Internet Security Association and Key Management Protocol (ISAKMP)

draft-ietf-ipsec-isakmp-08.txt, .ps

Douglas Maughan, Mark Schneider, Jeff Turner
{wdm, mss, sjt}@tycho.ncsc.mil

Mark Schertler
mjs@terisa.com

Major Changes

- Messages aligned on 4-octet boundaries instead of payloads aligned on 4-octet boundaries
- Clarification of Commit Bit in Flags field and its use with the Informational Exchange
- Informational Exchange - Notify/Delete Payloads
  - Clarification on when to send
  - Clarification on how to handle receipt
  - Under protection of existing ISAKMP SA => impact on values in ISAKMP header

Minor Changes

- SPI's
  - Size field (variable length); Examples changed
  - Relationship to Proposal Payload and Protocol
- Added SPKI Certificate Type
- Notify Message Type values - "binary friendly"
- Clarification on Transform Payload field ordering
- Added clarifying text for processing multiple Proposals - "ownership and control" of SAs

Interoperability Issues

- Data Attributes field in Transform Payload
  - Aligned on 4-octet boundary?
    - If NO, then padding at the end of the message (see Major Changes, first item)
- Informational Exchange IV
  - Generate IV independent from current exchange using procedures outlined in I/O Resolution draft 4
  - Protects against loss of unidirectional Info Exch

Additions - Interoperability

- Certificate Request Payload
  - Removal of # Cert Types and # Cert Auths fields
    - Eliminates parsing problems for multiple certificates and authorities or non-existent authorities (e.g. PGP)
  - Chain multiple Certificate Request Payloads
- Additional Bit in Flags field for Authentication Only Informational Exchange
  - Expected usage with the Notify Payload
  - Allows passing information with integrity checking, but no encryption (e.g. "emergency mode")

Comment Contributors

- John Burke, Cylink
- Greg Carter, Entrust
- Dan Harkins, Cisco
- Angelos Keromytis, U Pa
- Harald Koch, SCC
- Tom Markham, SCC
- Dave Mason, TIS
- Baiju Patel, Intel
- Roy Pereira, TimeStep
- Michael Richardson, ISC
- Ben Rogers, Ascend
- Edward Russell, FTP Soft.
- Jim Ryder, IBM
- Luis Sanchez, BBN
- Norman Shulman, SCC
- Ruth Taylor, NSA
- Matt Thomas, AltaVista
- Richard Waterhouse, GTE
- Elfed Weaver, DERA