Towards Quantum-resistant Virtual Private Networks

Joo Cho[1], Stefan-Lukas Gazdag[3], Alexander von Gernler[3], Helmut Grießer[1], Sophia Grundner-Culemann[4], Tobias Guggemos[4], Tobias Heider[4], and Daniel Loebenberger[2]

[1] *ADVA Optical Networking SE*
[2] *Fraunhofer AISEC, Weiden i. d. Opf.*
[3] *genua GmbH*
[4] *Ludwig-Maximilians-Universität München*

31th Crypto Day, 17/18 October 2019

In 1994 mathematician Peter Shor developed an algorithm [8] requiring a quantum computer to find the prime factors of a composite number in much less time than needed today. Shor's algorithm is especially relevant for cryptography as many encryption schemes are based on the assumption that finding prime factors of a sufficiently large number is a computationally hard problem. A quantum computer that could run Shor's algorithm to attack today's cryptographic schemes does not yet exist, but recent advancements in the field of quantum computing suggest that such machines may become reality in the not too distant future [1, 9]. Indeed, first experimental implementations exist, noteably [4, 10].

A patient attacker may intercept today's network traffic and use a quantum computer in the future to break the cryptography employed [7] and the fear is that secret services are actively doing so [6].

Consequently, a new class of cryptographic schemes which are secure against attacks from quantum computers is being developed and standardized [5]. Although secure against quantum attacks, those new methods typically come with severe limitations compared to the ones used today, such as huge keys or high computational requirements.

For secure network communication, most VPN solutions use a key exchange method, like the Diffie-Hellman key exchange, or an asymmetric encryption scheme, like RSA, to derive a shared session secret. To make the protocols post-quantum safe not only the cryptographic primitives have to be replaced, but also the structure of the protocol has to be modified [11, 2].

In the IPsec protocol suite, the key exchange is handled by the IKEv2 protocol [3], which by design utilizes a single Diffie-Hellman key exchange. In the talk, we give an overview of existing quantum-resistant key exchange methods and their integration into the IKEv2 protocol to defy future quantum-based attacks. We discuss the progress in the NIST standardization efforts and explain how future implementations of the IPsec protocol suite can withstand quantum attacks.

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-22

References

[1] Lily Chen et al. *Report on Post-Quantum Cryptography.* NISTIR 8105 (Draft). U.S. Department of Commerce/National Institute of Standards and Technology, Feb. 2016. URL: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

[2] ETSI. *ETSI TR 103 617: Quantum-Safe Virtual Private Networks.* Technical Report DTR/CYBER-QSC-009. European Telecommunications Standards Institute (ETSI), Sept. 2018. URL: https://www.etsi.org/deliver/etsi_tr/103600_103699/103617/01.01.01_60/tr_103617v010101p.pdf.

[3] Kaufman, C. and Hoffman, P. and Nir, Y. and Eronen, P. *Internet Key Exchange Protocol Version 2 (IKEv2).* RFC5996. Sept. 2010. URL: %7Bhttp://tools.ietf.org/rfc/rfc5996.txt%7D.

[4] J. C. F. Matthews, A. Politi, and J. L. O'Brien. "Shor's Quantum Factoring Algorithm on a Photonic Chip". In: *Science* 325.5945 (2009), p. 1221.

[5] National Institute of Standards and Technology. *Post-Quantum Crypto Project.* http://csrc.nist.gov/groups/ST/post-quantum-crypto/. 2016.

[6] National Security Agency. *NSA Utah Data Center – Serving Our Nation's Intelligence Community.* https://nsa.gov1.info/utah-data-center/. [Online; accessed 02 August 2019]. 2019.

[7] Steven Rich and Barton Gellman. "NSA seeks to build quantum computer that could crack most types of encryption". In: *The Washington Post* (Jan. 2014). URL: https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html.

[8] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509.

[9] Frank K. Wilhelm et al. *Entwicklungsstand Quantencomputer.* Studie BSI Projektnummer 283. Bundesamt für Sicherheit in der Informationstechnik (BSI), Mai 2018. URL: https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer_node.html.

[10] N. Xu et al. "Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System". In: *Physical Review Letters* 108.13, 130501 (2012), p. 130501. arXiv: 1111.3726 [quant-ph].

[11] Ephraim Zimmer. "Post-Quantum Kryptographie für IPsec". In: *Sicherheit in vernetzten Systemen - 22. DFN-Konferenz.* Ed. by Christian Paulsen. DFN-CERT, 2015.