在后量子计算时代，
是否能缩短暴力攻击攻破系统所需的时间？

Microchip Technology Inc.
Kyle Gaede

——量子计算转变了我们在处理暴力攻击数据时的现有知识和准备情况。

为什么网络安全应当是 2023 年的头等大事？

在过去十年里，数据中心一直是黑客攻击的焦点，他们利用各种技术窃取敏感数据。网络安全态势不断演变，以应对最新的威胁，因此保持与时俱进对于缓解安全风险和趋势至关重要。仅在 2023 年，数据中心环境中的多个网络安全领域就有可能产生重要影响。

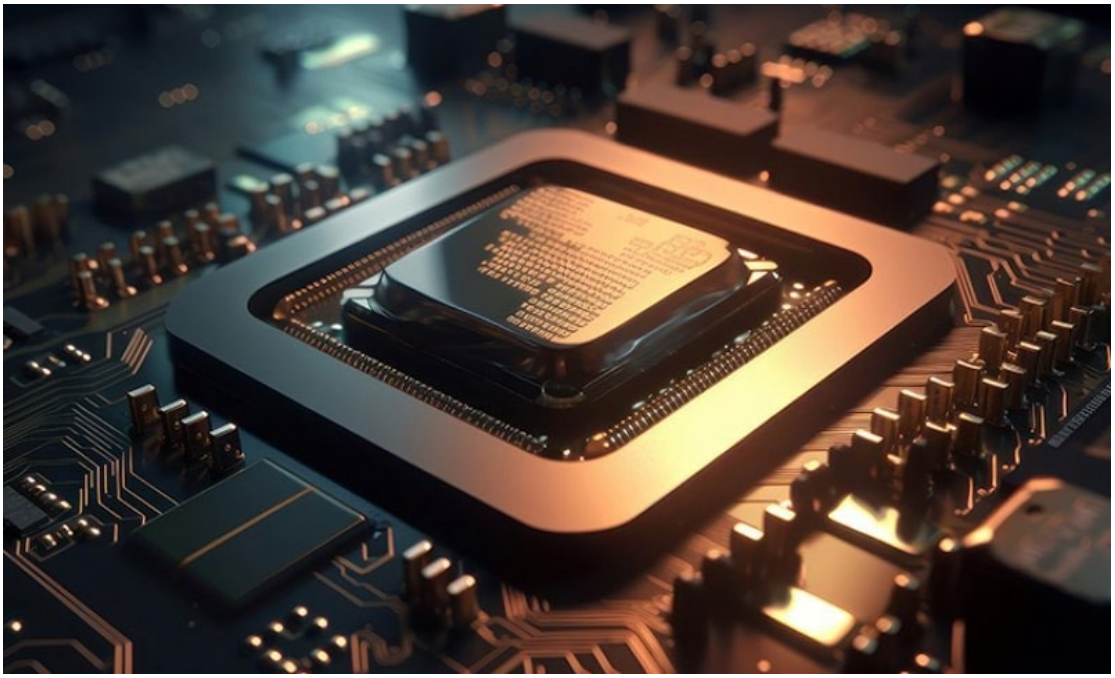
这听起来有些奇怪，但其中一个威胁是网络安全专家的短缺或过度供给，这最终会导致每个人都精疲力竭。虽然这本身不会造成网络安全风险，但却极大增加了数据中心的管理难度。这也可能促使将更多数据转移到云端，在云端，公司需要应对的攻击范围会缩小。这意味着，与在传统数据中心工作的情况不同，此时维护安全环境需要的网络安全专家更少。

根据 IBM 的说法，尽管勒索软件在过去一年有所减少，但它仍然是一个切实的威胁。这便会引发一个问题：勒索软件的减少到底是因为企业加强了防御，还是因为黑客找到了更简单的方法来削弱安全防护？无论如何，数据中心都会在防御投资方面多管齐下，其中包括服务器的强大端点安全、基于网络的勒索软件监控和反网络钓鱼解决方案。最后，勒索软件的减少并不意味着企业可以放松安全工作，而是应该继续保持严峻的态势来应对高威胁。

为此，威胁分析师发现黑客越来越善于规避传统的安全措施。一些网络罪犯将目光投向 MFA（多因素身份验证）和 EDR（端点检测和响应）技术来规避安全措施。物理数据中心的安全威胁也是过去十年里不断增加的一个大问题。例如，一些攻击者可能无法通过数字方式攻入系统，因此他们将目标定为侵入 HVAC 系统、电源和其他关键系统。另外，还存在员工物理窃取硬盘驱动器、U 盘和其他组件以出售给第三方或用于获取其他数据的情况。

接下来是暴力攻击，当其他一切手段都用尽时，黑客会利用这类攻击来攻入系统以获取数据。攻击方法是通过提交大量密码和密码短语，并希望其中之一最终会授予访问权限。攻击者可以采用多种技术进行暴力破解；然而，根据所采用的加密方式，大多数技术需要大量时间才能完成，这可能是几小时、几天、几周甚至几个月。

暴力攻击的工作原理是通过计算每种可能的密码组合。随着密码强度的提高，破解密码所需的时间呈指数级增长。作为对比，虽然如今的算法可以利用 128 到 256 位的高强度密钥，但美国的出口管制却一般限制为 56 位的对称密钥长度。密钥越长，暴力破解密码所需的时间就越久。因此，从理论上讲，如果黑客试图用暴力破解方法攻破一个采用 **AES-128 加密**的密钥，即使利用当今最强大的硬件，也需要约 10 亿年才能破解。

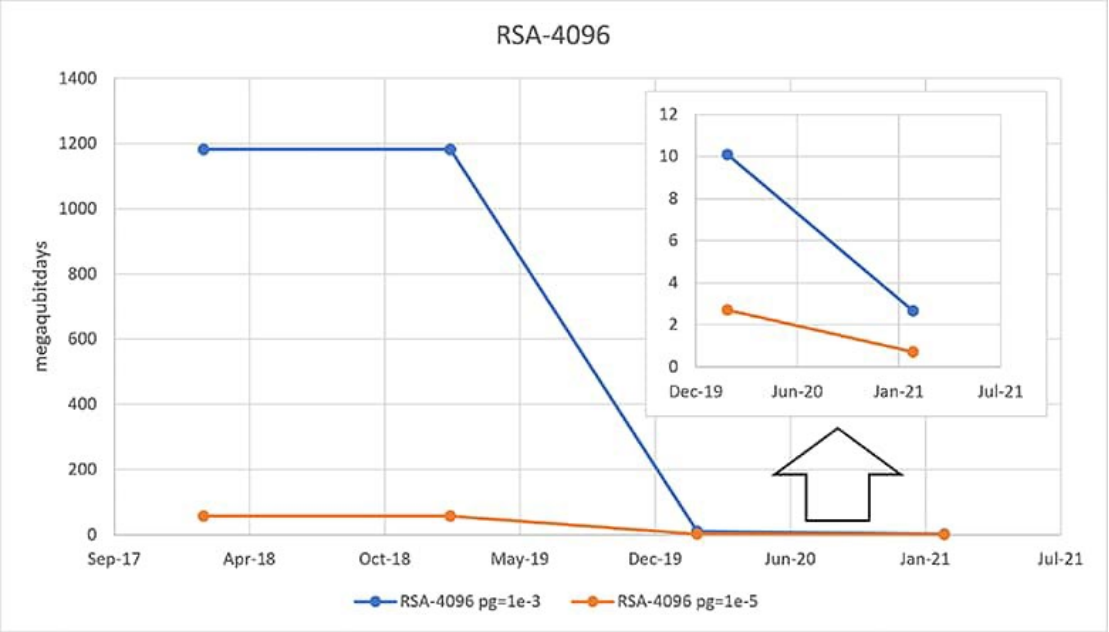


DWave 的芯片是一种采用 128 量子位超导绝热量子优化处理器的量子芯片。

但是，假如我们生活在后量子计算时代呢？对流行的密码技术进行暴力攻击需要多长时间？虽然我们可能还有十到二十年才能拥有能够轻松破解当今诸多密码技术的量子计算机，但现在就必须启动规划过程。为什么？因为量子计算改变了处理暴力攻击或密钥猜测计算的现状。与当今依靠 0 和 1 来处理数据的计算机不同，量子计算机利用量子位（量子比特）来发挥量子力学的作用。尽管量子位在利用双态系统处理数据方面与传统处理器类似，但它们也可以存在于这两种状态的叠加态，并且同时使用两种值来处理信息。新系统正处于开发阶段，其目标是利用量子计算机所涉及的物理原理来实现特殊算法（例如舒尔算法），从而显著缩短找到密钥的时间。

量子计算机可能会破坏和影响网络安全领域的多个行业，包括消除非对称加密。例如，在最近发布的一份报告中，根据全球风险研究所（GRI）的数据，使用理论上的 1 兆量子位

计算机破解 RSA-4096 的时间不到三天，而使用传统计算技术则几乎无法破解。尽管离实现 1 兆量子位计算机还有很长的路要走，但所需的资源和时间正在迅速减少，与此同时，我们看到量子计算的发展速度也在不断加快。



鉴于一些公司目前正在寻求减轻对安全性的影响的方法，政府、企业和网络安全专家了解量子计算的工作原理并开始研发保护数据免受未经授权侵入的保护措施至关重要。像 Prescouter 这样的预测机构已经概括了企业可以利用的一些网络安全解决方案，包括风险管理的开发和利用量子计算本身来降低任何风险。

量子计算机的诞生，虽不至于要等待数十年，但仍需若干年时间，届时只有最具实力的组织和政府才能承担得起并运用这种前沿技术。与此同时，对抗量子计算优势的计算机、服务器和互联网标准需要数年的时间来构筑、实施、测试和部署。之后，这些系统将继续投入使用多年。此外，一旦技术可行，就可以获取、存储并在之后解密有价值的数据。

如今，专业人员必须在成本、性能和安全性三者之间寻找平衡点，因为密钥尺寸越大，意味着处理时间也会更长。我们需要采用基于 NIST 的最新美国国家商用安全算法套件 2（CNSA 2.0）抗量子标准，并且在选择合适的用例和实施时间线时运用智能决策，以此推动组织的发展并保障其安全。对于组织来说，如 Microchip 这样的企业所拥有的专家至关重要，因为他们能帮助评估目前需要采用的协议，并指导如何有效应对未来可能面临的安全威胁。