务提供商以及客户在供应链中相互关联[SCLTG2006]。

2012年1月美国《全球供应链安全国家战略》给出的描述是:全球供应链提供食品、医药、能源和产品来支持我们的生活。许多不同的实体负责或者依赖全球供应链,这些实体包括监管部门、执法部门、国营及私营贸易部门和其他国内外合作者。全球供应链系统依赖于运输基础设施、信息通信技术、互联网和能源网络的相互关联。这种关联性能够促进经济活动,然而也会在广泛的地理区域或者产业界引起局部或者区域性破坏传播风险[NSGSCS2012]。

维基百科给出的定义是:供应链是以完成从采购原材料,到制成中间产品及最终产品,然后将最终产品交付用户为功能的、由一系列设施和分布选择形成的网络。

我国国家标准《物流术语》(GB/T-18354-2006)的定义是:生产及流通过程中,涉及将产品和服务提供给最终用户活动的上游与下游企业所形成的网链结构。

随着全球供应链的逐渐发展,供应链安全问题也日益突出起来。为确保供应链的安全,目前世界各个国家及地区纷纷制定了自己的供应链规范。

2003年,美国推出“海关-商业伙伴反恐计划”(Customs-Trade Partnership Against Terrorism, C-TPAT),包括一系列获得广泛认同和支持的要求。C-TPAT目前仍然是美

国最主流的法案，若符合此项要求，在与美国相关的贸易中可获得相关便利。

在美国制定相关规范的同时，国际组织也制定了通用的国际标准，其中包括全球贸易安全与便利标准架构(SAFE)与 ISO/PAS 28000 标准。

相比于美国和国际组织，欧盟制定的供应链的规范优质企业认证(AEO)和《国际船舶和港口设施保安规则》(International Ship and Port Facility Security Code，ISPS Code 或 ISPS 规则)相对较晚，但这也为制定欧盟的规范提供了更多的参考。

由于经济发展和政治体制的原因，亚洲和大洋洲地区并没有形成较为统一的供应链规范体制。各国呈现“百花齐放，百家争鸣”的景象。亚太地区的供应链规范主要参考 C-TPAT 和 AEO，由于没有统一的规范和完整的体系，不同国家和地区的供应链活动产生了一系列的问题。

在世界各国和地区制定自身供应链规范的同时，企业联盟也同时公布了自己的规范。其中较著名的是 TAPA 制定的 FSR。

在南美及拉丁美洲地区，还存在一个安全商业联盟(BASC)，它是由一家北美公司成立的一个自愿性的组织。BASC 的主要参与者是拉丁美洲公司。有人提议引入美国对供应链采取的安全措施，以防范关税风险、走私毒品、盗窃及散发受污染货物等。

1.2 ICT 供应链定义

ICT(Information and Communication Technology)通常被称为信息通信技术。ICT 是当今世界发展最迅速、渗透最广泛、应用最成熟的新兴技术。2011 年 12 月，美国巴特尔(Battelle)慈善信托基金会发布了《2012 全球研发经费预测》报告[GFF2011]，该报告认为过去 20 年里，ICT 已成为许多领域的关键创新因素，并极大地改变了全球范围内的社会行为。表 1-1 列举了近年来世界部分国家及地区政府部门为促进 ICT 产业发展所采取的一系列政策或措施。

表 1-1 近年部分国家和地区 ICT 计划

国家和地区	计划或战略	起止年份	主要内容或目标
美国	国家宽带计划	2009	保证在美国人人都有宽带接入
加拿大	扩大宽带接入	2009—2012	投入 2.25 亿加元用于扩大宽带接入
欧盟	数字化议程	2009—2020	2020 年，欧盟至少一半的家庭宽带速率超过 100Mbps
英国	数字英国	2009	建设高速光纤网络，全面升级数字广播
法国	数字法国	2009—2020	构建“连接全国居民的宽带网”和“ICT 数字支柱产业”；发展固定和移动宽带，推广数字化应用和服务，扶持电子信息企业
德国	数字化德国	2010—2015	促进物联网、服务联网、云计算、3D 技术等新技术的研发，改善数字世界的安全与可信度
芬兰	立法保证宽带接入	2010	到 2015 年年底前，要让至少 100Mbps 速度的宽带接入成为芬兰人的法定权利

续表

国家和地区	计划或战略	起止年份	主要内容或目标
澳大利亚	光纤进家庭	2009	组建一个全国性高速光纤宽带网络，将耗资434亿澳元
巴西	国家宽带计划	2010—2015	投入57亿美元的资金建设国家宽带
日本	i-Japan战略	2009—2015	发展电子政府和电子地方自治体，推动医疗、健康和教育的电子化
韩国	IT韩国	2009—2013	把信息整合、软件、主力信息、广播通信、互联网5个领域确定为信息核心战略领域
新加坡	智慧国2015计划	2006—2016	高速宽带网将遍布全国
中国	2006—2020年国家信息化发展战略	2006—2020	把信息通信技术的应用和发展作为一个战略议程；加快建设宽带、融合、安全、泛在的下一代国家信息基础设施，推动信息化和工业化深度融合，推进经济社会各领域信息化[GJXX2006]
	国务院关于大力推进信息化发展和切实保障信息安全的若干意见	2012	实施“宽带中国”工程，构建下一代信息基础设施；推动信息化和工业化深度融合；鼓励大中型企业开展网络采购和销售，加强供应链协同运作[GWY2012]
	中国共产党第十八次全国代表大会报告	2012	建设下一代信息基础设施，发展现代信息技术产业体系，健全信息安全保障体系，推进信息网络技术广泛运用
	中共十八届三中全会公报	2013	设立国家安全委员会，完善国家安全体制和国家安全战略，确保国家安全

ICT供应链，包括硬件供应链和软件供应链，通常涵盖采购、开发、外包、集成等环节。其最终的安全很大程度上取决于这些中间环节，涉及到终端用户、政策制定方、采购方、开发方、系统集成方、网络提供方以及软件/硬件供应商等。ICT供应链是所有其他供应链的基础，实际上，它们是“供应链的供应链”。几乎所有的供应链都依赖相互交汇的计算机和通信技术[BAH2012]。

在美国马里兰大学发表的《建立网络供应链保障参考模型》报告中，提出了网络供应链的概念，可以称为ICT供应链的另一种表述形式。网络供应链是指包含于或使用网络基础设施的关键行动者的全部集合，包括终端用户、政策制定者、采购专家、系统集成商、网络提供者以及软件/硬件供应商。这些用户/供应商之间通过组织和过程层互动来计划、构建、管理、维护和保护网络基础设施。与实体供应链相类似，网络供应链是一个端到端的过程。该过程始于软件开发商，其职责与实体供应链上的供应商类似。实体供应链上采购部门、生产和分发管理者的角色与网络供应链上的政策制定者和系统集成商、硬件/组件开发商、软件供应商的角色极其类似。实体供应链上的消费者与网络供应链上的操作者/终端用户相对等[SAICM2009]。

相对于传统领域的供应链，ICT供应链有其特殊性。ICT系统通常是“采购+开发+集成”模式，其最终用户感知到的安全很大程度上取决于采购、开发和集成等这些中间环

节，涉及更多的外包方、集成商以及其他第三方等，这些供应商的安全素养、流程和产品质量的重要性愈发地凸显出来。

简要来说，ICT 的供应链的特点包括：使用的设备多，通常包括硬件、软件等众多组件；项目涉及全球很多地区的供应商、生产厂、集成商、运输服务商等；ICT 业界主要依靠采购成熟的商业组件和设备，对供应链的依赖性更强；设备之间有很多通信功能等关联关系；设备的功能和质量很难被完全地测试、测量和直观地展示出来，等等。

ICT 供应链作为特殊的供应链，ICT 供应链风险管理较一般物流供应链风险管理涉及的方面更广，更加复杂，如图 1-1 所示。

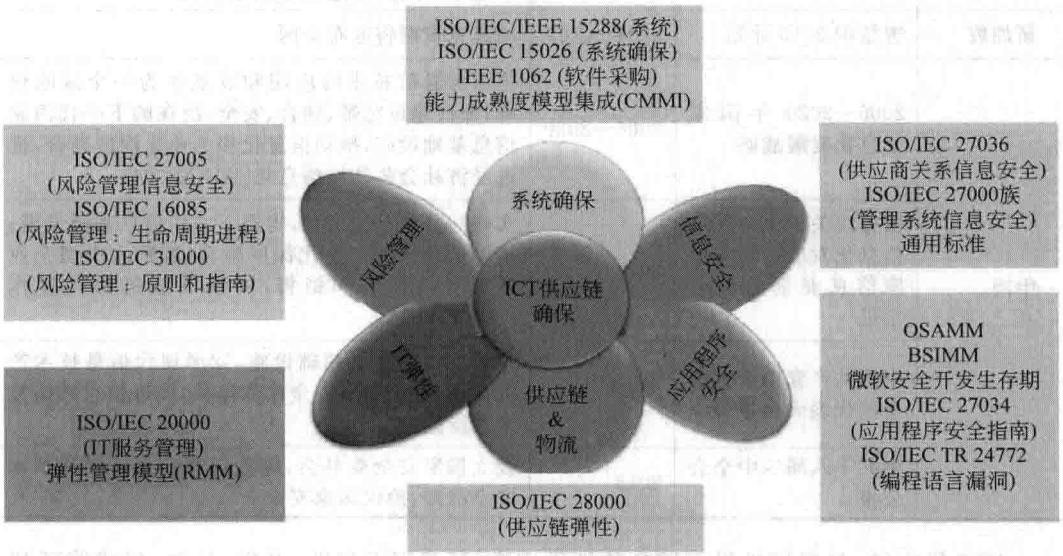


图 1-1 ICT 供应链风险管理

1.3 ICT 供应链安全挑战

2011 年 2 月，伊朗突然宣布暂时卸载其首座核电站“布什尔核电站”的核燃料，因为布什尔核电站遭到“震网”病毒攻击，使其 1/5 的离心机报废。事实上，自 2010 年 8 月该核电站启用后就发生连串故障，原因是核电站遭一种名为“震网”(Stuxnet)的蠕虫病毒入侵。该病毒沿着供应链侵入了伊朗工厂企业甚至进入西门子为核电站设计的工业控制软件，并可夺取对一系列核心生产设备尤其是核电设备的关键控制权。整个攻击过程如同科幻电影：由于被病毒感染，核电站的监控录像被篡改。监控人员看到的是正常画面，而实际上离心机在失控情况下不断加速而最终损毁。

震网的攻击载体直指西门子公司的 SIMATIC WinCC 系统。这是一款数据采集与监视控制(SCADA)系统，被广泛用于钢铁、汽车、电力、运输、水利、化工、石油等核心工业领域，特别是国家基础设施工程。该系统运行于 Windows 平台，常被部署在与外界隔离的专用局域网中。震网病毒之所以能够成功进入伊朗核电站与外界隔离的专用网中，并

不是通过人们常见的互联网，而是利用了ICT供应链的漏洞，提前被植入系统中。

此后，伊朗还曾发现一种名为“毒区(Duqu)”的数据窃取病毒，针对的也是工业控制系统，但它并没有危害伊朗核能实验室和工业设施内的电脑。

2012年5月，国际电信联盟和多家电脑安全公司宣布，一种名为“火焰”的破坏力巨大的全新电脑恶意软件被发现，它是迄今为止世界上最复杂的计算机病毒。俄罗斯IT安全公司卡巴斯基实验室在当天的报告中说，“火焰”已侵入伊朗、以色列、巴勒斯坦、叙利亚、黎巴嫩和沙特等中东国家数百台电脑，全球受感染电脑估计在1000～5000台之间。

该消息随即得到伊朗方面的证实。该国官员称，“火焰”曾侵入伊朗一些行业的电脑，“所幸被及时发现”。该病毒企图收集伊朗石油行业的关键信息，曾在今年4月份对伊朗石油网络系统造成影响，导致当局短暂切断石油部、石油出口数据中心等机构与互联网的连接。

2012年5月，美国参议院军事委员会(Senate Armed Services Committee)发布报告称，历时一年的调查发现，在2009—2010年间，美国国防部供应链中共发生1800起假冒零部件事件[SASC2012]。美国空军C-130J运输机采用了假冒电子零件，特种行动直升机和海军的“海神”(Poseidon)侦察机的组件中也有假冒电子零件。报告称：“一个电子部件的失灵可能导致士兵、海员、飞行员或海军陆战队在危急关头命悬一线。”“不幸的是，大量假冒电子部件明显加大了安全预防工作的难度。”除影响国家安全并造成安全风险外，假冒电子部件还增加了系统成本。以美国导弹防御局一个导弹为例，更换其中一个假冒存储设备的成本便高达270万美元。

2013年1月7日至16日，在短短的10天之内，美国波音787“梦想飞机”就出现了7次程度不同的事故，引发了人们对其安全性的强烈质疑。随后，美国、日本、波兰、卡塔尔、印度、智利、埃塞俄比亚等国家的8家航空公司全部宣布停飞787客机。专家指出，波音787客机连发电瓶起火、燃油泄漏、刹车故障、驾驶舱玻璃裂缝、飞机连接线等故障，其背后可能是全球“碎片化”供应链制造模式惹的祸，这给飞机制造的质量管控带来了严峻挑战。787客机采用外包制造，大部分零部件供应商分布在全球各地，有媒体称欧航高管认为波音把技术用到极限，外包也用到了极限。波音出于降低成本的考虑将模块外包时埋下了隐患，模块承包商势必也将自己的任务进一步分解外包，依此类推，直至产品细化到一个铆钉。一级承包商以下的工作是波音公司无法控制的，所以当下面任何次一级生产出现问题的时候，就像推倒了多米诺骨牌，导致整个飞机出现故障。

众多特点给ICT供应链来了很多新的威胁与挑战。从软件工程过程中出现的软件缺陷，到供应商内部的恶意人员，到可能的商业间谍甚至国家网络战等各种各样的威胁，针对目标的供应链的攻击已成为攻击其ICT系统的一个重要路径。

ICT供应链的实际活动开始于采购，但是很少有采购系统可以在供应链中完整地跟踪最终产品，不管它是制造电子部件的原材料，由电子部件装配而来的电路板，还是构成一个子系统的电子部件均是如此。大多数的项目办公室、制造商和供应商都视自己的责任为：从他们的供应者那些获得物资、实施他们负责的行动(合同的或者官方的)、向供应链的下一阶段传送产品。

当事者通常不会考虑全球性的系统评估，只看眼前的工作：部件只要能简单地工作，