IPsec support for SCTP in IPv4 and/or IPv6

R. Vamshi Krishna Kuldeep Gharat Gautham Anil

November 27, 2004


IPsec : a framework for security at network layer

There exist many application-specific security mechanism in many application areas.

- PGP,S/MIME for e-mail security
- Kerberos for Client/Server etc.
- Secure Sockets Layer (SSL) for web access

But by using IPsec we implement security at the IP level.

Thus IPsec provides security for not only applictions that have security mechanisms but also to the many security ignorant applications also.


IPsec Architecture

IPsec encompasses these functional areas.

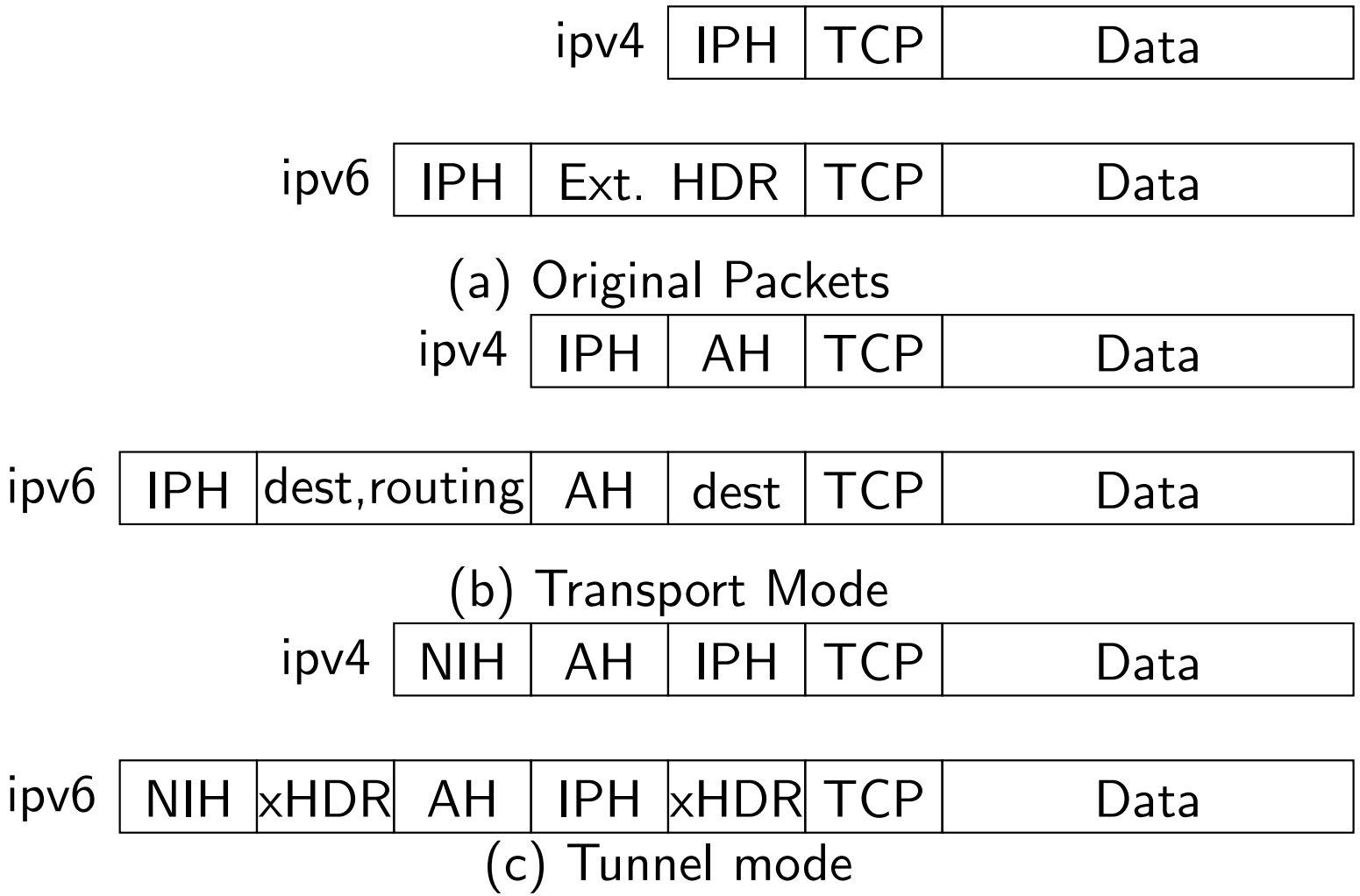
- Authentication Header(AH)
  - AH protocol is used to authentiate packets.
- Encapsulating Security Payload(ESP)
  - ESP protocol is used for packet encryption and optionally also authenticate packets.
- Encryption Algorithms
- Authentication Algorithms
- Key Management
  - Internet Key Exchange(IKE)
- Domain Of Interpretation(DOI)
  - DOI Contains various values like identifiers, selectors for SA etc..


IPsec services

IPsec provides these services.

- Access Control
- Connectionless Integrity
- Data Origination Authentication
- Rejection of Replayed Packets
- Confidentiality
- Limited Traffic flow Confidentiality

Transport Mode vs Tunnel Mode



Security Association(SA)

A Security Association(SA) is a collection of various parameters that two peers negotiate during connection establishment.

- Source and Destination addresses of resulting IPsec header.
- IPsec protocol identifier : AH or ESP or IPCOMP
- Algorithm and secret key used by IPsec protocol
- Security Parameter Index(SPI) - a 32 bit value to identify an SA

Some implementations might include these additional parameters

- IPsec mode (Transport or Tunnel)
- Size of sliding window to protect against replay attacks.
- Lifetime of Security Association

Security Association(SA) and Security Association Database(SAD)

As SA's include both source and destination addresses, it is can protect only one direction of the traffic in a full duplex IPsec communication.
Hence we need two unidirectional SA's, one for inbound packets and the other for outbound packets.

Security Associations only tell us how IPsec is supposed to protect the traffic. We need addition information to define which traffic to protect.

This info is stored in Security Policy(SP) which in turn is stored in Security Policy Database(SPD).

Security Policy(SP)

Security Policy specifies

- Source and Destination address of packets to be protected
  - In transport mode they are same as SA src. and dst. addresses
  - In Tunnel mode they may differ
- Protocol (and port) to be protected
  - Some implementations do not allow defining specific ports
  - In that case all ports are protected
- The SA to use to protect the packet

SCTP : A new transport layer protocol

Stream Control Transport Protocol (SCTP) is a new transport layer protocol approved by IEFT.

- Uses IP as the network layer protocol.
- Is similar to TCP, UDP protocols.
- Like TCP, SCTP
  - Provides reliable transport service
  - Is connection oriented

SCTP : An Improvement over TCP

Unlike TCP, SCTP

- Supports Multi-Streaming
  - This feature allows data to be partitioned into multiple streams
  - They have the property that they can be delivered independently
  - Message loss in any of the streams affects the delivery within that stream
- Supprorts Multi-Homing
  - Multi-Homing is the ablility of a single end point to support multiple IP addresses
  - Beneifit is greater survivability of the session in the presence of network failures
- Is message oriented against the stream oriented nature of TCP

Issues in IPsec support for SCTP

For any IPsec implementation to claim support for SCTP the following issues must be considered

- Proper changes to code to incorporate the new protocol
  - SCTP is very similar to other protocols like TCP
  - Thus will not require much changes
- Supporting Multiple address lists
  - Only one SA must be created even if end-points are multi-homed
  - Every query on an address from the list must return the same SA
  - Hence need for 'list' type for addreses.

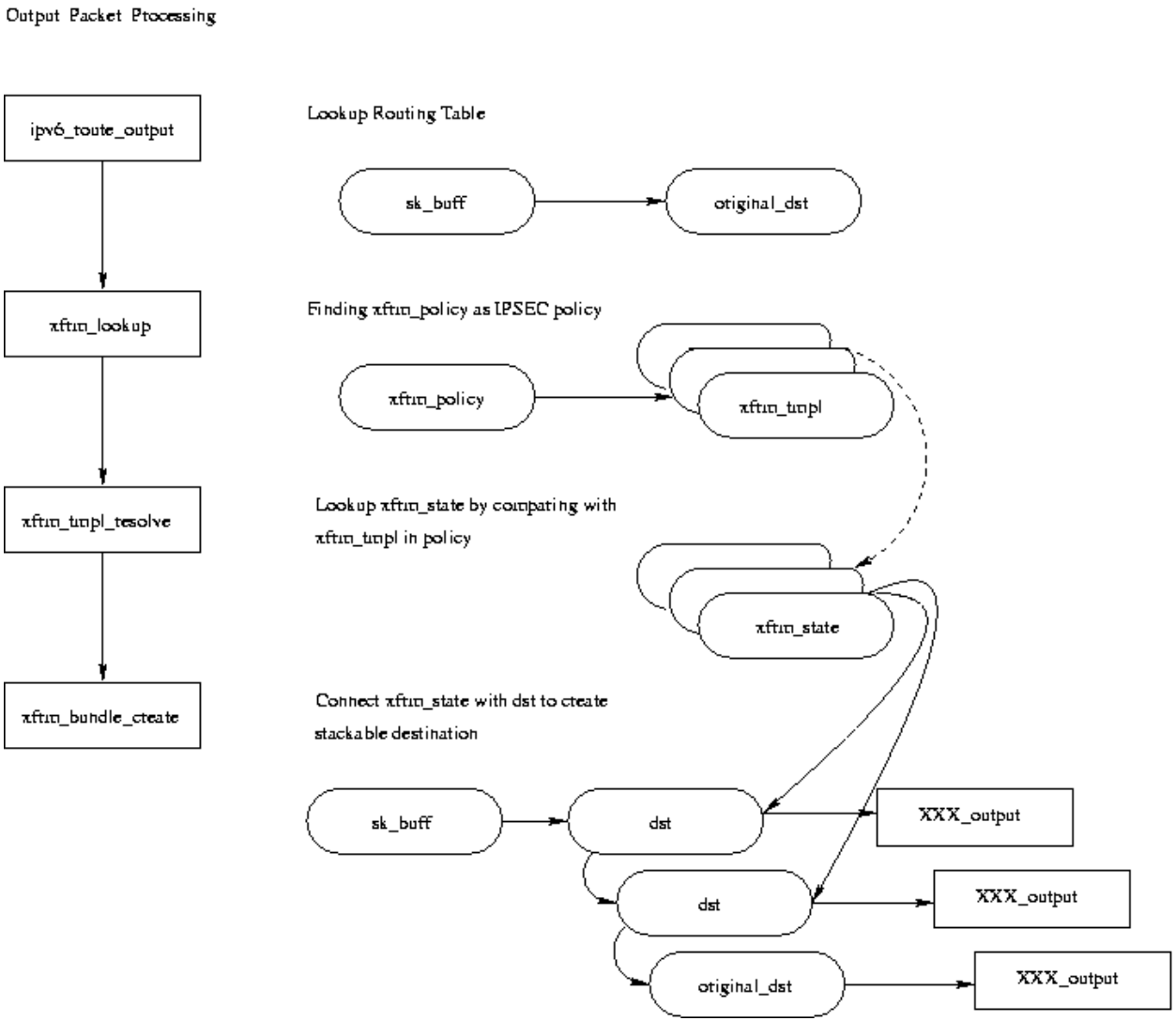
Issues in IPsec support for SCTP

- Supporting Multiple SA's in case of destination does not fully implement the address list feature.
  - Not all implementations at present support the multiple address lists.
  - So until the implementations support multiple address lists, they must be able to setup multiple SA's.

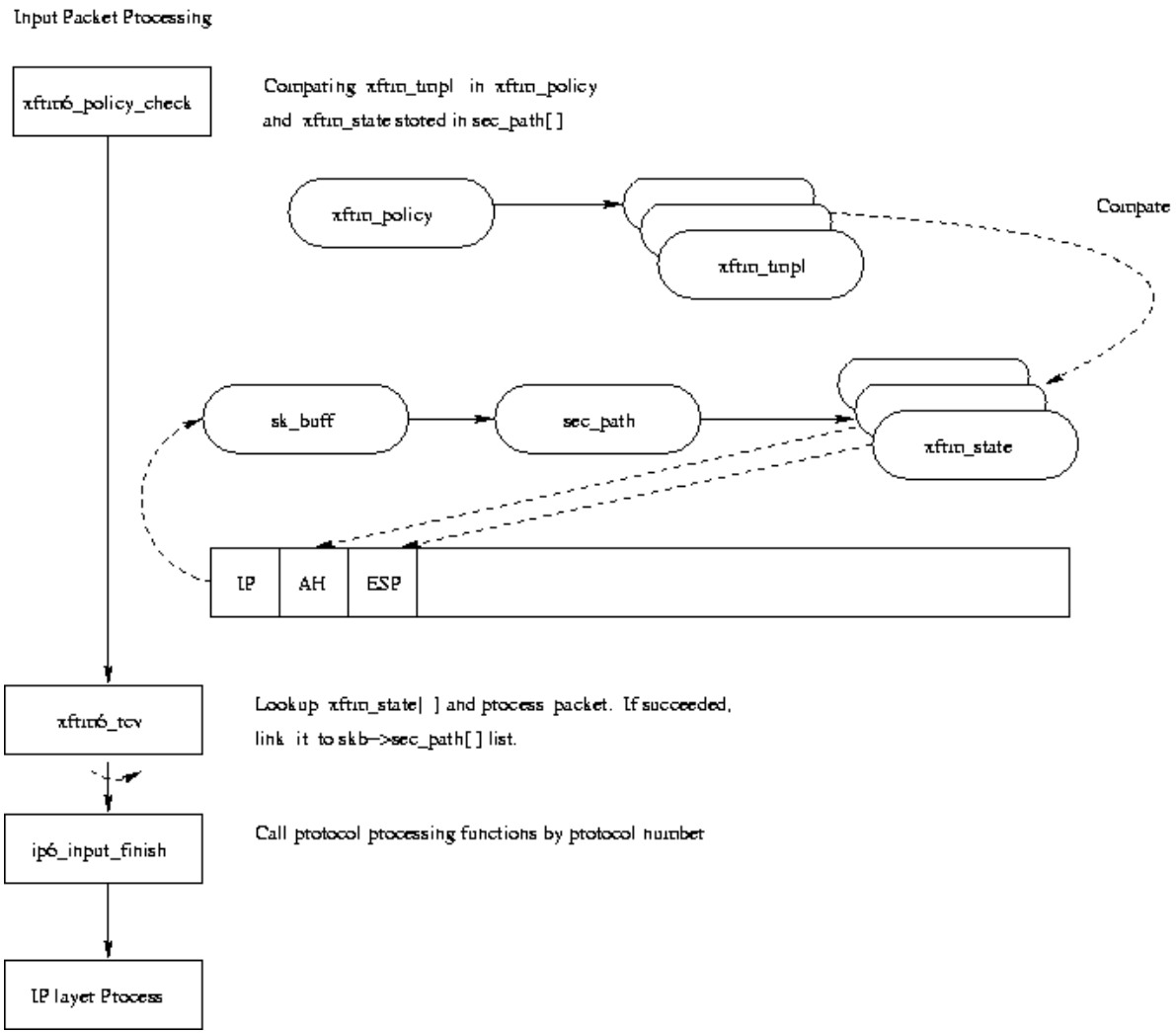
The Linux Kernel IPsec implementation

- A new framework has been introduced since Linux Kernel 2.5.x series.
- It is called XFRM and Stackable Destination.
- XFRM stands for transformer.
- struct xfrm_state stands for SA.
- struct xfrm_policy stands for SP.
- struct xfrm_tmpl is an intermediate structure between xfrm_state and xfrm_policy

IPsec Output packet Processing



IPsec Input Packet Processing



Proposed modifications and enhancements

After studying the underlying kernel implementation we propose the following

- Create a new data structure to implement address lists
- Implementation can create multiple SPD entries or a single entry.
- Include the 'address list' as selector in SA
- Incorporate changes to IKE to be able to send address lists in digital certificates.
- Write a new function or modify an existing function to create multiple SA's if a destination does not support address lists.

Bibliography


Steve Bellovin.
On the use of Stream Control Transmission Protocol (SCTP) with IPsec, July 2003.


S. Kent.
IP Authentication Header, November 1998.


S. Kent.
IP Encapsulating Security Payload, November 1998.


Q. Xie R. Stewart.
Stream Control Transmission Protocol (RFC 2960)., October 2000.

Dummy MultiColoured Table

Courses			
Course code	Course Name	Instructor	Credit/Audit
CS 621	Artificial Intelligence	Prof. Pushpak Bhattacharyya	Credit
CS 601	Algorithms and Complexity	Prof. Sundar Vishwanathan	Credit
CS 631	Implementation techniques in DBMS	Prof. Krithi Ramamritham	Credit
CS 701	Software Laboratory	Prof. G. Sivakumar	Credit
CS 694	Seminar		Credit
HS 699	Communication and Presentation skills		

Dummy Graph using GnuPlot