Simple Key Establishment Methods for the TCP-AO Option

Brian Weis

The TCP-AO Use Case

- The TCP Authentication Option (TCP-AO) option is expected to replace the use of RFC 2385
  - Used to protect BGP & LDP routing protocols
- The most important target platforms are very large IP routers operated by service providers
  - Highly available special-purpose routers
  - A router may have many (I.e., up to 2000) BGP peers

Availability

- Commercial network operators consider *availability* to be more important than *integrity* in their threat model
- Any key establishment method will be evaluated by network operators according to its perceived risk to availability.
- A simple and reliable key establishment method is most likely to maintain current levels of *availability*.

Known Simple Key Establishment Methods

- Simple key establishment methods with known security properties exist. E.g.,
  - Key Transport
    - Encrypted key protected with a long-term KEK
  - Key Derivation Using a Counter
    - Derive a key from a master key and a counter

Summary

- *Simple* and *reliable* key establishment is needed.
  - Any method perceived by network operators as negatively affecting *availability* will not be deployed.
- It would be a shame if operators refused to use whatever key establishment method is standardized because it did not match their operational model.
  - We need a clear set of requirements stating the operational constraints