QUANTUM RESISTANT CRYPTOGRAPHY

X.509 now: navigating “PQC”

A tale of two approaches - continued

Stiepan A. Kovac, CEO Quantum Resistant Cryptography (EU, US, global) September 5, 2025

Decision point 1: Hybrid v.s. direct KEM(s)

Combining known weak techniques, or betting on strong ones?

- In the migration from current quantum-unsafe mechanisms, 2 approaches are proposed: -“hybrid” (both classical crypto-enabled key exchanges & pqc, usually lightweight such as NTRU or similar lattice-base) -direct (pqc/qrc only)
- From a performance standpoint, the only approach that makes sense is the direct approach: indeed no matter the efficiency of the chosen pqc algorithm, combining it with classical ones makes the overall construction heavier.
- From a security standpoint, if the right (stronger, code-based, as NIST started standardising & ISO does) mechanisms are used, it also makes most sense, with one caveat: as usual in cryptography, the older **and** unbroken, the better.
- Choose wisely, especially in times of multidimensional cognitive warfare.

Decision point 2: when pq needs alternatives

Means of hierarchical key distribution using symmetric keys/certs

- In many cases, such as legacy and/or industrial devices with a long life span, upgrading the hardware to support pqc, as lightweight - and insecure - as it may be (and even less so, a hybrid of it with classical RSA/ECC), is not an immediate possibility. This calls for innovative ways and the payment industry can inspire us here
- One evolutive way to go about it is to upgrade whenever feasible to symmetric-only hierarchical key distribution solutions, typically hash function-based, where keys for specific devices are derived from a root key with a large but limited number of uses, in the manner of a certificate (except it is the number of uses, vs time, that matters).
- Upon expiry/provision, such root keys are replaced with new, securely generated new ones. Ways to do this range from hardware, including but not limited to ‘Q’ RNGs, to strong, hash- and/or other strong symmetric cipher construction-based PRNGs.

Future use cases for PKI and cryptography

The “final” frontier

- Brain computer interfaces provide one of the most interesting and frightening at the same time opportunities to do things “right” security-wise.
- Especially having in mind non-invasive BCIs, knowledge-based authentication may be facilitated (log in with your brain), yet gets challenged too.
- That in turn creates the need for cyber-physical/physiological protection systems, where the credential storage system, in this case our brain, is protected from undue interference and spying (or psying, as I mistyped!).
- Actual postquantum (i.e. beyond quantum physics) tech can be an ally here. To be continued!