Son of IKE Protocol Reqts

Cheryl Madson
Cisco Systems

Son-of-IKE Protocol Requirements

draft-ietf-ipsec-son-of-ike-protocol-reqts-00.txt

- Goals
- Non-goals
- Scoping
- Protocol characteristics
- Scenarios
- Areas needing additional work

Goals

- Describe the characteristics of an optimal protocol
  - Need to balance the needs of simplicity with sufficient functionality and flexibility
- Describe the scoping and base scenarios that should be accommodated by SOI
  - Scoping has become a requirement for other protocols, why not this one?
  - Protocol designers need to keep in mind operational needs; this is no longer a theoretical exercise

Non-goals

- This draft did not attempt to discuss security requirements
  - Others have been actively discussing this
  - How to describe the requirements in such a way that it doesn't unfairly favor one class of proposal over another, while still being meaningful
- Future revisions of the requirements draft should be expanded to include this

Scoping

- Few protocols (and WGs) can be successful without defining a reasonable scope
- What domains of usage need to be accommodated by SOI?
  - Identify scenarios, discuss details
  - Still allow for some degree of future flexibility

Scoping

- How much of the functionality associated with setting up a secure connection should be a part of SOI?
  - Not answered by this draft, but future ones should
  - Problem not solved until the “external” pieces also addressed

Protocol Characteristics

- Attempt at describing ideal characteristics for a protocol
- Shouldn’t be just fixated on simplicity at expense of other needs

Protocol Characteristics

- Ease of extensibility
  - No clean way of adding new payloads, etc., and declaring their “security criticality”
    - Many implementations will fail if an unrecognized payload is encountered
    - While vendor-ID is useful, it’s been overloaded to “solve” this problem
    - New payloads not hash-protected

Protocol Characteristics

- Modularity
  - Good modularity can be used to:
    - subdivide the protocol into pieces which are more easily understood
    - make pieces of SOI easily available to other key management mechanisms
  - Subdividing the protocol requires defining clean boundaries
    - Important characteristics of this module
    - What does this module require from others
    - What does this module do for others?

Protocol Characteristics

- Improve Convergence Characteristics
  - Peers need to behave in a predictable manner in the face of dropped packets, retransmissions, etc.
  - Peers need to “rapidly” have a common view of the state of the connection
  - Behaviors must be well-understood

Protocol Characteristics

- Improve Simplicity
  - Can be partially addressed by removing unnecessary stuff
  - Can also be addressed by good scoping, modularity and well-defined behaviors
  - Need to consider “ease of accomplishing a particular function”
    - negotiation
    - protocol phases

Authentication and IKE

- Perception of “IKE requires X.509” is a stumbling block in certain cases
  - Some parties won’t deploy it as they don’t want X.509
- What is specified for authentication mechanisms is fairly incomplete, resulting in lots of interoperability problems
- No real discussion of general authentication model
- Base draft needs to spell out what needs to be supplied from any authentication mechanism

Authentication and IKE

- Base draft should have only one mechanism, which is spelled out in more detail
  - All other mechanisms moved to separate drafts, and implementation details spelled out in greater detail

Scenarios

- Identify base scenarios which must be addressed by SOI
  - Incomplete list includes
    - Site-to-Site VPN
    - Remote Access
    - End-to-End
    - Mobile IP

Scenarios

- Currently a rough cut at identifying important classes of criteria that need to be considered/ accomodated
  - Operational characteristics
  - Policy
  - NAT
  - Dynamic addresses
  - Authentication

Future Work

- Tackling security requirements
- Flesh out scoping
  - What functionality should/shouldn't be a part of SOI?
  - Scenario domains of usage
  - Criteria
- The usual editorial stuff…