简译版

要实现安全的云计算，需掌控加密密钥

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	For Secure Cloud Computing, Get Control of Your Crypto Keys		
原文作者	Brian Jenkins	原文发布日期	2019 年 2 月 22 日
作者简介	Brian Jenkins 是 StrongKey 公司的产品副总裁。https://www.networkcomputing.com/author/brian-jenkins		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/cloud-infrastructure/secure-cloud-computing-get-control-your-crypto-keys		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

要实现安全的云计算，需掌控加密密钥

Brian Jenkins

2019 年 2 月 22 日

对于投资于云计算或迁移到云计算的企业而言，必须始终将云安全状态放在首位。

由于其规模经济（economies of scale）和易用性，云计算已被企业迅速接受。对于中等企业来说，相比于搭建自己的基础设施，将所需的基础设施外包出去（特别是在多租户环境中），要容易得多。

然而，安全性已经成为云端的重要问题。使用云就像把房门钥匙留在门垫下面一样——企业不仅外包了基础设施，还外包了保护敏感数据和文件的加密密钥。

谁能够访问你的加密密钥？这一问题的答案决定了云中的数据是否安全。除非企业拥有对加密密钥的独有控制权，否则就会面临风险。不幸的是，云端的情况并非如此，这也是企业不断收到数据泄露通知邮件的原因之一。每个云服务和“软件即服务”（software-as-a-service）提供商都代表着巨大的攻击面，是重要的攻击目标。随着企业将所有内容迁移到云端，他们应该如何进行密钥管理呢？这是一个亟待解决的问题。

密钥在哪？

云解决方案中最简单的概念是“多租户”——即云中托管的应用程序、数据库、文件等内容。之所以说“多租户”是最简单的概念，是因为本地基础设施的可视化（作为云实例）很容易理解。许多企业认为他们需要多租户解决方案。但是，使用三种常见的云解决方案中的任何一种将密钥管理系统（KMS）迁移到云端，都会带来很大的风险。

云 KMS（企业拥有密钥，但它们存储在云软件中）

基于软件的多租户云 KMS 特别不适合加密密钥的管理。由于硬件资源在多个客户端之间共享，因此对这些密钥的保护更加不完善——“幽灵”（Spectre）和“熔毁”（Meltdown）漏洞就是很好的证明。

外包 KMS（云服务提供商拥有密钥）

云提供商会对你说，你的所有数据和文件都是受保护和加密的。这样很好——前提是

云提供商或你的帐户凭证没有遭到黑客攻击(典型的例子是 Uber 攻击——攻击者通过 AWS 云服务对 Uber 的服务器实施了攻击)。你的文件可能已经加密了，但如果你将加密密钥存储在这些文件中，那么一旦攻击者获取了密钥，他们就可以解密所有内容了。

云 HSM（企业拥有密钥，但它们存储在云硬件中）

这是保护加密密钥的理想方案，即使用安全的加密处理器（cryptoprocessor）——硬件安全模块（HSM）和可信平台模块（TPM）。虽然使用基于云的 HSM 或 TPM 可以缓解某些风险，但事实是，在云端，即使应用程序使用安全的加密处理器，它仍然是多租户基础设施的一部分。从攻击者的角度来看，在专用硬件加密处理器和多租户环境中运行的应用程序之间，后者是更容易攻击的目标。

了解相关法则

部署具有下一代防火墙、入侵检测和其他保护措施的边界安全方案是有必要的，而云提供商可以提供这些方案。但要保护核心元素（敏感数据和文件），企业需要根据基本的“加密密钥管理法则”对其进行加密：

（1）加密密钥仅由企业的多个密钥管理者控制。

（2）使用安全的加密处理器（HSM/TPM）保护加密密钥。

使用加密处理器处理敏感数据的应用程序，不得在公有多租户环境中运行。这是因为，在多租户环境中，敏感数据不受保护，验证应用程序身份的密钥也不受保护。攻击者可以利用加密处理器破解加密数据。

虽然有这些法则是好事，但遗憾的是，目前还没有能够满足这些法则的公有云。完全依赖云提供商来保护密钥的企业，可能会遭到当头一棒。

迈向更安全的云

制定密钥保护方案并不难，不需要什么工程博士学位。我们的建议是：将敏感数据和文件存储在云端；同时在公有云之外的受控环境中，在安全的加密处理器的保护下，保持对加密密钥的独有控制权。

如果企业使用该框架，即使攻击者攻破了云服务提供商，他们也无法获取任何内容，因

为他们只能获得加密的信息，没有密钥，他们就无法解密这些信息。在保护数据的同时，该方法还可以实现云的优势。这样一来，公司既能够利用云（私有云或公有云）的优势，又能够符合数据安全法规。

对于投资于云计算或迁移到云计算的企业而言，必须始终将云安全状态放在首位。即使云应用程序使用的数据是加密的，加密密钥也是真实存在的。企业不仅要保护这些信息，还要保护其加密密钥。

考虑到云环境的现实问题，中型企业可以采用企业级工具和实践，来实现更强大的安全性。

企业不应该认为云提供商会保护他们的数据。相反，他们应该假设云提供商无法保护他们的数据，并找到符合“加密密钥管理法则”的解决方案，以便实现更安全的云计算。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*