IKEv3

Dan Harkins
IETF 85
Atlanta, GA, USA
What’s the Problem?

• IKEv1 had numerous issues
  – Too many permutations of options
  – Confusing and wordy
  – Hard to implement—needed lots of bakeoffs

• IKEv2 was supposed to fix them; it didn’t
  – IKEv2 has, arguably, more options than IKEv1
  – IKEv2 is, arguably, less wordy and confusing than IKEv1 but that is: 1) arguable; 2) a backhanded compliment
  – Has gone through 40 iterations and “clarifications”, and a few bakeoffs, and still interoperability is problematic

• IKEv2 has growing pains from poor design choices
  – Notify payload is now taking on negotiation responsibilities
  – ECDSA is an inelegant graft; ECC itself is an afterthought
What’s the Solution?

• IKEv3— a slimmed down key exchange for IPsec
  – Fewer options: D-H group, authentication method, hash algorithm, and AEAD scheme
    • Different security levels give rise to options (level --> key length, hash, D-H group, etc)
    • Only need 1 way to skin a cat
  – A fully-specified state machine!
  – Authentication method doesn’t change message flow
  – Concise specification of required and expected behavior, not a collection of colloquialisms
  – True peer-to-peer protocol
    • Both sides can initiate at the same time
    • No initiator/responder, no client/server, just peers
What’s the Motivation?

• Simpler, easier-to-implement specification
  – Compliance to defined state machine ensures interoperability
  – Protocol defined from view of an implementation, not a broad, 3rd party, description of packet flows

• Hit a functionality/complexity sweet spot
  – X% of the functionality causes Y% of the complexity (X < 20%, Y > 70%? Maybe)
  – Keep “need to have” functionality; shed “nice to have” functionality if it causes spec bloat
What’s New/Different With IKEv3?

• One-and-done—no long-lived IKE SA
  – No issues with keep-alives, no issues with deletion of IKE SAs, no delete exchanges, no state to maintain
  – IKEv3 creates IPsec SAs and then goes away

• No ID protection
  – Only entities in the middle can see the IDs and those entities can launch an attack to discover an identity anyway—ID protection was of dubious value

• Attribute assertion, not negotiation
  – Aside from vanity there really isn’t a need for numerous attributes to negotiate—it’s just a key exchange!
  – No point in identifying unchosen D-H groups

• Simpler: just four messages, two from each side
What’s New/Different With IKEv3?

• Mutual authentication based on credential
  – A secure PSK-based method for pre-shared keys
  – Digital signatures for (certified) public keys
  – No authentication asymmetry
  – No EAP!

• Authentication is stated up front, not assumed based on presence/absence/content of payloads

• Assertions defined by attributes
  – No more Proposal/Transform/Attribute cruft
  – No more DOI/IKEv1 baggage

• No need for an encrypted payload
  – Which messages get secured is a matter of the state of the state machine. How they get secured is well-defined.
What Else To Do?

• Add critical, but missing, features
  – NAT traversal
  – Configuration (for when it really is client/server)
  – ???

• Implement it and verify premise (well-defined state machine ensures interoperability)
Questions?