IVs, DTLS, and ChaCha

Stephen Kent

BBN Technologies

Quick IV Review

- An Initialization Vector (IV) is fixed size input used with a block or stream cipher
- For some cryptographic modes an IV is required to be random or pseudo-random, but for others it may be predictable, e.g., a counter value
- In all cases, the set of IV values should be unique over the lifetime of a key
- If a receiver needs to be able to decrypt individual packets or messages independent of the order of arrival, it is common to carry an IV with each packet/ message

ESP use of IVs

- ESP allows for carriage of an IV with each packet, as part of the payload
- Each algorithm defined for use with ESP describes how the IV is carried
- Although some algorithms/modes could make use of the ESP packet sequence number as all or part of an IV, they don't: RFC 3686, 4106, 4309, …
- The current proposal for using ChaCha20 with ESP (draft-nir-ipsecme-chacha20-poly1305) follows this convention, i.e., it calls for use of an explicit, per-packet IV

DTLS use of IVs

- AES-CCM and GCM use an explicit 8-byte IV/nonce (RFC 6655)
- Camellia (RFC 6367) uses an explicit 128-bit IV (although it's not clear if this is intended for use with DTLS as well as TLS.
- The current proposal for using ChaCha20 with DTLS (draft-agl-tls-chacha20poly1305) calls for using the TLS record sequence number (plus the 16-bit epoch) as the IV/once.

Why an Explicit, Independent IV?

- If a counter is acceptable as an IV for an algorithm/mode, why not use a packet sequence number if it is already present, big enough, and cleartext?
  - From a security assurance perspective, an IV based on a protocol-supplied value expands the scope of what has to be analyzed (to ensure uniqueness)
  - An algorithm implementation submitted for FIPS evaluation must be independently evaluable
  - If DTLS and ESP adopt different IV approaches for the same algorithm/mode, chip vendors have problems
  - In some cases, a non-counter IV approach can be faster than a counter (in hardware)
  - Allowing each sender to choose its own IV generation approach is more flexible

NIST Approval for ChaCha?

- At the SAAG meeting in Vancouver Tim Polk was asked if NIST would evaluate ChaCha
- Tim didn't say no
- If ChaCha were to be evaluated and approved, one would expect algorithm mode validation would mandate that the IV/nonce be independent of an application/protocol context, as has been the case for all other NIST-evaluated algorithms
- So, if you want to keep that option alive …

QUESTIONS ?