HZ BOOKS
华章科技

· 网络空间安全技术丛书 ·

BUILDING THE INFRASTRUCTURE FOR CLOUD SECURITY

A Solutions View

云安全基础设施构建

从解决方案的视角看云安全

[美] 罗古胡·耶鲁瑞（Raghu Yeluri） 恩里克·卡斯特罗－利昂（Enrique Castro-Leon） 著
詹静 庄俊玺 张建标 译

本书以可信计算技术为基石，全面介绍了建立云安全基础设施相关的应用模型、解决方案、具体实现所需的软硬件组件

机械工业出版社
China Machine Press

· 网络空间安全技术丛书 ·

云安全基础设施构建

从解决方案的视角看云安全

BUILDING THE INFRASTRUCTURE FOR CLOUD SECURITY

A Solutions View

[美] 罗古胡·耶鲁瑞 (Raghu Yeluri) 恩里克·卡斯特罗-利昂 (Enrique Castro-Leon) 著 詹静 庄俊玺 张建标 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

云安全基础设施构建——从解决方案的视角看云安全 /（美）罗古胡·耶鲁瑞（Raghu Yeluri），（美）恩里克·卡斯特罗-利昂（Enrique Castro-Leon）著；詹静，庄俊玺，张建标译 . —北京：机械工业出版社，2017.8
（网络空间安全技术丛书）
书名原文：Building the Infrastructure for Cloud Security: A Solutions View

ISBN 978-7-111-57696-9

I. 云… II. ①罗… ②恩… ③詹… ④庄… ⑤张… III. 计算机网络－网络安全 IV. TP393.08

中国版本图书馆 CIP 数据核字（2017）第 194025 号

本书版权登记号：图字：01-2017-2052

云安全基础设施构建——从解决方案的视角看云安全

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：陈佳媛　　责任校对：李秋荣
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2017 年 9 月第 1 版第 1 次印刷
开　　本：186mm×240mm　1/16　　印　　张：13.75
书　　号：ISBN 978-7-111-57696-9　　定　　价：49.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

华章科技
HZBOOKS | Science & Technology

Preface 序

随着信息技术与产业的高速发展和广泛应用，人类社会进入了信息化时代。在信息化时代，一方面信息技术和产业高速发展，呈现出空前繁荣的景象。另一方面危害信息安全的事件不断发生，形势是严峻的。信息安全事关国家安全、事关社会稳定。因此，必须采取措施确保我国的信息安全。

当前，云计算、大数据等新技术突飞猛进地发展，运用广泛。这些新技术的发展和应用给人们带来极大的便利，但同时也给信息安全提出了一些新的挑战。

云计算是面向服务的计算：基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。云计算旨在使计算像水、电、油一样，成为公共基础资源，因此可以极大地降低用户的开支。但是，面向服务的计算在工作模式上必然是资源共享，而资源的共享将引发诸多信息安全问题。例如，基础设施和平台安全问题：云计算有几乎无限的计算资源（基础设施、平台和软件），但是用户不知道这些资源是否是可信的。服务安全问题：云计算有几乎无处不在的服务，但是用户不知道这些服务是否可信。数据安全问题：云计算有几乎无限的存储空间，但是用户不能感知自己数据的存在、不知道自己的数据存储在哪里、更不能控制自己的数据。于是，用户就不信任云计算，不信任自然就不会应用。

大数据处理与云计算是一对“双胞胎”。一方面，云计算有几乎无限的存储能力。另一方面，大数据需要巨大的存储空间。因此，大数据必然存储在云计算的存储系统中。一方面，云计算有几乎无限的计算能力。另一方面，大数据处理需要巨大的计算能力。因此，大数据必然由云计算系统进行处理。只有这样结合，才是最合理、最节省的方案。由此可见，云计算与大数据的开发应用与安全可信是彼此联系在一起的。

于是，云计算的安全问题也会影响大数据的安全。反过来，大数据带来的隐私保护和密码的工作效率等问题，也会影响云计算安全。

可信计算是一种旨在增强计算机系统可信性的综合性信息安全技术。而且，可信计算特别适用于提高信息系统的基础设施和平台的可信性。很多年前，张焕国教授就提出“可信≈可靠＋安全”的通俗观点。这也就是说，稳定可靠和安全保密是可信性的主要方面。因此，采用可信计算技术增强云计算、大数据系统的可信性，成为一种必然的选择。

中国在可信计算领域起步很早、成果可喜、有很多创新，整体水平处于国际前列。早在 2003 年，武汉瑞达公司就和武汉大学合作开发出中国第一款嵌入式安全模块和第一款可信计算机（SQY14 嵌入密码型计算机），并得到实际应用。

英特尔（Intel）公司是国际可信计算组织（TCG）的发起单位之一，为可信计算做出了重要贡献。为了介绍可信计算技术的新进展和可信计算在云计算基础设施中的安全作用，在英特尔的组织下，ApressOpen 出版了三本可信计算和云系统安全的技术图书，现由机械工业出版社华章公司引进，中文版会在 2017 年 9 月至 2017 年 10 月陆续出版：

①《 A Practical Guide to TPM 2.0 ： Using the Trusted Platform Module in the New Age of Security 》（中文版：《 TPM 2.0 原理及应用指南——新安全时代的可信平台模块》）。TPM 2.0 是 TCG 标准，也是国际标准，并得到中国国家密码管理局的支持。TPM 2.0 扩展了加密算法灵活性，支持中国商用密码算法。

②《 Intel Trusted Execution Technology for Server Platforms ： A Guide to More Secure Datacenters 》（中文版：《面向服务器平台的英特尔可信执行技术——更安全的数据中心指南》）。英特尔用 TXT 技术把以上 TPM 标准和物理机的可信扩展到虚拟环境（VMM）和虚拟机（VM），并结合 Intel VT 虚拟技术把虚拟机的隔离、可信和安全做得更好。

③《 Building the Infrastructure for Cloud Security, A Solutions View 》（中文版：《云安全基础设施构建——从解决方案的视角看云安全》）。在以上 TPM 标准和 TXT 技术基础上，通过远程认证（OAT）和云完整性技术（CIT）把可信扩展到完整云安全基础设施和所有数据中心安全。

这些可信基础设施包括可信软件定义的存储（Trusted SDS）、可信软件定义的网络（Trusted SDN）、可信交换机（Trusted Switch），直至可信软件定义数据中心和基础设施（Trusted SDDC 和 Trusted SDI）。

这些数据中心安全技术可扩展到：大数据安全和隐私保护、端到端物联网的安全、5G 网络安全、智慧城市安全、精准医疗安全和隐私保护等。

所以说，以上三本书是技术上非常相关、由下而上渐进、自然延伸扩展的可信云计算安全图书。

2012 年 6 月，武汉大学和英特尔、与多家企业联合发起成立了中国可信云社区（ChinaSigTC）。宗旨是，基于中国商用密码和可信计算标准，发展中国可信云计算技术与产业。工作方式是，通过开放开源和自主开发，一起研发中国本土化可信云安全解决方案。为全面支持开源和本土开发，英特尔开源了 UEFI BIOS 及其 TPM 2.0 安全模块、TPM 2-TSS 可信软件栈、Tboot TXT 可信启动模块、OAT 开源远程认证技术和 OpenCIT 云完整性技术。这些都与这三本书中的内容密切相关。中国可信云社区也开源了 GMSSL 国密 OpenSSL 等。该社区的活动推动了可信云计算的本土化发展。（相关内容请参考本书附录。）

这三本书也是该社区技术工作的重要参考书。2012 年至 2014 年，该社区的国民技术、中标软、武汉大学与英特尔合作一起开发了支持中国商用密码的 TPM2.0 芯片、BIOS 及其 OS 驱动。2014 年至 2015 年，该社区的华为、浪潮、大唐公司分别与英特尔和武汉大学合作开发出自己的可信云服务器，全面支持 TPM 2.0/TXT、可信虚拟化、远程认证和安全可信管控，并实现了产业化。这些产品的开发和应用，从实践上证明了采用可信计算增强云计算、大数据系统安全是十分有效的。2016 年至今，该社区的大唐公司、英特尔、XSKY、XNET 和武汉大学一起合作开发出可信存储、可信交换机、可信软件定义的数据中心（Trusted SDDC/SDI）。从实践证明可信计算技术完全可以扩展到整个数据中心的所有计算、存储、网络节点并得以统一的 CIT 认证，从而大大提高整个系统的可信性。

全面实现信息系统安全可信，任重而道远，让我们和社区一起将可信进行到底！

为满足社区成员的需要，也为了使广大中文读者能够读到这三本书，在英特尔公司支持下，机械工业出版社华章公司组织武汉大学和北京工业大学的老师把它们翻译成中文并出版发行。其中《 TPM 2.0 原理及应用指南——新安全时代的可信平台模块》由武汉大学的老师翻译，《云安全基础设施构建——从解决方案的视角看云安全》和《面向服务器平台的英特尔可信执行技术——更安全的数据中心指南》由北京工业大学的老师翻译。

这三本书内容丰富、新颖实用，是难得的好书。本书可作为从事信息安全、计算

机、通信、电子信息等领域的科技人员的技术参考书，也可用作信息类专业的教师、研究生和高年级本科生的教学参考书。

相信这三本译著的出版发行将会促进可信计算、云计算安全、大数据处理系统安全等领域的技术交流、进步和产业发展。

由于译者的专业知识和外语水平有限，我们也请了中国可信云社区和英特尔中国技术专家一起校阅，但书中错误在所难免，敬请读者指正，我们在此先致感谢之意。

张焕国（于武汉大学珞珈山）

李彦（于英特尔上海紫竹）

2017 年 8 月

Forword 推 荐 序

在我的职业生涯之中，我扮演过很多角色，从投资银行家到风险投资人再到商业企业家。我很幸运一直处于几大技术浪潮前沿，这些技术浪潮包括大型机向客户机 / 服务器计算的转变、互联网的兴盛，以及现在移动和云计算的兴起。每一次新的浪潮都带来技术颠覆，并且每一次浪潮都会推动生产效率和运营生产力提升到新的水平。然而，随之而来每次新的浪潮也带来了新的安全风险和运营问题。

虚拟化和云技术与以前的技术浪潮并没有什么不同。在过去的 20 年它们带来的最显著的变化就是数据中心转型，而且在节约成本、提升灵活性和业务敏捷性方面都取得了巨大的成效。但与此同时，安全风险态势也发生着显著变化。云环境创建的新平台将组织的所有关键系统、应用和数据汇聚在一起，在本质上导致了风险的集中。这些变化应该引起公司高管们的特别注意。如果没有适当的控制（你能想象到后果），数据中心甚至整个企业会面临灭顶灾难。关键系统和数据可能只需轻触按钮就能被轻易访问、复制或删除。服务器，在过去的 IT 技术中是堆叠的物理设备，而现在可以看成仅仅是文件集。数据中心正在变成为一个可以完全被远程控制的软件抽象（softwore abstraction）。

另外，在这个新的环境中，最高特权被赋予能控制所有虚拟化资源的权力。一个系统管理员或劫持他人权限就能发起一次严重的攻击事件，例如在几分钟之内复制一台虚拟机或删除整个完整的虚拟数据中心。由于各种系统数量庞大，即使简单的配置错误在现在都可能造成严重的宕机事件。同时，由于要求审计新的平台，所以很可能会造成审计失败。

此外还有更多问题，当前技术正在走向软件定义的网络和存储，并产生“软件定

义的数据中心”，这将使风险更加集中，带来更多的安全和合规的挑战。

正是这些根本性的变化，迫使我们需要寻求新的、专门针对这些风险的方法来建立安全和信任链。现在的形势比以往更为严峻，主要基于这些因素：（1）如前所述风险的集中化；（2）攻击变得更加复杂；（3）更高的风险，如内部威胁和数据泄漏、高级外部威胁、特权劫持以及升级持续攻击。一些明显的例子如爱德华·斯诺登泄露美国国家安全局机密文件；美国零售巨头塔吉特公司数以亿计的客户个人信息被窃取；Adobe 公司的攻击导致数千万用户的账户和支付信息泄露，更别提绝密级的源代码泄露。

新的信任链必须从硬件以及虚拟基础设施开始，确保用户能信任在虚拟机上运行的操作系统和各种应用。不论私有云、混合云和公有云上都是如此，以确保荷载所需的策略可以自动制定并执行。同时新的信任链必须与数据安全绑定，确保虚拟机是加密的，除非虚拟机已经运行在授权环境中。

展望未来，云安全（从硬件到数据）将成为云服务快速推广的重要因素。

这本书对寻求为云环境建立安全基石的读者来说尤其值得一读。作为经验丰富的虚拟化、企业架构和安全技术专家，Raghu 和 Enrique 在本书中提供了非常有价值的讨论，包括迁移到云后公司所面临的挑战和云安全问题，应对新的安全需求和安全控制要求的基础设施解决方案组件。

——Eric Chiu，HyTrust 公司董事长及创始人

The Translator's Words 译 者 序

随着云计算技术的深入发展，国内外越来越多的企业和个人用户通过租用云来快速开展业务、随时随地使用服务。然而，由于云计算较之传统网络服务具有多租户租赁、虚拟化共享、数据及计算完全外包等新特点，显见云基础设施的攻击价值更高，安全防范难度也更大。近年来云安全事件更是不断出现，极大影响了用户对云计算的信任程度。

信任是网络空间安全交互的基础，可信计算作为一种向人们提供基于硬件的可信功能及服务的信息系统安全技术，近年来备受关注。可信计算的发展也印证了 IT 技术发展的浪潮，从早期对高可靠、高容错能力服务器的研究，逐步转向对终端节点计算机的安全性研究，以及当前对云计算、物联网、移动互联网和工业控制系统等新兴大规模复杂信息系统的主动、动态的安全保障研究。

本书以可信计算技术为基石，全面介绍了建立安全云基础设施相关的应用模型、解决方案、具体实现所需的软硬件组件。为了填补用户理解的云安全与业界的安全技术之间的空白，本书在介绍当前云计算安全与合规性需求的基础上，详细阐述了如何采用可信计算技术建立云安全基础设施和提供云安全方案，这些方案包括基本的可信计算池 TCP，可信证明平台 TAP，使用地理标记的可信计算池和可信虚拟机，分别用于保护云平台启动完整性，保证云平台可信性能够被验证，保护云边界和保护云虚拟机的完整性。除此之外，本书还对云安全相关的网络安全技术、身份管理控制技术以及安全云爆发技术进行了介绍。对急需了解云安全的读者来说是一本不可多得的专业技术书。

由于原著者都来自 Intel 数据中心、云安全相关一线部门，具有丰富的云安全工程

经验，书中提供了大量可信云技术细节和 Intel 及其合作伙伴的真实技术案例资料，以帮助读者掌握建立可信云基础设施的方法。本书的目标读者包括已经熟悉云计算，了解基本可信计算知识的云基础设施运维人员、应用方案师、系统架构师以及公司高管，通过阅读本书能让他们认识到云安全的重要性，理解和掌握云安全保障方法。

最后，感谢原著者 Raghu Yeluri 以及 Intel 公司首席架构师李彦在本书翻译期间与笔者的讨论，感谢北京工业大学可信计算实验室硕士生王霞、吴欢、蔡磊和杨静等同学为本书所作出的贡献，感谢机械工业出版社的张梦玲和陈佳媛编辑在翻译过程中给予的耐心帮助，感谢国家高技术研究发展计划（No. 2015AA016002）及高等学校博士学科点专项科研基金（No. 20131103120001）对译者在可信云调研过程中的支持，感谢家人在翻译本书过程中的关心和帮助。

詹静

2017 年 6 月 20 日于北京

About the Authors 作者简介

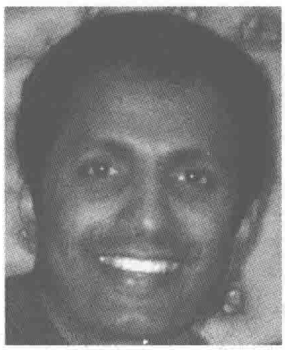
Raghu Yeluri 负责英特尔数据中心和云产品部的安全解决方案架构，主要研究方向是虚拟化和云安全应用、解决方案架构和先进技术，是英特尔首席工程师。他不断推进安全解决方案的寻找和开发过程，致力于交付能在多租户云环境中提供深度可视化、编排和控制能力的基于硬件的安全解决方案。在此之前，他曾在系统开发部署方向的多个工程架构岗位工作过，在英特尔信息和制造技术部主要从事面向服务架构和大数据分析工作，拥有 15 年以上工作经验。Raghu 在虚拟化和云计算的安全、证明和控制领域拥有多项专利，并且还是《 Creating the Infrastructure for Cloud Computing: An Essential Handbook for IT Professionals 》一书的合著者。他拥有计算机科学硕士学位和电子工程学士学位，另外他加入英特尔之前还曾参与过多个人工智能 / 知识工程方面企业的创业。

Enrique Castro-Leon 是英特尔架构部的企业架构师和技术战略师，致力于企业 IT 解决方案整合、云计算、服务工程方面的工作。作为一名技术战略师，Enrique 一直从事市场新兴技术的颠覆效应研究。他是《 The Business Value of Virtual Service Grids: Strategic Insights for Enterprise Decision Makers 》一书的第一作者，这本书主要关注虚拟化、面向服务方法学和分布式计算。他还是《 Creating the Infrastructure for Cloud Computing: An Essential Handbook for IT Professionals 》一书

的第一作者。Enrique 具有普渡大学电子工程博士学位、电子工程和计算机科学硕士学位，哥斯达黎加大学电子工程学士学位。他还是邻域学习中心（Neighborhood Learning Center，NLC）的合作创始人兼董事长。邻域学习中心是一个免税组织，旨在面向美国俄勒冈州基础教育提供计算机教育和辅导服务。自 2000 年开办以来，邻域学习中心帮助了 300 多名有落后风险的在校生，以及超过 60 个家庭的孩子。邻域学习中心近期获得了来自 Meyer 纪念信托、Templeton 基金会和 Rose E. Tucker 慈善信托的表彰奖。

About the Reviewers 审校者简介

Martin Guttmann 是英特尔首席工程师，拥有 30 年以上的丰富从业经验。他的研究方向涉及计算机系统、软件、操作系统、数据中心运维、安全解决方案和企业架构等。作为英特尔首席技术官团队成员，他负责为企业信息技术和数据中心架构、系统、产品和解决方案定义端到端管理和安全架构。



Uttam Shetty 是英特尔云安全方案部门负责人，领导其工程团队交付云基础设施安全解决方案，并提供与平台相关的可信保障。他拥有超过 25 年领导全球开发中心的丰富从业经验，为电子商务、制造系统和基础设施建设提供关键变革所需的技术和解决方案。

Mitch Koyama 是英特尔企业产品、解决方案和技术的专题专家。Mitch 致力于在云计算中应用英特尔安全技术，与各技术供应商和开发商一同工作，解决云计算应用障碍。Mitch 在许多地方工作过，在此领域拥有超过 10 年从业经验。

Ren Wu 是英特尔数据中心部安全技术方向的技术整合工程师。Ren 在系统和解决方案架构方面拥有丰富工作经验。任职于英特尔、AT&T 贝尔实验室、朗讯科技，并在光纤网络架构、标准和长距离密集型光波复用系统方面做出许多有益贡献。

李彦，清华工学学士、复旦 MBA 硕士。1991 年加入英特尔美国，2000 年回国，现任英特尔中国研发中心平台安全部门系统软件架构师、云计算可信安全方案首席架构师、2009 年被特邀为中国电子学会云计算和大数据专家委员。

他与武汉大学张焕国老师及其团队一起联合可信产业链（华为、国民技术、中标软、浪潮等），组建了中国可信云社区，推动 TPM 2.0 国际标准，推广英特尔 TXT 和其他安全技术，支持中国本土化和开源可信解决方案，打造了中国完整的端到端可信云安全产学研产业链。

魏刚，英特尔数据中心部门安全技术方向的软件技术专家，长期在虚拟化和安全相关领域从事系统级开发工作，《OpenStack 设计与实现》作者之一。他在英特尔拥有超过十年的相关工作经验，是 tboot、OAT、tpm2.0-tools 等多个英特尔安全相关开源项目的创始人之一，也是 TPM2.0-TSS、OpenCIT、Xen、Linux Kernel 等开源项目的代码贡献者。

黄艳，现任职于 Intel 中国区安全事业部，负责战略规划。曾任职于 Dell、Cisco、McAfee 和 Forcepoint，拥有多年的 IT 经验和安全行业经验。

Preface 前　言

对于云中的应用和数据而言，安全是个永远存在的问题。这对试图制定迁移应用准则的企业主管、试图定位成革新技术采用者的营销组织、试图建立安全基础设施的应用架构师，以及试图保证坏人不能为所欲为的运营人员来说，都是必须考虑的问题。应用是否准备迁移到云或是否已经基于云组件运行并不重要，甚至应用成功运行多年并没有发生重大安全事件也不重要：因为完美无缺的记录并不代表其所有者能声称自己在安全上无懈可击。企业主管已敏锐地意识到，完美无缺的记录所代表的荣誉其实只是对攻击的邀请。自然，过去的表现也绝不代表未来。

无论问谁，安全都是抑制云计算广泛应用的最大障碍。要弃用本地部署系统转而采用云计算，企业组织需要设定一个更高的标准，也就是应用安全标准的最佳实践。迁移或采用云服务可以提供一个优势，让公司可以从头开始设计内嵌安全的、新的、基于云的基础架构，从而避免当前大部分数据中心在安全建设上出现的零碎化、事后扩充化的问题。但不同的建立内在安全性的方法也有细微差别，在第 1 章中我们将会看到。云服务提供商努力构建的安全基础架构，启用多租户环境，为用户提供工具、可视化和控制的基石。他们开始把安全看成云服务触力的一个重要关注点，与性能、功耗、正常运行时间等需综合考量。这为方案架构师在安全设计上根据所在场景实现不同灵活性和安全粒度提供了可能，例如，金融服务业和企业资源管理应用的安全需求在产品宣传册上就截然不同，然而它们都可能使用相同存储服务商的存储服务，这些服务将要求高级别的完整性、机密性和安全防护。

一些具体实践方式可能会带来一些战术优势，例如使用内部私有云而不是使用第三方托管的公有云资源，但其实并没有从根本上解决安全问题，比如，还是采用如“瑞