CYBERSECURITY
RESEARCH LAB

CRL 101 Series

Crypto Agility through Hybrid Cryptography

By Brian Goncalves & Dr. Atefeh Mashatan

Cryptography allows digital communication to remain private and confidential through the use of encryption, and still have trust and authenticity by way of digital signatures, hash functions, and message authentication codes (MACs). These primitives act as some of the building blocks that the digital world is built upon, and are based on resource intensive and difficult to solve math problems in order to make them safe to use. When the security of a cryptographic primitive is guaranteed by the computational difficulty of an underlying mathematical problem, we refer to it as a computationally secure primitive. The alternative is an unconditionally secure primitive which is proven to be secure regardless of the computational power of the attackers.

As we have seen in the past, computational assumptions surrounding an attacker's capabilities may have expiry dates. Indeed the attackers, like the rest of us, will have access to more powerful computing infrastructure as time passes. Moreover, there may be more efficient ways of solving an encryption scheme's underlying mathematical problem that have not been discovered yet. As a result, there is no guarantee that the cryptographic primitives we use today will remain secure. As such, it is imperative to transition to new algorithms that are more secure. When an exploitable flaw in the algorithm or code is found, such as the KRACK attack for WPA2 WIFI protocol (Vanhoef and Piessens 2017), the algorithms can no longer be used.

However, abandoning the algorithms in use is not a simple task and can, in fact, be a complicated, costly, and time-consuming process. In a large organization there may be numerous upstream and downstream dependencies on a single cryptographic function. Hence, changing a cryptographic primitive may dictate a wide variety of other changes in hardware, software and networking infrastructure of an organization that deals with a lot of legacy hardware and applications. Vendor dependencies can add another layer of complexity to this transition so it is imperative for any organization anticipating a cryptographic transition to plan ahead and dedicate adequate resources to this change.

Cryptographic agility is therefore the ease with which organizations can carry-out cryptographic transitions (Mehmood 2018). Importantly, it is not a singular end state, but rather and ongoing process of planning and preparing. Most organizations are not currently agile enough to carry out cryptographic transitions within a reasonable timeframe. This has been demonstrated in several major recent cryptographic transitions the industry has gone through. For example with symmetric encryption algorithms DES and 3DES to AES (NIST 2004, 2017), and with hash functions SHA-1 to SHA-2 (NIST 2011). Although these algorithms are no longer thought to be secure or part of acceptable standards set by regulatory agencies such as the National Institute of Standards and Technology (NIST), or European Telecommunications Standards Institute (ETSI), they lingered long after new standards were introduced. In fact, many organizations are still not completely free of SHA-1 certificates. In 2017, a study found that of 33 million websites analyzed, 21% of websites were still using SHA-1 certificates (Venafi Research 2017), years after destandardization.

There is another major cryptographic transition that the industry is anticipating in the horizon. It is one that is perceived to be much bigger than the recent cryptographic transitions, creating a lot of

discussions with some comparing it with the Y2K and the chaos that came with it. It has been aptly named as Y2Q, Years to Quantum (Hutchinson 2018).

Quantum computers pose a serious and significant threat to much of public key cryptography as they are able to quickly solve the mathematical problems which public key cryptography is based on, thanks to Shor's algorithm (Shor 1994). The CRL 101: Quantum Threat provides some insight on how the developments in quantum computing will impact the world of information security.

As part of their efforts in helping the industry become resilient against the quantum threat, NIST put forth a request for post-quantum cryptographic algorithms for standardization in 2016 (NIST 2016). The standardization process is expected to be completed between 2022-2024 (NIST 2019). However, as previously discussed fully transitioning away from insecure algorithms is a difficult and slow process, and can leave a significant gap in security. By 2031, for instance, there is a 50% chance that "some of the fundamental public-key cryptography tools upon which we rely today will be broken" (Mosca 2015), leaving a relatively small window in which it will still be secure to use. It is then still an important question as to what can ease this transition and what can be done now that prepares us for this upcoming industry-wide change. In other words, what can increase our cryptographic agility and ensure security both *during* and after the transition to protect against quantum computers?

Hybrid Cryptography is an approach that addresses all these challenges through the use of *hybrid cryptosystems*. A hybrid cryptosystem is a cryptographic system which uses both traditionally secure and quantum-resistant components. Importantly, hybrid cryptosystems are able maintain security against either traditional or quantum attacks. This dual resistance means that hybrid cryptosystems are well suited for the challenges presented by quantum computers transitioning to newer algorithms (Bindel et al. 2018).

By developing hybrid cryptosystems that work with generic algorithms, both older and newer algorithms can be replaced more efficiently to help cryptographic agility. Equally important, the systems also solve the gap in security presented as dual resistance ensures that even if older, less secure algorithms remain in use after destandardization the risk of them being exploited is marginal. Consequently, this also means that transitioning can be done on a longer timeframe offsetting the cost and other factors delaying more immediate action.

Here at the Ryerson Cybersecurity Research Lab (CRL), both cryptographic agility and hybrid cryptography are active areas of research. Research into cryptographic agility is motivated by real world constraints faced in industry settings and seeks to address these constraints in a practical and effective manner. Research into hybrid cryptography seeks to develop new hybrid cryptosystems with provable security that are computationally efficient, and easily adoptable on top of current cryptographic infrastructure.

July 22, 2019
CRL 101 Series

References

Vanhoef, Mathy, and Frank Piessens. "Key Reinstallation Attacks." *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS 17*, 2017. doi:10.1145/3133956.3134027.

Mehmood, Asim. "What Is Crypto-agility and How to Achieve It?" What Is Crypto-agility and How to Achieve It? Accessed July 29, 2019. https://content.hsm.utimaco.com/blog/what-is-crypto-agility-and-how-to-achieve-it.

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), and Department of Commerce. "Announcing Proposed Withdrawal of Federal Information Processing Standard (FIPS) for the Data Encryption Standard (DES) and Request for Comments." Federal Register. July 26, 2004. Accessed July 29, 2019. https://www.federalregister.gov/documents/2004/07/26/04-16894/announcing-proposed-withdrawal-of-federal-information-processing-standard-fips-for-the-data.

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), and Department of Commerce. "Update to Current Use and Deprecation of TDEA." CSRC. July 11, 2017. Accessed July 29, 2019. https://csrc.nist.gov/News/2017/Update-to-Current-Use-and-Deprecation-of-TDEA.

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), and Department of Commerce."Announcing Draft Federal Information Processing Standard 180-4, Secure Hash Standard, and Request for

Comments." Federal Register. February 11, 2011. Accessed July 29, 2019. https://www.federalregister.gov/documents/2011/02/11/2011-3129/announcing-draft-federal-information-processing-standard-180-4-secure-hash-standard-and-request-for.

"Venafi Research: Twenty-One Percent of Websites Are Still Using Insecure SHA-1 Certificates and Putting Users at Risk." Venafi Research: Twenty-One Percent of Websites Are Still. Using Insecure SHA-1 Certificates and Putting Users at Risk. Accessed July 29, 2019. https://www.venafi.com/news-center/press-release/venafi-research-twenty-one-percent-of-websites-are-still-using-insecure.

Hutchinson, Alex. "Schrödinger's Hack." The New Yorker. April 23, 2018. Accessed July 29, 2019. https://www.newyorker.com/tech/annals-of-technology/hacking-cryptography-and-the-countdown-to-quantum-computing.

P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124-134. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=365700&isnumber=8384

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, and Department of Commerce. "Public-Key Post-Quantum Cryptographic Algorithms: Nominations." CSRC. December 20, 2016. Accessed July 29, 2019.

https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms.

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, and Department of Commerce. "Workshops and Timeline - Post-Quantum Cryptography." CSRC. Accessed July 29, 2019. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline.

Mosca, Michele. "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *Cryptology ePrint Archive, Report 2015/1075.* https://eprint.iacr.org/2015/1075

Bindel, Nina, and Jacqueline Brendel, and Marc Fischlin, and Brian Goncalves and Douglas Stebila. “Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange.” *PQCrypto*(2018).