Post Quantum Trust Anchors

Security and Trust in a post-quantum computing world

Introduction

The potential for the first viable quantum computers to appear on the scene has many in the industry concerned about the impact this will have on current cryptography standards. A quantum computer could break essentially all the public key cryptography standards in use today: ECC, RSA, DSA, and DH.

Someone could store a captured TLS negotiation and decrypt the encrypted data within using a quantum computer sometime in the future, thus breaking the confidentiality of the protected data. In another scenario, if a digital signature used to validate file integrity is embedded in software or burned into a piece of hardware, a quantum computer could be used to forge a new signature of an arbitrary software or data. The potentially malicious forgery would then appear as if it is an authentic asset loaded from a known, trusted entity.

Despite the hype, viable quantum computers are not right around the corner. But extensive, critical efforts are already underway in academia, the standards bodies, and within the industry to devise quantum-resilient algorithms that will continue to keep us secure in the post-quantum (PQ) world.

The remainder of this paper provides an overview of the potential solutions for designing quantum-resilient systems, and what Cisco, in particular, is doing about it today.

Security and trust in a post-quantum world

At Cisco, we take product trust seriously. Cisco Trust Anchor Technologies provide the foundation for trustworthy systems across Cisco. The Cisco Trust Anchor and a Secure Boot check of signed images help ensure that the code running on Cisco hardware platforms is authentic and unmodified, establishing a hardware-level root of trust and an immutable device identity. Subsequent validation of all levels of software running on the platform during startup establishes a chain of trust for the system anchored to the hardware root. Such boot-code-integrity procedures are mandated in the Cisco Secure Development Lifecycle for all Cisco platform-based products. Furthermore, Cisco Trust Anchor Technologies provide product assurance functionality as well as foundational security features: immutable identity, highly secure storage, a random bit generator, and secure key management.

It is natural to prepare Trust Anchor Technologies to be secure in a PQ world. Cisco has already started deploying quantum-secure signatures in a limited number of systems and is continuing to expand their usage.

PQ signatures

Grover's algorithm is a quantum computer search algorithm that is exponentially faster than conventional (non-quantum) computers. It is believed to halve the effective key size used as input to a function. For example, it can search for a 128-bit key in the same amount of time it takes a conventional computer to search for a 64-bit key. Thus, using 256-bit keys in a PQ world is considered as secure as using 128-bit keys in today's classical crypto world.

It is also believed that the effort of finding a pre-image of a hash function is n/2, where n is the output size of the hash. Thus, to have quantum security equivalent to classical 128-bit security level, we would need at least 256-bit hash functions. Brassard et al. claimed that the effort to find a pre-image in the quantum search case is n/3. Thus, we would need 384-bit hashes for 128-bit equivalent quantum security. Bernstein, however, proved that the latter claim is not useful due to practical limitations.

For asymmetric schemes, like signatures, multiple PQ secure algorithms have been proposed for standardization by NIST. At Cisco, we focused on proven schemes based on simple primitives (repeated application of a hash function) that were efficiently implemented in hardware and Field Programmable Gate Arrays (FPGAs). That is why we focused on Hash-based Signatures (HBS). An HBS is composed of information that forms a structure known as a hash tree (or Merkle tree). This structure is built from a collection of one-time signatures (OTS) that serve as the leaves of the tree and are hashed with their siblings to compute the parent in the next level of the hierarchy. At the final level, the root of the tree becomes the public key for all the messages signed by the tree (Figure 1).

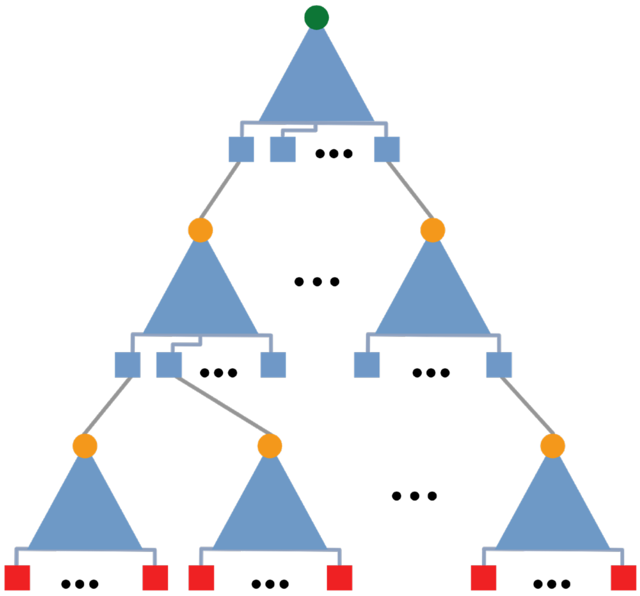


Figure 1: HBS tree using one-time signatures (OTS) as the leaves and forming a Merkle tree to the root. The public key is the root of the tree. A message signature consists of the partially-computed OTS and the path to the root. A verifier verifies that, by using the message and its HBS, they can complete the OTS computation and use the provided path to build a hash tree whose root node value matches the public key.

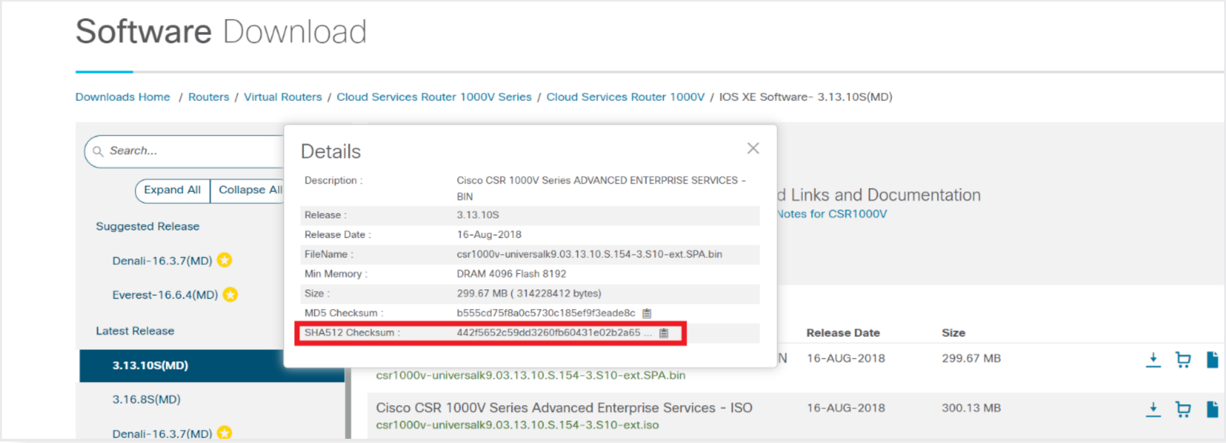
Due to their well-understood and analyzed primitives, HBS schemes are widely accepted as good candidates for quantum-secure signatures. Two stateless HBS schemes are included in Submissions of the NIST PQ Project and two stateful schemes (RFC8391, draft-mcgrew-hash-sigs) have been submitted to the IETF.

What else is Cisco doing?

To make our Trust Anchor technologies secure against a quantum computer, Cisco has started employing quantum-secure key sizes and algorithms in some of our platforms and we are working on adding them into more.

Hashes

We verify software integrity using hashes, so we want to ensure that the hashes we use are PQ secure. To be conservative against any quantum attack of the future, we chose to use 512-bit hashes with our software, which should provide PQ security for many years to come. Thus, we use SHA512 of the SHA2 hash family (Figure 2).



Details

Description :	Cisco CSR 1000V Series ADVANCED ENTERPRISE SERVICES - BIN
Release :	3.13.10S
Release Date :	16-Aug-2018
FileName :	csr1000v-universalk9.03.13.10.S.154-3.S10-ext.SPA.bin
Min Memory :	DRAM 4096 Flash 8192
Size :	299.67 MB (314228412 bytes)
MD5 Checksum :	b555cd75f8a0c5730c185ef9f3eade8c
SHA512 Checksum :	442f5652c59dd3260fb60431e02b2a65 ...

	Release Date	Size
N csr1000v-universalk9.03.13.10.S.154-3.S10-ext.SPA.bin	16-AUG-2018	299.67 MB
Cisco CSR 1000V Series Advanced Enterprise Services - ISO csr1000v-universalk9.03.13.10.S.154-3.S10-ext.iso	16-AUG-2018	300.13 MB

Figure 2: Snapshot of a software download from cisco.com that includes the SHA512 hash for manual integrity verification before loading the software on a virtual machine (VM). The Secure Boot feature provides automatic integrity and authenticity verification of the chain of loaded firmware and software on a device.

Symmetric algorithms

We use constructs like FPGAs to achieve a variety of system functions. Often these FPGAs are used to implement system-critical security functions such as trust anchor designs as well as datapath crypto FPGAs. Where possible, we use 256-bit AES keys to encrypt the configuration bitstream of these devices.

Signatures

We chose HBS for their straightforward implementation and minimal code size, their well-understood nature, and the simple primitives upon which they are based. Scott Flurher and David McGrew are standardizing LMS, a stateful HBS scheme that is the evolution of LDWM. LDWM is an HBS scheme based on research pioneered by Lamport, Diffie, Winternitz, and Merkle decades ago. LMS builds on LDWM by adapting ideas published in Leighton and Micali's work from 1995 and introducing certain parameters that offer domain separation. Readers should note that attacker-produced hash collisions are irrelevant for LMS as LMS never hashes a string where the attacker selects the value.

LDWM is already used as a firmware verification algorithm on certain Cisco platforms. It also exists in Cisco's Trust Anchor modules implemented using FPGAs in various service provider platforms. The parameters chosen include SHA256 hashes, Winternitz parameter W=4 and tree height H=10.

PQ software signing, as designed for certain Cisco FPGAs and hardware when this work started in 2013, currently leverages LDWM in order to verify software images or firmware before loading it. New hardware roadmaps will be switching to more PQ image-signing schemes like LMS.

The future

Ubiquitous PQ Trust Anchors is Cisco's goal. We will continue to introduce quantum-safe algorithms in our Trustworthy Systems technologies. The LDWM and LMS signature schemes will continue to be integrated into more and more platforms.

We will also keep researching PQ cryptography and, along with the industry, introduce it in protocols and use cases in the medium-term in order to achieve a quantum-safe future where confidential data exchanged online and potentially stored today cannot be decrypted at a later time when viable quantum computing becomes available.

Acknowledgments

Panos Kampanakis (panosk[at]cisco[dot]com)
Product Manager, Security & Trust Organization

Chirag Shroff (cshroff[at]cisco[dot]com)
Principal Engineer, Security & Trust Organization

Michael Curcio (micurcio[at]cisco[dot]com)
Senior Hardware Engineer, Security & Trust Organization

References

SPHINCS+ Stateless HBS NIST candidate – https://sphincs.org/

LMS Hash-Based signatures IETF draft – https://tools.ietf.org/html/draft-mcgrew-hash-sigs

XMSS Hash-Based signatures IETF RFC8391 – https://datatracker.ietf.org/doc/rfc8391/

NIST’s PQ Round 1 Submissions – https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

Cisco Trust Anchor Technologies – https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trust-anchor-technologies-ds-45-734230.pdf?ccid=cc000742