PQC AND TLS

Sofía Celi and Thom Wiggers

Preface

- This is definitely not a complete overview
- We will mainly focus on the authentication part of TLS 1.3
- We’re not pitching a draft here or any path to go:
  - Opening the door for discussion
  - Opening the door for experimental design

See NISTs report: https://csrc.nist.gov/publications/detail/nistir/8413/final

Brief note on the KEX of TLS 1.3

- KEX: Key Exchange
- First NIST KEM to-be standard:
  - Kyber [1]
- Round 4 of KEMs:
  - SIKE, BIKE, HQC
- TLSWGs hybrid mechanism: draft-ietf-tls-hybrid-design
  - Parked for the moment
  - The way to go

[1] if NIST can’t resolve the patent situation, they say they may still go for NTRU

Authentication in TLS 1.3

- Certificate-based authentication
- Pre-shared key
- Password-based authentication

Authentication in TLS 1.3

- **Certificate-based authentication**
- Pre-shared key
- Password-based authentication

Certificate-based authentication

- Usage of signatures:
  - **Online** signatures:
    - Signature of the handshake: signing and verifying
  - **Semi-online** signatures (signed at different moments, and verified by different parties)
    - Signature(s) of the certificate chain: offline signing and online (offline) verifying
    - OSCP staple: offline signing and online (offline) verifying
      - Online (i.e. OCSP and CRL) checks are not, generally, performed by major browsers
      - Underlying system certificate library performs the checks
    - SCT: offline signing and online (offline) verifying
      - Depends on browsers policy:
        - Google Chrome requires CT log inclusion
        - Safari requires a varying number of SCTs (https://support.apple.com/en-gb/HT205280)
        - Firefox or Brave do not check or require the use of CT logs (https://bugzilla.mozilla.org/show_bug.cgi?id=1281469)

Post-quantum signatures: tradeoffs

Scheme	**Public key bytes**	**Signature bytes**	**Notes**
RSA-2048	272	256	Pre-quantum
Ed25519	32	64	Pre-quantum
Dilithium-II (MLWE)	1312	2420	NIST's "primary" selection/recommendation
Falcon-512 (NTRU)	897	666	NIST's choice for small signatures "if implemented correctly"
SPHINCS+ 128s	32	8080	slow, conservative
XMSS (RFC8391)	32	979	Stateful hashing not fit for general purpose
On-ramp candidate	*????* *UOV:* >400k uncompressed	"small and fast to verify" UOV: smaller than RSA	Probably no standards before 2028

Prior work: PQ (experiments) on the web

- Google/Cloudflare: CECPQ1, CECPQ2 key exchange
  - https://www.imperialviolet.org/2016/11/28/cecpq1.html
  - https://www.imperialviolet.org/2018/12/12/cecpq2.html
  - https://blog.cloudflare.com/the-tls-post-quantum-experiment/
- Cloudflare: Performance impact of large certificate chains
  - https://blog.cloudflare.com/sizing-up-post-quantum-signatures/
- OpenSSH 8.9 uses NTRUPrime as default key exchange algorithm

Prior work: Academic studies

- PQ authentication in TLS: a performance study
  - https://eprint.iacr.org/2020/071
- PQ TLS on embedded platforms
  - https://eprint.iacr.org/2021/1553 wolfSSL: Kyber/SABER + Falcon/Dilithium
  - https://eprint.iacr.org/2020/308 mbedTLS: Kyber + SPHINCS+
- Prototyping PQ KEX and authentication in OpenSSL and OpenSSH
  - https://eprint.iacr.org/2019/858
- Post-Quantum password-based authentication using RLWE
  - https://eprint.iacr.org/2017/1192

Selection of ongoing IETF work

- pqc@ietf.org
- TLS:
  - draft-ietf-tls-hybrid-design
  - draft-celi-wiggers-tls-authkem
- CFRG:
  - XMSS / LMS RFCs
- LAMPS:
  - draft-turner-lamps-nist-pqc-kem-certificates, draft-massimo-lamps-pq-sig-certificates, draft-perret-prat-lamps-cms-pq-kem, draft-ounsworth-pq-composite-keys, draft-ounsworth-pq-composite-sigs, draft-becker-guthrie-cert-binding-for-multi-auth, draft-uni-qsckeys

THANK YOU!

@claucece
@thomwiggers

See also our CFRG slides for more links!