HZ BOOKS
华章科技

Apress®

· 网络空间安全技术丛书 ·

INTEL TRUSTED EXECUTION TECHNOLOGY OR SERVER PLATFORMS

A Guide to More Secure Datacenters

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

[美] 威廉·普拉尔 詹姆斯·格林 著 张建标 等译
(William Futral) (James Greene)

- 从解释为什么 Intel TXT 技术如此重要开始，介绍它的硬件功能，然后循序渐进地阐述 OEM、数据中心、OSV 和 ISV 的作用。
- 简单来说，本书从架构到部署揭开 Intel TXT 技术的神秘面纱。

机械工业出版社
China Machine Press

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

INTEL TRUSTED EXECUTION TECHNOLOGY OR SERVER PLATFORMS

A Guide to More Secure Datacenters

[美] 威廉·普拉尔 詹姆斯·格林 著 张建标 等译
(William Futral) (James Greene)

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

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 /（美）威廉·普拉尔（William Futral），（美）詹姆斯·格林（James Greene）著；张建标等译 . —北京：机械工业出版社，2017.9
（网络空间安全技术丛书）
书名原文：Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters

ISBN 978-7-111-57937-3

Ⅰ. 面… Ⅱ. ①威… ②詹… ③张… Ⅲ. 数据库系统 Ⅳ. TP311.13

中国版本图书馆 CTP 数据核字（2017）第 219327 号

本书版权登记号：图字 01-2017-2054

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

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：张梦玲 责任校对：李秋荣
印 刷：北京诚信伟业印刷有限公司 版 次：2017 年 9 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：12
书 号：ISBN 978-7-111-57937-3 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，并逐步广泛运用。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 8 ~ 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 或 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，武汉大学和英特尔发起、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。（详细请参考附录。）

这三本书也是该社区技术工作的重要参考书。2012~2014 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。2014~2015 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、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

The Translator's Words 译者序

随着计算机和网络技术的飞速发展，数据中心和云计算环境成为应用集中的主要平台，其安全性显得越来越重要。服务器是构成数据中心和云计算环境的主要设备，如何保证服务器安全至关重要。Intel 公司的可信执行技术（Intel TXT）是保证服务器安全的关键技术。

本书的两位作者有着多年的信息安全从业经验，并在 Intel 公司担任重要的信息安全技术研发和推广职位，书中融合了他们的实践经验。与单纯的理论教科书不同，本书提供了从理论到实践的有机衔接融合。本书介绍了计算机中的信任概念和 Intel TXT 的基本原理，以及如何配置 Intel TXT，建立启动控制策略及验证的功能等。最后介绍了 Intel TXT 在数据中心和云环境中的应用及可信计算的未来发展方向。通过本书的学习，读者不但可以了解 Intel TXT 的一些基本概念、基本原理，更重要的是，还能学会在数据中心和云计算环境中运用 Intel TXT 技术。

本书适合作为信息安全相关专业的研究生教材，也可以作为相关领域专业人员的参考书。

本书由张建标教授组织翻译，参加翻译的人员还有赵子枭、朱元曦、张亚昊和王晓，最后由张建标负责统稿和审校。

由于译者的水平有限，书中翻译不妥或错误之处在所难免，恳请广大读者批评指正。

译者

2017 年 5 月

推荐序 *Forword*

我完全可以想象出这样的场景：Intel 上层，或者说智库成员，正在某处进行英特尔可信执行技术（Intel TXT）的激烈讨论。从设计、集成团队到销售和营销主管，所有相关人员都在场，他们对 Intel TXT 的每个方面都有不同的观点和视角，有点像联合国会议。然而，当出现一个关于实现的问题时，现场突然鸦雀无声，所有人都转而看向威廉·普拉尔。

威廉无疑是硬件安全方面的权威专家。虽然我的团队得以与詹姆斯·格林、威廉·普拉尔以及 Intel 其他在可信硬件方面的专家紧密共事，我们的合作之旅仍然挑战极大、常有争议，甚至偶尔让人望而生畏。大约十年前，我参与了一个开发工具集的小组。这个小组有个雄心勃勃的假设：有种方式能收集、存储和查询来自每个地方、每个系统的每个事件。这应该能让我们更准确地检测、关联并在某些情况下比以前更精准地预测安全事件。当时我没有意识到，安全信息和事件管理（SIEM）很快会成为各地信息安全计划中的关键组成部分，并正在形成十亿美元级的行业。

一家大型服务供应商注意到我们的工作并联系了我们。他们认识到，如果他们可以使用传统的 IP 监控工具为其网络运营中心（NOC）提供世界一流的网络服务，那么更可以使用我们的安全事件监控软件构建安全操作中心（SOC）来帮助满足客户日益增长的安全需求。这对我来说很有意义，所以我继续完成这项工作，并一头扎进服务供应商的产品阵列中。他们没有告诉我的是，他们还有一个雄心勃勃，足以颠覆传统数据中心安全的想法，称之为云计算。

这种新产品由共享的物理基础设施组成，供应商将通过网站门户直接向订阅者提供。这样可以让订阅者通过在供应商的共享硬件上使用即付即用模型来访问、配

置和管理自己的虚拟基础设施。这种安全实现十分特殊，对我而言是完全陌生的。作为安全从业者，通常认为如多租户、共享基础设施、虚拟域和服务交付等因素是别人应考虑的事情。一开始，我无法接受任何头脑清楚的用户会将对基础设施的完全控制权交给服务供应商，并且服务供应商还会告诉他们将与其他用户共享硬件，甚至服务供应商也不知道其他用户是谁。从安全的角度来看，这真是疯狂的想法！

我们部署了所有常规的安全控制手段（有些手段并不那么常规），实施了可以想到的每个策略和程序，从我们的 SOC 中进行管理，从而促成了世界上最大的 SIEM 实现系统。我们已经完成了很多非常好的工作，将安全编排到了云的各个部分。然后有一天，我的上司，公司首席执行官罗伯特·罗萨瓦（Robert Rounsavall）正在带领美联邦客户参观我们的设施，解释我们的所有安全服务。那时他们刚好听说了一些供应链事件和 BIOS 级攻击的报告，所以他们问我们正在做什么保护硬件平台。我也听说过一些外国硬件神秘地出现在出口的安全设备主板上的报告。这些设备据说被“海关扣压了几个星期”。当时，我们没有做太多的事情处理这个威胁，只是制定了手动过程来更新我们提供的每个平台上的固件，并重新审视了采购方法，确保以最低的风险购买尽量安全的设备。而世界开始发现云供应商最黑暗的小秘密之一：完全没有办法在硬件级别度量、验证或者自动化任何东西。

很难提高对风险的战略认识，因为人们对如何有效地说明风险知之甚少。管理高层正在努力界定和量化威胁，业界也是日益关注。美国国家标准技术研究所（NIST）、可信计算组（TCG）和开放式数据中心联盟（ODCA）等开始发布关于配置硬件、可信计算和数据边界的最佳实践及使用模型。此时，我正在为一家大型云服务供应商运行 SOC，可以考虑其基础设施完整性的可见性几乎为零可能造成的后果。更令人不安的是，我们正在对虚拟机（VM）进行实时事件响应，但却不知道这些虚拟机在哪，它们过去的位置在哪，甚至其他的哪些客户机正在使用这些受损系统共享的物理服务器！如果我不知道，客户更不知道了。这成了一个让我夜不能寐的噩梦。这个噩梦不亚于如下 NSA 认定的最糟糕的情景之一：如果一个核武器被偷运进美国怎么办？如果供水系统被致命细菌秘密感染了怎么办？如果我们所有的云服务器都遭到 BIOS 级篡改怎么办？

Intel TXT 终于浮出水面。我第一次接触 Intel TXT 是在 2010 年，与几位 Intel 战略家和一些 VMware 专家共同参会后。我心想，终于出现了一些度量服务器中的

固件和嵌入式代码的实际工作。经过不断回避基础设施安全和硬件完整性问题、忽略我认为是安全监控方面的巨大盲点的三年之后，终于到了实现这一新的基于硬件的安全技术的时候了。这意味着我们找到了一种方法，不仅使用新发现的硬件可信数据，还可以将其集成到传统的安全工具，如 SIEM 中，以实现可见性、策略执行、拦截和关联入侵分析。

除了度量底层硬件的完整性外，我们发现这项技术还可以用于解决其他一些领域的问题。例如，如果可以设计一种自动化的方法来捕获和监视这些度量值，就可以使用它们唯一地识别每个物理服务器，从而可以轻松地对上虚拟机监视器和 VM。想象一下，能够实时识别云中每个 VM 的位置并跟踪其随时间的变化的情景。现在正是宣传这项变革的时候了！

这需要在现实世界中进一步探索，所以我决定暂停之前的事件处理工作，直接与客户一起工作，以便安全和负责任地将资产移动到云中。在我进一步探索如“自带设备（BYOD）”和不同云风格相关的基于硬件的攻击面时，我发现如果漏洞利用能影响硬件行为，攻击向量似乎没有尽头，一切都可能发生。最近，在 Intel 和一些开创性云供应商的帮助下，我们有了一些令人振奋的成功案例，但仍然还有一些未知领域需要探索。

本书的重要性和 Intel TXT 的进一步发展不容忽视。我们目前正在见证一种模式转变，云中硬件之上的抽象软件核心功能不再强大到能让人忘记硬件的存在。任何软件都必须运行在某处的某个硬件平台上，这是个不能被忽视的事实。Intel TXT 正是一项帮助在云上花费了大量时间的业界找到坚实硬件基础的技术。

阿尔伯特·卡瓦列罗

Trapezoid 公司 CTO

Preface 前言

虽然已有许多关于 Intel TXT 的论文以及其他形式的文档，但大多数都注重于帮助平台设计者和操作系统供应商（OSV）在硬件或软件平台上实现这种技术。然而，也有少量更注重结果和技术使用的工程、销售和配置资料，这对 IT 专业人员更有帮助。通常情况下，这些资料更加客观。也就是说，它们告诉设计者或实施者能做什么，但是并不一定告诉他们应该做什么，或者是为什么选择这项技术而不是那项技术。在实际使用新技术的实践中，这种差距会造成问题。

经验显示，当平台抵达数据中心时，实际上几乎没有提供多少信息指导系统管理员充分利用新功能，比如 Intel TXT。Intel 很擅长与平台架构师、操作系统架构师以及软件开发者等核心受众协商实施细节，此外，Intel TXT 的实施经验能够让新的受众群体受益或者提供新的机遇。我们不断从想要知道这项技术如何和应该如何部署的 IT 经理们和云方案架构师们那里收集到问题，让其能够评估在他们各自的环境中有何能够付诸实践的选择。硬件和软件设计者也很好奇数据中心如何部署这项技术，会面临什么问题，以及哪些特性是重要的。

因此，很明显需要一本书来提供更完整的蓝图，从解释为什么这项技术如此重要开始，介绍硬件功能是什么，然后循序渐进地阐述 OEM、数据中心、OSV 和 ISV 的作用。简单来说，我们的目标是：打造一本揭开新技术神秘面纱的书——从架构到部署。本书的出版也使得我们有机会提高对新兴威胁的可见性，并且能够在我们的核心用户很可能已经购买了相关产品（如支持 Intel TXT 技术的服务器以及操作系统或虚拟机监视器）的基础之上给出解决方案。令人高兴的是，我们也注意到，集成或启用基于这项技术的解决方案只需以“小小的”额外花销（比如 30 ~ 50 美金），为 OEM 服务

器添加一个 TPM 模块。简言之，这些解决方案确实近在咫尺，问题仅仅在于宣传和帮忙展示相关方法和收益！

本书为数据中心提供了一份使用 Intel TXT 的综合指南，同时也为平台及软件供应商提供了额外的相关见解。因此，本书的前半部分解释了这项技术能做什么及其工作原理，解释了证明如何工作，讨论了不同特性的作用，以及引领读者逐步了解启用该技术、创建载入策略以及为数据中心选择最佳策略的整个流程。并且还解释了哪些选择是可选的及其背后应该注意的关键点。简言之，前半部分内容主要介绍了如何实施，即 Intel TXT 是什么以及如何工作。

本书的后半部分内容提供了为什么要实施 Intel TXT 技术的整体概览。它注重于模块的使用，即使用它能够在运营、安全性以及业务方面获得哪些好处？它还注重于在云或企业中应用 Intel TXT 的生态环境需求，即现在到将来需要的关键硬件、软件以及服务。这些讨论意在帮助 IT 管理者或企业安全架构师根据其业务需求进行技术功能和使用模型依赖性的评估。本书最后展望了该技术的未来。

没有一个 IT 管理员或架构师愿意花费精力和资源来建设或实施一个一次性的解决方案。因此，我们不仅应解释当前的功能（和局限性），还应提供现有基础下的技术走向和如何将之对应到快速演变的业务需求的专业见解。本书的目的是帮助 IT 和安全领导者发现新的机遇，解决当前所面临的安全挑战，并定位于加强安全以便更好地为企业的未来保驾护航。

Intel TXT 如今已被全球范围内不同行业的多家公司所使用。它们需要进行 IT 基础设施的“更新换代”来获取 Intel TXT 提供的防护能力吗？绝对不是。这不是 IT 的工作方式。它们会部署装有 Intel TXT 的新服务器并建立面向关键点的可见性、可控性及一致性使用模型，尤其是云基础设施。事实上，它们正在现有设施上建立新的、更加安全的、更合适于承载更敏感或规范要求的工作负载池。这种优化部署模型也是常说的面向资源及利用托管它们的最优平台的 IT 最佳实践。

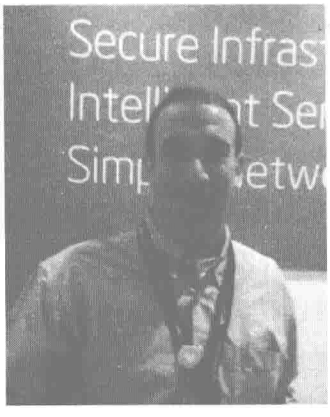
这些早期的应用者正在获取实际收益，并在为其业务规划更加安全的未来。他们从开辟解决方案到市场与技术成熟的过程中收获良多（实际上，他们通过与 Intel 及其他厂商共同实施这些方案并帮助确定了成熟的方向）。本书的目标是分享专家和先驱者的基础工作，降低实施这些技术的门槛，以便基于可信计算的解决方案能够在业界发挥更为广泛的作用。

Acknowledgements 致谢

十分感谢外部和内部技术评审者的贡献、编辑和建议，尤其是我们 Intel 公司的同事 Patrick Hauke, Lynn Comp, Michael Hall, Iddo Kadim, Steve Bekefi, Tracie Zenti, Sham Data, Raghu Yeluri, Alex Eydelberg, Will Arthur, Mahesh Natu, and Jeff Pishny，以及外部评论者 Albert Caballero, Michael Dyer, Hemma Prafullchandra, Merritte Stidston, John McAuley, Alex Rodriguez, Pete Nicoletti, Murugiah Souppaya, Gargi Mitra Keeling, and Robert Rounsavall.。他们的时间、指导以及专业知识对本书来说有无尽的价值。我们也意识到了许多来自 Intel TXT 开发、解决方案、销售及市场组和生态伙伴、初始客户的直接或间接的贡献，正是他们的努力为本书添加了浓墨重彩的一笔。

关于作者 *About the Authors*

威廉·普拉尔（William Futral）是Intel公司数字企业部的高级架构师。在Intel公司20年的工作生涯里，他在新兴科技领域中举足轻重，如Intel TXT、虚拟化、Intelligent I/O（I^2O）、InfiniBand和其他主要创新性项目。他是《*InfiniBand Architecture: Development and Deployment—A Strategic Guide to Server I/O Solutions*》一书（Intel 2001年出版）的作者，也是其他许多科技出版物和设计指南的作者。他还是许多国际标准协会的成员，如ARINC、IEEE，以及美国国家标准学会（ANSI）。



詹姆斯·格林（James Greene）是Intel的安全技术产品营销工程师。他负责数据中心和云安全解决方案的产品定义和应用模型，例如Intel TXT。2005年Intel收购Conformative Systems公司时，他来到了Intel。在Conformative Systems就职时，詹姆斯带领团队负责所有关于XML处理应用文件的产品营销活动。在那之前，詹姆斯在Compaq和Hewlett-Packard负责企业服务器、工作站、业务存储单元领域，担任营销、战略、市场开发以及商业和技术计划方面的领导职务。

About the Reviewer 技术评审人

孙宁，计算机专业博士，2003 年加入英特尔，工作至今。曾任英特尔中国研究院高级研究员和英特尔博锐技术平台架构师，负责中国区的主动管理技术和产品的研发和推广工作。目前任英特尔 SGX 和 TXT 技术及产品开发安全架构师。现在美国加州 Santa Clara 英特尔公司工作。

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构架师、云计算可信安全方案首席构架师、2009 年被特邀为中国电子学会云计算和大数据专家委员。

特别是 2012 年近期，和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。