Post-Quantum Software Updates

Stefan-Lukas Gazdag
Research Engineer
genua GmbH
Kirchheim bei München

28th Crypto Day, 7/8 June 2018

As one of our efforts in the field of post-quantum cryptography we have worked on bringing hash-based signatures into practice. In this presentation we present hands-on experience and lessons learned from the process of transferring academic research to actual use in real-world applications, first and foremost the use of the eXtendend Merkle Signature Scheme (XMSS) for software updates.

In a three year industrial research project which was undertaken in cooperation with TU Darmstadt, Germany, and which ended in June 2017, we have been working on practical aspects of hash-based signature schemes and the steps required to integrate these schemes in suitable use cases with a focus on update mechanisms.

We use XMSS, a modern hash-based signature scheme. It is described in an IETF/IRTF Internet-Draft Huelsing, Butin, Gazdag, Rijneveld & Mohaisen (2018), which was written in cooperation with TU Eindhoven and which is likely to become an RFC within the next few weeks. Though many applications like key exchange methods or resulting use cases for e.g. TLS or SSH receive more attention than the somewhat basic software or product updates, these are essential for IT companies: Once quantum attacks emerge, it is quite troublesome for manufacturers if their products are not yet post-quantum secure and have to be updated. Only by adapting update mechanisms to use post-quantum schemes like hash-based signatures one can provide reliable updates for customers and users. Hash-based signatures are suitable for the early adoption of quantum-safe schemes and are therefore an important starting point towards fully post-quantum secure products.

We have already introduced XMSS as additional update signatures for some of our products and want to share our experience on overcoming peculiarities like the statefulness of most hash-based signature schemes and other stumbling blocks to the implementation of post-quantum schemes.

We also want to give a brief overview on the pros and cons of using hash-based signatures in other scenarios such as SSH.

References

Andreas Huelsing, Denis Butin, Stefan-Lukas Gazdag, Joost Rijneveld & Aziz Mohaisen (2018). XMSS: Extended Hash-Based Signatures. Internet-Draft draft-irtf-cfrg-xmss-hash-based-signatures-12, Internet Engineering Task Force. URL `https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-xmss-hash-based-signatures-12`. Work in Progress.

crypto day matters 28 (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-11