In the Boxing Ring
2025年9月

Network Box技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2025年9月的 In the **Boxing Ring**

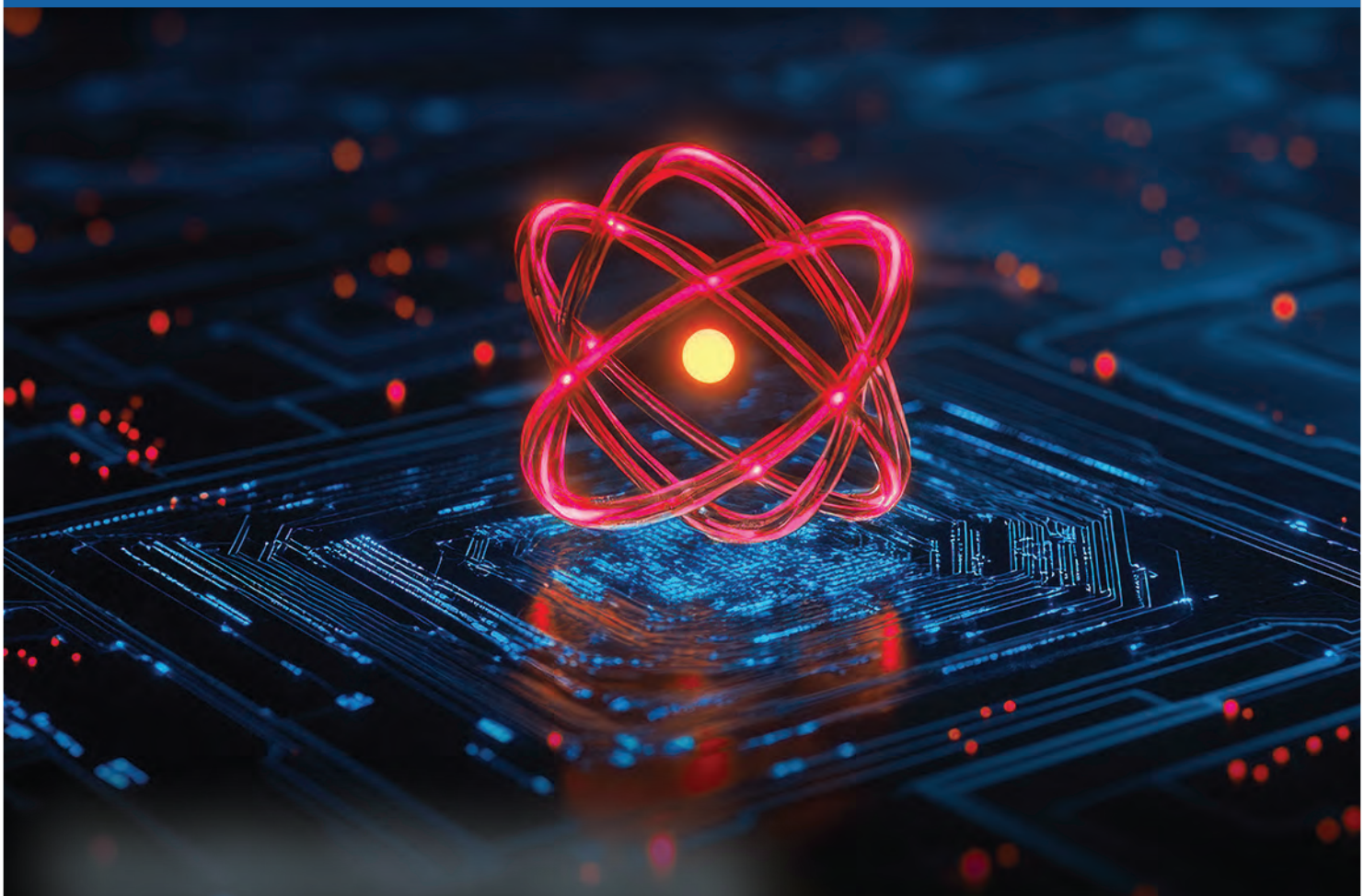
本月，我们推出了一份简短的指南，介绍量子密码学的基本概念。随着量子计算日益接近实际应用，目前用于保护网络、数据和通信的加密方法可能将不再足够。尽管这一技术仍在发展中，但其破坏广泛采用的安全协议的潜力意味着组织不能等到问题出现才采取行动。在第2到3页，我们讨论了量子密码学的核心原理，概述了它带来的风险和机遇，探讨了新兴的后量子解决方案，并提供了实用步骤，帮助系统应对量子技术带来的挑战。

在第4页，我们重点介绍了本月“补丁星期二”发布的Network Box 8和我们的云服务的增强功能和修复内容。

此外，Network Box自豪地推出了下一代M-298i，专为寻求高级UTM+保护的中型办公室设计。Network Box香港还邀请了香港明爱，举办了一场网络安全研讨会，内容涵盖了即将实施的关键基础设施和隐私法律、Network Box服务的各个方面，以应对最新的现实世界网络威胁，以及黑暗网络的危险。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
September 2025

本月摘要：



理解量子密码学

IT管理员指南

在当今迅速发展的数字化环境中，量子密码学正成为保护敏感信息的关键话题。作为IT管理员，您已经熟悉管理网络、防火墙和加密协议。然而，量子计算带来了新的挑战和机遇，可能会重新塑造我们保护数据的方式。在本文中，我们将探讨这一技术的基本原理、它可能对您产生的影响，以及您需要了解的知识，以保持领先。

量子计算机与传统计算机

传统计算机，例如您每天管理的服务器和笔记本电脑，使用比特（bits）进行操作——这些是二进制单位，要么是0，要么是1。它们顺序处理信息，通过将问题分解为一个个步骤来解决问题，每个步骤依次执行。这种经典方法已经为几十年来的邮件服务器和云存储提供支持。

另一方面，量子计算机利用量子力学原理，这是物理学中的一个分支，研究原子尺度的粒子。它们使用的是量子比特（qubits），而不是传统的比特，量子比特可以同时存在于多种状态。这使得量子计算机能够并行执行复杂计算，解决那些传统计算机需要几年甚至数百年才能完成的问题，只需几秒钟或几分钟。可以把量子计算机看作是针对特定任务的专用工具，而不是替代日常硬件的设备。

量子技术仍处于早期阶段，目前的系统受限于量子比特数量较少且错误率较高。像IBM和Google这样的主要玩家正在推进原型设计，但广泛的实际应用可能还需要数年的时间。

为什么量子计算机构成威胁？

传统的密码学通过使用依赖于假定难以解决的数学问题的算法对数据进行加密来保护数据。公钥系统，如RSA和ECC（支撑HTTPS和VPN等协议的技术），使用一对密钥，其中一个是公钥（用于加密），另一个是私钥（用于解密）。这些相同的算法也用于数字签名，它们的安全性源于大质数分解或求解离散对数的难度——这些任务传统计算机在处理极大数时效率低下。

量子计算机威胁到这一基础。像Shor（1994年开发）这样的算法，可以在足够强大的量子机器上将这些大数分解速度指数级地加快。这意味着，具备量子能力的攻击者可以从公钥推导出私钥，从而使今天的加密方法失效。像AES这样的对称密码虽然更具弹性，但仍然可能受到Grover算法的威胁，这种算法加速了暴力破解攻击。对于IT管理员来说，这不仅仅是理论问题。这可能会使加密的通信、存储的数据和数字签名暴露在攻击面前。

现在收集，稍后解密

一个特别狡猾的风险是“现在收集，稍后解密”策略。对手，如国家或网络犯罪分子，可以使用传统方法拦截并存储今天加密的数据。这些数据，如通过TLS传输的财务记录或知识产权，目前仍然安全，因为用传统计算机破解它是不现实的。

然而，一旦可扩展的量子计算机问世，可能是在未来十到二十年内，这些相同的对手可能会追溯性地解密已收集的数据。想象一下，2025年通过互联网加密传输的电子邮件或数据库备份，在2035年被解锁，揭示了早已发送的秘密。这个“现在收集，稍后解密”攻击增加了紧迫感，因为具有长期敏感性的数据显示，即使量子威胁不是立即存在，依然脆弱。作为IT管理员，审查您的数据保留策略并考虑加密资产的生命周期是一个聪明的、前瞻性的步骤。

什么是后量子密码学？

后量子密码学（PQC）是指设计用来承受量子攻击的新算法，这些算法可以在经典硬件上运行。这些算法包括基于格的、基于哈希的和基于代码的方案，它们的安全性基于量子计算机难以解决的问题。与量子密钥分发（需要专门的硬件）不同，PQC可以无缝集成到现有系统中，如服务器和浏览器。

PQC在2025年成为焦点，主要因为一些里程碑事件，包括NIST在8月最终确定的标准，其中包括ML-KEM、ML-DSA和SLH-DSA等算法。包括微软和谷歌在内的政府和科技巨头正在通过旨在应对潜在风险的项目推动量子计算的采用。

这直接与TLS 1.3（最新的安全通信协议）相关，世界各国正在逐渐转向使用它来处理Web流量。TLS 1.3强调前向保密性和效率，但为了实现后量子安全，它引入了混合密钥交换——结合了像X25519这样的经典方法和像ML-KEM这样的PQC方法。即使其中一个算法失败，这也能确保安全性。IETF已经为TLS 1.3标准化了这些混合方法，OpenSSL和浏览器中已经开始实现这些方法。较旧的TLS版本缺乏这种灵活性，因此迁移到TLS 1.3对于准备PQC至关重要。对于您的网络，启用TLS中的PQC意味着需要更新证书和配置，以支持这些混合方法，在安全性和性能之间找到平衡。

好消息是，您不必单独应对这个问题。最新的Network Box NBRS-8固件已支持后量子密码学，允许您配置混合TLS设置和量子抗性算法。此功能使得关心的用户能够为关键连接激活PQC，而不会中断操作。然而，我们必须保持适度的热情，平衡前进的愿望与保持与遗留系统兼容性的需求。这对于像SMTPS邮件和HTTPS网页等关键技术尤其重要。

Network Box 8 新特性
2025年9月

2025年9月2日星期二，Network Box将发布本月的补丁星期二增强功能和修复内容。各地区的SOC将以分阶段的方式在接下来的14天内进行新功能的发布。

本月，针对Network Box 8，以下内容包括：

NBRS-8

- 提高事件日志时间戳的粒度到微秒级别
- 配置系统启动速度的微调
- 增强高可用系统对配置更改的响应
- 改进软件包更新程序
- 修复wireguard和openvpn的网络VPN启动顺序
- 增强4in4隧道配置
- 改进GMS连接跟踪传感器

NETWORK BOX 8

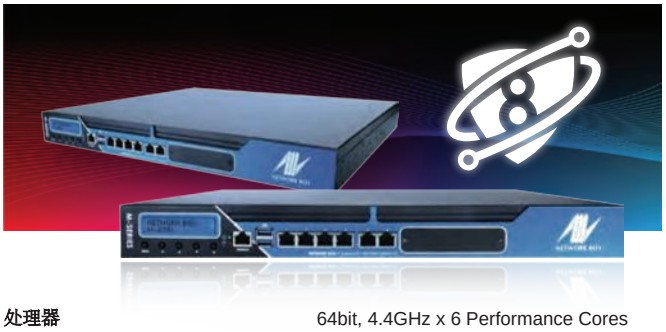
在大多数情况下，以上更改不会影响正在运行的服务或要求设备重启。然而，在某些情况下（取决于配置），可能需要设备重启。如果需要，您的本地SOC将与您联系安排此事。

如果您需要关于上述任何内容的更多信息，请联系您的本地SOC。他们将安排部署和联络。

Network Box HIGHLIGHTS

M-298i | 硬件平台

Network Box自豪地推出了M-298i，专为寻求高级UTM+保护的中型办公室设计。M-298i配备了增强的硬件性能，并由强大的NBRS-8平台驱动，带来了能力上的显著跃升。它是M-295i的继任者，M-295i的官方支持计划将在2028年7月结束。



处理器	64bit, 4.4GHz x 6 Performance Cores 64bit, 3.3GHz x 4 Efficiency Cores
内存	2 x 16GB, 3200MHz DDR4
存储	4TB HDD
网络	6 x 2.5Gb RJ45
I/O 接口	1 x RJ45 management console 2 x USB 3.0
尺寸	430(w) x 44.5(h) x 370(d) mm
重量	6.11kg
可选插件	4 x 1Gb RJ45 LAN Port or 4 x 10Gb SFP+ LAN Port

月刊主办

Mark Webb-Johnson
主编

Michael Gazeley
Kevin Hla
产品支持

Network Box HQ
Network Box USA
贡献者

订阅

Network Box CNNOC
cnnoc@network-box.cn

或者上门到:
深圳市福田区深南大道
竹子林求是大厦西座
920

+86 (755) 3336 1581
www.network-box.cn

Network Box 香港 网络安全研讨会

Network Box香港欢迎香港明爱举办了一场深入的网络安全研讨会。研讨会探讨了即将出台的关键基础设施和隐私法律，并全面介绍了我们的托管安全服务——旨在应对当今最紧迫的网络威胁，包括勒索软件、数据泄露和内部风险。

与会者还深入了解了暗网的常被忽视的危险，包括被盗的凭证、地下市场和更广泛的网络犯罪活动。

此外，客人们还获得了Network Box安全运营中心（SOC）的独家参观机会，亲眼见证了Network Box蓝队的实际行动。

中文翻译：James　校对：Jason