Requirements Discussion

Cheryl Madson
Cisco Systems

Goals of –00 Document

- Protocol scoping
- Ease of extensibility
- Modularity
- Improve convergence characteristics
- Improve simplicity
- There are tradeoffs: need for weighting?

Protocol Scoping

- What are the important scenarios?
  - Site-to-Site VPN
  - Remote Access
    - Client to RAS
  - Mobile IP
    - Should there be subclass for wireless?
  - End-to-End
    - Subclasses?
  - Traffic types
    - Time/delay sensitive
    - Normal bulk transfer
    - Streaming media

Protocol Scoping

- Need model to evaluate scenarios
  - Operational description
  - Policy/provisioning needs
    - Push vs. pull model?
  - NAT
  - Dynamic addresses
  - Authentication model

Protocol Scoping

- What should be addressed by IKE and what should be addressed elsewhere?
  - "elsewhere" may be another protocol protected via IKE
  - What gets yanked out of IKE still needs to be solved in the same timeframe!
  - NAT discovery
    - Co-existence of UDP encaps?
  - Legacy authentication
  - Policy learning/discovery
  - Provisioning
  - Dead peer detection

Other Protocol Requirements

- Minimal message size and number of messages
- Minimal processing expense
  - Expense relative to lighter-weight devices
  - Expense in crash/restart scenarios on large servers
- If connection establishment requires stuff "outside" of IKE, it should be accommodated by state machine (e.g. handling the provisioning/ policy via a "phase 1.5" or "special phase 2")

Security Requirements Discussion

- Is provable security required?
- Base protocol will use key agreement based on STS
- Repudiation?
- Preshared shared secret keys?
- Identity hiding?
- Stateless cookies?
- What is meaning of PFS?
- DoS protection: what subset needs to be addressed within IKE?
  - (minimum) Delay saving state as long as possible
  - Does one side deserve better DoS protection?