ChaCha20 + Poly1305 For IPsec & IKE

Yoav Nir

IETF 92

Agenda

- ChaCha20 + Poly1305
- CFRG Draft
- IPsecME Candidate Draft
- Please Support

ChaCha20 + Poly1305

- ChaCha20 is a stream or counter-mode cipher
- Poly1305 is an authenticator function
- Both were designed by D. J. Bernstein
- Both have been reviewed extensively

ChaCha20 + Poly1305

- ChaCha20 offers a performance advantage:

Algorithm	Modern Intel	Old Intel	ARM
AES-CTR	1.95	14.19	19.32
ChaCha20	1.24	4.71	13.29
Advantage	57%	201%	45%

- Source: http://bench.cr.yp.to/results-stream.html

- When comparing AES-GCM to ChaCha+Poly, AES-GCM has a slight advantage on modern Intel

CFRG Draft

- The algorithms were proposed to both IPsecME and TLS.

- The feedback from both groups was: go to CFRG and get their approval.

- So we did: http://tools.ietf.org/html/draft-irtf-cfrg-chacha20-poly1305

CFRG Draft

- NIST-approved algorithms come with a publication that contains great documentation:
    - Algorithm details
    - Pseudo-code
    - Test vectors
    - Implementation advice
- We tried to replicate that in out draft

CFRG Draft

- Multiple implementations based on the draft
- Thorough review
- Security review of the AEAD composition
- Approved. Document is in the RFC Editor’s queue.

IPsecME Candidate Draft

- Simple draft - AEAD only for both IKE and IPsec
    - Early review said the WG didn't want ChaCha20 and Poly1305 separately
- Also defines a UI Suite: "VPN-C" or "Suite-C"
    - "C" stands for "civilian" - non-government
    - Currently uses P-256 for key exchange, and HMAC-SHA256 for PRF
    - Replace with Curve25519 and Blake2 ?

Please Support

- The TLS working group is discussing adopting the equivalent document.
- They would like (yet to be confirmed on the list) to make it a SHOULD-level algorithm in TLS 1.3.
- Best algorithm we have around with good performance and a chance for wide adoption
- Please support