A MODEST PROPOSAL FOR HPKE

Dan Harkins, HPE

IETF 113, March 2022

HPKE does not work well for some use cases

- **Serialization of NIST curves is more than twice as long as it needs to be**
  x-coordinate is all that's needed ("compact output" per RFC 6090)

```
p256 with SEC uncompressed serialization:

041e9081e36299e5d4c7c30f3eeae1b4ccef32b9953f6cd3cf97e3fb76cd7e6791a0e8aee893612305ae4f32b2f9f0219ecede8fabd96ee07c063f802b43731471

p256 with RFC 6090 compact output serialization:

1e9081e36299e5d4c7c30f3eeae1b4ccef32b9953f6cd3cf97e3fb76cd7e6791
```

Simple solution: new KEM assignments for NIST curves using compact output

- **Assumes guaranteed, in-order delivery of frames, fails on lossy networks**
  Management of AEAD nonce is entirely in the HPKE context
  - No way to know which nonce was used with a given ciphertext
  - No way to synchronize after loss/reorder
  - No way to even notice except everything suddenly stops working
  - Packet loss or packet reordering is tragic with HPKE

The Internet does not provide guaranteed, in-order delivery of packets

Addressing lossy networks

- Use a deterministic AEAD mode– no nonce needed

  - To keep the IND-CCA2 assurance of HPKE, this must only be used when the plaintext is idempotent or contains some probabilism that a nonce normally would've provided.
  - Rogaway and Shrimpton paper on SIV* has a security proof for this type of "key wrapping".

- Otherwise, use existing AEAD mode and do a rolling replay window ala RFC 2401

  - Window is a bitmap of received packets, packets can be skipped and received out of order.
  - Replays are dropped and valid packets get marked as received.
  - Valid packets whose sequence number is greater than the window advance the window.
  - Packets that are "too old" will be dropped.

  This requires the sequence number (but not the secret nonce to which it is XOR'd) to be exported as part of the ciphertext– first 4 octets are the sequence number– data that is already exposed to a passive attacker who can count.

* Rogaway, P. and T. Shrimpton, "Deterministic Authenticated Encryption, A Provable-Security Treatment of the Key-Wrap Problem", EUROCRYPT '06, Saint Petersberg, Russia, 2006

Proposal: Add the following…

Compact representation
- New KEMs for NIST curves
- Compact representation (RFC 6090)

Deterministic Authenticated Encryption
- Support for AES-SIV (RFC 5297)
- No nonce generated/used in HPKE context

Option to set in context to use/support replay window
- Both sides must agree
- Agreement in same way everything else is agreed on

Internet-Draft:

draft-harkins-cfrg-dnhpke-01

Source code:

Running Code!

https://github.com/danharkins/hpke-wrap

- Fully compliant with RFC 9180
- Supports compact representation with new KEM values*
- Supports deterministic authenticated encryption ciphers*
- Supports setting a flag to use a rolling replay window for lossy networks
- Complete test vectors (based on the latest version of HPKE test vectors) for new KEMs and ciphers

* Took the liberty of stealing some values reserved to IANA for test vector generation

Adopt as a CFRG Work Item?