Innovative Research

中国联通研究院创新研究系列丛书

云计算安全技术与应用

张尼 刘镝 张云勇 李正 陈豪 等 编著

人民邮电出版社
POSTS & TELECOM PRESS

nnovative Research

中国联通研究院创新研究系列丛书

云计算安全技术与应用

张尼 刘镝 张云勇 李正 陈豪 等 编著

人民邮电出版社

北京

图书在版编目（CIP）数据

云计算安全技术与应用 / 张尼等编著. -- 北京 : 人民邮电出版社, 2014.5
（中国联通研究院创新研究系列丛书）
ISBN 978-7-115-34309-3

Ⅰ. ①云… Ⅱ. ①张… Ⅲ. ①计算机网络－安全技术－研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2013)第315105号

内 容 提 要

本书从当前的云计算发展现状分析云计算的特征、机遇与挑战，引出云计算安全的内涵，并从安全事件出发，分析云计算面临的安全威胁和安全需求。在此基础上，分析标准组织的主要工作，并从云服务域、云终端域、云监管域的角度详细阐述如何构建云计算安全体系架构，梳理体系架构中涉及的关键技术，同时分析了云服务运营必须满足的安全需求。随后分享了政府部门的云计算安全举措，云服务提供商和运营商的云计算安全解决方案及产品情况。最后分析了云计算安全的发展趋势。

本书可作为高等院校信息安全专业本科生和研究生的参考教材，也可作为云业务提供商职员、网络信息安全领域研究人员的参考书。

◆ 编　著　张　尼　刘　镝　张云勇　李　正　陈　豪　等
责任编辑　邢建春
责任印制　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：10.75　　2014 年 5 月第 1 版
字数：196 千字　　2014 年 5 月北京第 1 次印刷

定价：49.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

丛书编委会名单

本书编写组

主编： 张　尼　刘　镝　张云勇　李　正　陈　豪

编著： 王笑帝　申珉宇　胡　坤　宫　雪　刘明辉

陶　冶　童　博　房秉毅　陈清金　魏进武

郭志斌　程　莹　雷　磊　王智明　邓　浩

陈晓明　贾智宇　杨绍光　刘　露　毋　涛

李璐颖　黄存兰　马元英

序

云计算是互联网计算的一种商业模式，其凭借集中、发布、服务等特性使计算资源成为向大众提供服务的计算基础设施。云计算正在改变信息产业的现有形态，对信息技术及应用产生深远的影响。云计算的广泛普及对工业化和信息化的快速融合及国民经济发展均有积极的促进作用。

为了有效发挥云计算的优势，加快其在 ICT 领域的布局，世界各国均在大力推行云计算战略。2011 年 11 月，美国政府发布了《联邦政府云计算战略》，规定在所有联邦政府项目中优先使用云计算技术。2012 年 9 月，欧盟启动了云计算战略计划，鼓励欧盟及其成员国加大云计算的研发投入，以带动欧盟经济增长，创造就业。我国政府一直高度重视云计算的研发及示范性应用，《国家十二五规划纲要》和《国务院关于加快培育和发展战略新兴产业的决定》都把云计算列为重点发展的战略性新兴产业，以引领我国云计算技术与应用达到国际先进水平。

从云计算提出者的观点来看，云计算的核心内涵强调“云计算的边界是由经济原理决定，而不是由技术原理决定”。即部署大规模的云计算平台不存在技术障碍，关键在于用户的需求及其愿意为支撑大规模云计算平台运行所付出的费用。云计算与传统的业务模式相比具有开放性、动态边界、虚拟性、多租户、数据的所有权和

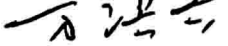
管理权分离、资源相对集中等特点，这使得云计算在技术、管理和法律等方面面临新的安全挑战。此外，云计算系统中存放着海量用户数据，对攻击者来说具有更大的诱惑力，云计算系统的安全需求比以往的 IT 系统更为迫切。

云安全可分为云计算技术在信息安全领域中的应用与云计算平台自身的安全两个方面。其中前者可称为云安全服务，例如，通过强大的云端能力快速实现地毯式搜索，查杀病毒。后者则包含 4 种形态：一是安全的云，其目的是保障云中租户自身安全及数据安全；二是可靠的云，主要是要确保云计算平台不会轻易出现故障，保证云业务的连续性与服务质量，注重云计算平台物理安全、配置安全、审计、评估、备份等环节；三是可信的云，强调云计算服务提供商（CSP）如何能保证自身不侵犯云中租户的隐私，使租户认定 CSP 是可信的；四是可控的云，主要是保证云中资源、操作的可管、可控，避免云端能力被网络安全攻击者所滥用，使云成为作恶的平台。

事实上，安全的云、可靠的云是 CSP 所关注的事情，因此目前的研究较为深入，成果也较多；但可信的云、可控的云则是监管者对 CSP 所提出的要求：一个优质、成熟的 CSP 必须具备可信、可控的安全能力。由于其研究动力不在于 CSP，因此当前在这两方面的成果较少。但是，如果 CSP 忽视可信的云，则迟早被高端用户及对隐私保护要求高的用户所抛弃；如果 CSP 忽视可控的云，那么监管者也将会因为各种突发事件不断地打扰 CSP，CSP 将面临运营危机。毫无疑问，伴随着云计算业务的落地，CSP 将会非常重视云安全问题，安全将成为云计算健康、持续发展的关键。

本书的主要作者张尼曾经是我的博士研究生，他及所在的安全团队在中国联通研究院长期从事信息安全研发工作。近年来，他们又代表联通公司在国内、外标准化组织、国家项目的示范应用中积极开展了安全的云、可靠的云、可信

的云的应用实践。为了迎接云计算发展契机，中国联通研究院撰写了《云计算安全技术与应用》一书，这是对云计算安全技术的内涵、体系架构、关键技术、产业现状及实践的一次深入分析和高度概括，为国内的相关从业人员提供了一份宝贵的参考资料。

中国工程院院士 

序 言

21 世纪以来，云计算逐渐兴起，Amazon、Sun、IBM、Google 等公司纷纷宣布云计算计划，并在云计算的商业应用方面走在了世界前列。2008 年以来，在经济危机的刺激下，全球企业努力寻求节省成本、降低开支的良方妙计。云计算的理念和模式满足了当下 IT 服务提供者和服务使用者的主要需求。

对于服务提供者，云计算满足了其对 IT 资源的高效管理需求，并利于其开拓新的业务和商业模式；对于服务使用者，可以按需获取 IT 资源，节省开支、降低企业运行成本。由于云计算的独特优势，欧美等国政府均大力推广使用云计算。云计算的广泛普及对工业化和信息化的快速融合与国民经济发展均有积极的促进作用。

云计算技术在商业模式、计算模型、用户体验等方面发生重要革新，但是其应用系统架构、用户访问行为仍然沿袭传统 IT 框架。因此，系统软硬件故障、拒绝服务攻击、病毒蠕虫、恶意代码和钓鱼网站等各类传统安全威胁仍然存在，且上述安全问题随系统规模化而被放大。同时，云计算与传统的计算模式相比具有开放性、动态边界、虚拟性、多租户、数据的所有权和管理权分离、资源相对集中、对安全设备的性能和扩展性等方面有新的要求等特点，这使得云计算系统在技术、管理和法律等方面面临新的安全挑战。此外，云计算系统中存放着海量用

户数据，对攻击者来说具有更大的诱惑力。如果云计算系统遭受攻击，将会给云计算服务提供商和用户带来重大损失，云计算系统面临比以往的业务系统更为严峻的考验。因此，随着云计算业务的落地，云计算安全问题成为学术界、产业界争相关注的焦点。

本书从云计算安全的基本定义和内涵说起，归纳云计算技术面临的安全威胁，分析云计算技术的安全需求，提出云计算服务安全体系架构，并分析了云计算服务安全相关的关键技术、标准现状、平台安全运营、产业应用现状等。全书是对云计算安全的一次深度总结和分析。

云计算是一场改变 IT 格局的划时代变革，健康发展的云计算具有极大的产业带动力量，将不断驱动新的产业形态和新的商业模式。未来，云计算将推动中国信息基础设施建设和信息化进程，构建更大规模的生态系统，带动我国 IT 产业的快速发展。

Preface 前言

近几年，云计算技术、应用、市场发展非常迅速，各国政府高度重视云计算发展。其中，美国政府机构正在大力推动云服务和自行构建云服务的计划，美国国防信息系统部(DISA)着手在其数据中心内部搭建云环境，美国宇航局艾姆斯研究中心推出名为“星云”(Nebula)的云环境。在欧盟及欧洲其他国家，越来越多的政府部门、企业、金融部门、医院、服务机构开始采用云计算技术，接受云计算服务。日本政府积极推进云计算的发展，提出了“有效利用信息技术，开创云计算新产业”的发展战略。韩国知识经济部、行政安全部和韩国广播通讯委员会于2011年联合公布了《搞活云计算综合计划》。新加坡政府明确提出，要在原来“智慧城市”的基础上，以云计算技术和方法推动智慧国家的建设。在中国市场，云计算逐步被越来越多的企业和机构采用，市场规模也从2009年的92.23亿元增长到2012年的606.78亿元，年均复合增长率达87.4%。

云计算已经普及并成为IT行业主流技术，其实质是在计算量越来越大、数据越来越多、越来越动态、越来越实时的需求背景下催生出来的一种基础架构和商业模式。如同其他新技术或新业务模式一样，云计算会创造新的机遇，同时也带来了新的风险。云计算的发展对传统计算模式和商业服务模式带来了巨大冲击，因此也带来了互联网网络资源、业务资源、用户资源在应用模式上的重大变化。与此同时，在云环境下，多租户、资源共享、数据存储的非本地化、承载业务类

型的多元化以及网络带宽的快速增长也对传统安全提出巨大挑战。

云计算环境下既包括一些通用的安全需求，如租户的接入控制、认证等，也包括随着虚拟化、分布式业务数据存取及多租户业务等引入而产生的一些特殊安全需求，如数据隔离、业务隔离、隐私策略及安全分配的业务安全策略等。此外，云计算服务滥用也会引发特殊的安全问题，如云计算所提供的弹性、可扩展的资源有可能被当作恶意的网络攻击工具，或被当作垃圾和有害信息的传播渠道。

对于各行各业的用户而言，无论是结合自身需求构建内部私有云，还是构建提供对外服务的公有云，都需要考虑云计算环境下的安全威胁，并在云中使用完善的安全措施，否则，云中的特性及云提供的服务不仅无法控制，而且还将对国家、企业、用户带来严重的安全威胁。

本书以此为背景，从云计算安全的基本定义和含义说起，归纳云计算技术面临的安全威胁，分析云计算技术的安全需求，提出云计算服务安全体系架构，并分析了云计算服务安全相关的关键技术、标准现状、平台安全运营、产业应用现状等。最后，结合信息产业发展现状对云计算安全发展趋势进行展望。本书内容可以为私有云及公有云的部署提供有益参考，对于完善云计算技术体系，保障云计算技术推广应用具有重要的意义。

本书结构如下：全书共 8 章：第 1 章介绍了云计算的核心概念和基础知识，包括云计算的定义、特征、服务模式、部署方式、行业应用等；第 2 章对云计算安全进行解读与剖析，并将云计算安全分成云计算服务安全与云计算技术在安全领域的应用两个类别，并以后者为重点开展下文；第 3 章讨论了云计算发展过程中具有代表性的安全事件，同时归纳出云计算面临的安全威胁及安全需求；第 4 章介绍国内外主流标准组织中的云计算安全工作的进展；第 5 章从运营商的视角出发，构建云计算安全体系架构，并从云服务域、云终端域、云监管域 3 个维度阐

述如何保证云计算服务的安全；第 6 章探讨了云计算服务在运营过程中应该注意的安全问题及其解决措施；第 7 章从政府部门、厂商、云服务商角度介绍云计算安全实践工作；第 8 章对云计算安全的后续发展进行展望。

本书适合各水平层次的云计算用户，尤其适合云服务商职员、网络信息安全领域研究人员，以及希望了解更多云计算安全知识的从业者和学生参考阅读。

本书具有如下 3 大特色。

1）通俗性

本书介绍了云计算安全的基本知识，涵盖了从相关的技术到实际案例部署相关的知识，读者只需具备基础的 IT 领域知识即可。每章的标题就是对该章内容的高度概括，在接下来的内容中对其进行的解释已尽可能做到了准确、翔实。

2）完整性

本书从云安全架构、云安全技术细节到具体安全应用场景、应用案例等方面都进行了周详的论述。

3）实用性

本书紧密结合实际，对云安全的背景、需求、技术、运营、部署应用等各方面进行分析和论述。

本书由丛书编委会负责策划和统稿。第 1 章、第 3 章由张云勇、李正、王笑帝编著，第 2 章、第 5 章由刘镝、李正、陈豪编著，第 4 章、第 8 章由张尼、陈豪编著，第 6 章、第 7 章由张尼、刘镝、申珉宇编著。

参加研究和写作的成员还有：胡坤、宫雪、刘明辉、陶冶、童博、房秉毅、陈清金、魏进武、郭志斌、程莹、雷磊、王智明、邓浩、陈晓明、贾智宇、杨绍光、刘露、毋涛、李璐颖、黄存兰、马元英、郭玉华、熊微。

本书能够出版，需要感谢中国联通研究院刘诚明院长、陈赤航副院长、信息

室孙兆欣主任、匡斌副主任、范云杰编辑，中国联通集团技术部裴小燕经理、王明会经理、彭久生经理、贾川、周晓霞、张文钺、石谊娜，中国联通集团网络公司运行维护部孙志光经理、万玉海经理、王翔、吕东芳，中国联通集团信息化事业部娄瑜经理、卢浩洋、刘险峰，北京邮电大学黄韬、姚海鹏、郭达副教授、四川大学计算机学院彭舰院长的帮助。

本书凝聚了笔者长期的安全实践经验以及研究思考的成果。在本书的编写过程中广泛收集了国内外相关材料，参考了一些最新论著，并引用了部分材料，在此向其著作人表示感谢。人民邮电出版社的邢建春编辑为此书倾注了大量的心血，在此致以诚挚的谢意。

本书内容是作者的大胆探索和思考，仅代表个人观点，与任何机构的立场无关。我们希望通过大家的共同努力，理清现阶段云安全技术的发展，为业务创新发展贡献一份力量。由于作者水平有限，加之时间仓促，书中难免有错误、不当之处，恳请广大专家、学者不吝批评指正。

作者

2014 年 2 月于北京

目录

Contents