2401 v 2401bis

Derek Atkins and Steve Kent

- The processing model has been revised to address new Ipsec scenarios, improve performance and simplify implementation. This includes a separation between forwarding (routing) and SPD selection, several SPD changes, and the addition of an outbound SPD cache and an inbound SPD cache for bypassed or discarded traffic.

- There is also a new database, the Peer Authorization Database (PAD). This provides a link between an SA management protocol like IKE and the SPD.

- The new processing model is based on decorrelation of the SPD, an optimization that allows caching of SPD entries. Decorrleation is not required, but the processing model assumes its use.

- If an implementation uses a decorrelated SPD, the it should send the list of linked, decorrelated SPD entries via IKE v2, when negotiating an SA.

- There is no longer a requirement to support nested SAs or "SA bundles." Instead this functionality can be achieved through SPD and forwarding table configuration.

- SPD entries were redefined to provide more flexibility. Each SPD entry now consists of 1 to N sets of selectors, where each selector set contains one protocol and a "list of ranges" can now be specified for the Local IP address, Remote IP address, and whatever fields (if any) are associated with the Next Layer Protocol (Local Port, Remote Port, ICMP message type and code, and Mobility Header Type). An individual value for a selector is represented via a trivial range and ANY is represented via a range than spans all values for the selector.

- TOS (IPv4) and Traffic Class (IPv6) have been replaced by DSCP and ECN. The tunnel section has been updated to explain how to handle DSCP and ECN bits.

- DSCP values MAY be copied from a tunnel header to the inner header by a receiver, based on per-SA configuration controls.

- For tunnel mode SAs, an SG, BITS, or BITW implementation is now allowed to fragment packets before applying IPsec. This applies only to IPv4. For IPv6 packets, only the originator is allowed to fragment them.

- For tunnel mode SAs, an SG, BITS, or BITW implementation is now allowed to fragment packets before applying IPsec. This applies only to IPv4. For IPv6 packets, only the originator is allowed to fragment them.

- RFC2401bis clarifies that for all traffic that crosses the IPsec boundary, including IPsec management traffic, the SPD or associated caches must be consulted.

- RFC2401bis defines how to handle the situation of a security gateway with multiple subscribers requiring separate IPsec contexts.

- A definition of reserved SPIs has been added.
- Text has been added explaining why ALL IP packets must be checked -- IPsec includes minimal firewall functionality to support access control at the IP layer.

- The tunnel section has been updated to clarify how to handle the IP options field and IPv6 extension headers when constructing the outer header.
- SA mapping for inbound traffic has been updated to be consistent with the changes made in AH and ESP for support of unicast, anycast, and multicast SAs.

- Guidance has been added re: how to handle the covert channel created in tunnel mode by copying the DSCP value to outer header.
- Support for AH in both IPv4 and IPv6 is no longer required.
- PMTU handling has been updated. The appendix on PMTU/DF/Fragmentation has been deleted.

- Added text saying "The IP Security Policy (IPSP) Working Group is a possible future source of guidance. One of their goals is to produce a Internet Draft on a "Security Gateway Discovery, Policy Exchange and Negotiation Protocol."

- Three approaches have been added for handling plaintext fragments on the protected side of the IPsec boundary.
- Added revised text describing how to derive selector values for SAs (from the SPD entry or from the packet, etc.)

- Added a new table describing the relationship between selector values in an SPD entry, the PFP flag, and resulting selector values in the corresponding SAD entry.
- Added Appendix B to describe decorrelation.
- Added text describing how to handle an outbound packet which must be discarded.

- Added text describing how to handle a DISCARDED inbound packet, i.e., one that does not match the SA upon which it arrived.
- IPv6 mobility header has been added as a possible Next Layer Protocol. IPv6 mobility header message type has been added as a selector.

- ICMP message type and code have been added as selectors.
- The selector "data sensitivity level" has been removed to simplify things.
- Updated text describing handling ICMP error messages. The appendix on "Categorization of ICMP messages" has been deleted.

- The text for the selector name has been updated and clarified.
- The "Next Layer Protocol" has been further explained and a default list of protocols to skip when looking for the Next Layer Protocol has been added.

- The text has been amended to say that this document assumes use of IKEv2 or an SA management protocol with comparable features.
- Text has been added clarifying the algorithm for mapping inbound IPsec datagrams to SAs in the presence of multicast SAs.
- The appendix "Sequence Space Window Code Example" has been removed.

- With respect to IP addresses and ports, the terms "Local" and "Remote" are used for policy rules (replacing source and destination). "Local" refers to the entity being protected by an IPsec implementation, i.e., the "source" address/port of outbound packets or the "destination" address/port of inbound packets. "Remote" refers to a peer entity or peer entities. The terms "source" and "destination" are still used for packet header fields.