IPSec implementation for SCTP

Aditya Kelkar
Alok Sontakke
Srivatsa R.

Dept. of CSE. IIT Bombay

October 31, 2004

1. Stream Control Transmission Protocol (SCTP)
2. IPSec
3. SCTP and IPSec
4. Proposed Modifications to IPSec
5. Conclusion and Future Work

Features and Comparison of SCTP[4] with TCP

- Connection Oriented , Unicast Protocol

Features and Comparison of SCTP[4] with TCP

- Connection Oriented , Unicast Protocol
- SCTP is Message Oriented

Features and Comparison of SCTP[4] with TCP

- Connection Oriented , Unicast Protocol
- SCTP is Message Oriented
- SCTP Multi-Streaming Feature

Features and Comparison of SCTP[4] with TCP

- Connection Oriented , Unicast Protocol
- SCTP is Message Oriented
- SCTP Multi-Streaming Feature
- SCTP Multi-Homing Feature

SCTP Message Format

- Header
  - Source and destination port numbers
  - 32-bit verification tag
  - 32-bit checksum

SCTP Message Format

- Header
  - Source and destination port numbers
  - 32-bit verification tag
  - 32-bit checksum
- Data/Control Chunk
  - Chunk type
  - Flag field
  - Length
  - Value

Benefits of SCTP

- Acknowledged reliable non-duplicated transfer of user data
- Application-level segmentation to conform to the maximum transmission unit (MTU) size
- Sequenced delivery of user datagrams within multiple streams
- Optional multiplexing of user datagrams into SCTP datagrams
- Enhanced reliability through support of multihoming at either or both ends of the association
- Congestion avoidance and resistance to flooding and masquerade attacks

Applications of SCTP

- **Telephony Signaling** - Loosely correlated messages (different calls) can be delivered without having to maintain overall sequence integrity.

Applications of SCTP

- **Telephony Signaling** - Loosely correlated messages (different calls) can be delivered without having to maintain overall sequence integrity.
- **Transfer of Multimedia documents** - SCTP allows transport of these components to be partially ordered rather than strictly ordered, and may result in improved user perception of transport.

IPSec [2]

- IPSec is a security mechanism in the TCP/IP protocol suite.
- IPSec operates between layers 2/3. Security services can be applied to layers 3-7.
- Provides following security services
    - **Confidentiality** - Sender can encrypt packets, decrypted by only designated receiver.
    - **Integrity** - Packets are not altered in transit.
    - **Data origin authentication** - Receiver can authenticate the sender.
    - **Anti replay service** - Receiver can detect replayed packets and reject them.
    - **Key management** - Secure exchange of keys.

IPSec Architecture

IPSec architecture includes standards for

- Encapsulating Security Payload (ESP).
- Authentication Header (AH).

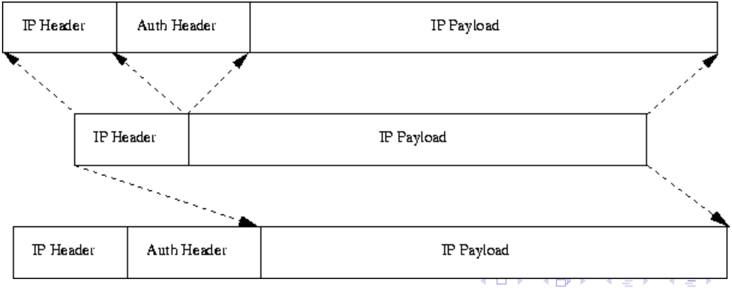
These two protocols operate in two modes.

- Tunnel mode - Applied to the whole packet.
- Transport mode - Applied to payload and selected portions of IP header.

Authentication Header

Authentication Header contains the checksum of fields with a pre-shared key.

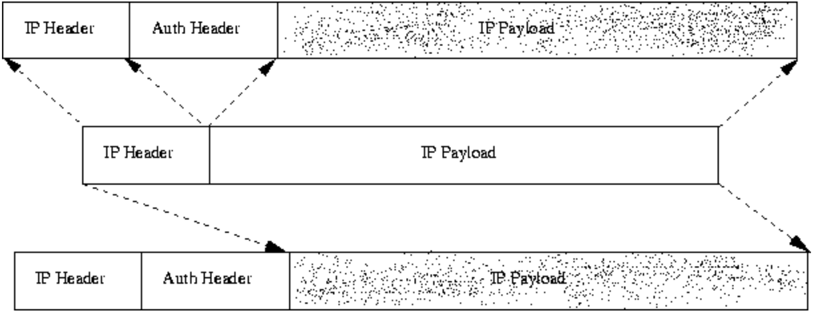
Reciever verifies the integrity by recomputing the checksum and comparing it with the checksum in the packet.



Encapsulating Security Payload

Sender encrypts the packet/payload with a pre-shared key.

Only receiver can decrypt the packet and recover the plaintext.



Security Policies (SPs)

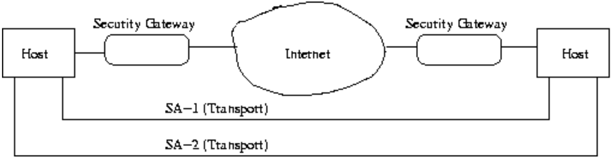
- Specifies security serivces and how they are to be applied to IP traffic.
- Policies are selected by matching selectors.
    - Source/Destination IP address.
    - Source/Destination ports.
    - Transport layer protocol.
    - User ID.
    - Data sensitivity level.
- Bypass, Apply, Drop?
- Process by applying bundles of transformation.

Security Association (SA)

- One-way connection between communicating parties.
- Parameterized by Destination Address, IPSec protocol and a unique 32-bit integer - SPI.
- Established when parties start communicating.
- Each bi-directional connection must create atleast two SAs.
- Security Association Database (SAD) stores all the parameters associated with an SA.
  - Sequence Number.
  - Sequence counter overflow.
  - Anti reply window.
  - Authentication Algorithm and Keys (for AH).
  - Encryption Algorithm and keys (for ESP).
  - Authentication Algorithm and keys for ESP.
  - Lifetime of the SA.

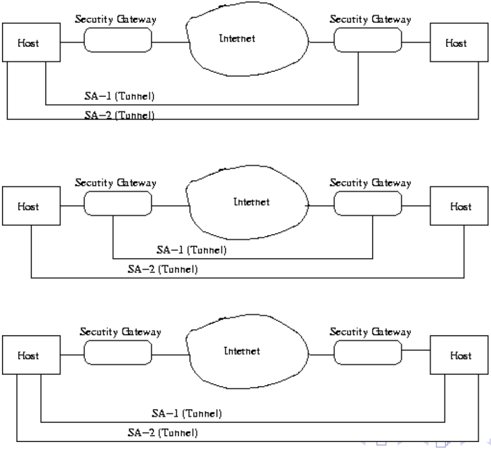
Combining security associations

- Security associations can be combined into bundles in two ways.
- Transport adjecency.



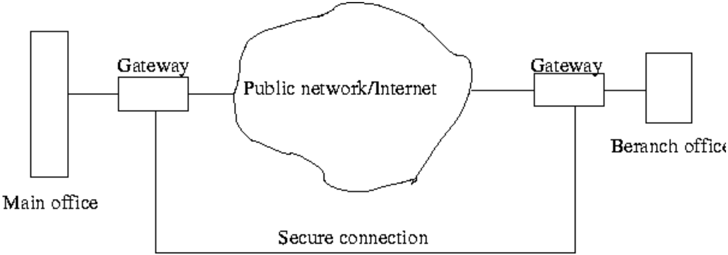
Combining security associations

- Iterated tunneling



IPSec Application - Secure Branch office connectivity

IPSec can be used for secure connection between main office and branch office.



SCTP over IPSec [1]

Why current IPSec implementation needs to be modified?

- Using SCTP endpoints in selectors - source and destination port numbers

SCTP over IPSec [1]

Why current IPSec implementation needs to be modified?

- Using SCTP endpoints in selectors - source and destination port numbers
- Single SA should specify all source-destination address pairs

SCTP over IPSec [1]

Why current IPSec implementation needs to be modified?

- Using SCTP endpoints in selectors - source and destination port numbers
- Single SA should specify all source-destination address pairs
- SPD entries should specify multiple source-destination IP addresses

SCTP over IPSec [1]

Why current IPSec implementation needs to be modified?

- Using SCTP endpoints in selectors - source and destination port numbers
- Single SA should specify all source-destination address pairs
- SPD entries should specify multiple source-destination IP addresses
- IKE

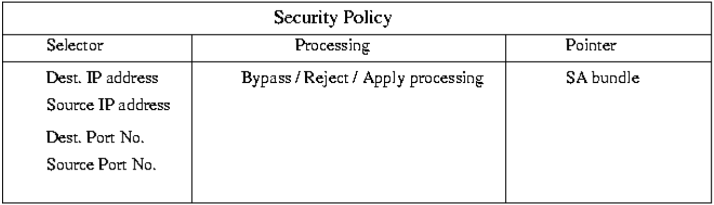
SCTP over IPSec [1]

Why current IPSec implementation needs to be modified?

- Using SCTP endpoints in selectors - source and destination port numbers
- Single SA should specify all source-destination address pairs
- SPD entries should specify multiple source-destination IP addresses
- IKE
- Address updates of SCTP sessions must be authenticated

Data structures for SAD and SPD

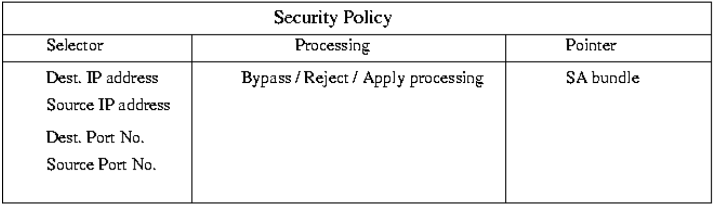
- Security Policy



Security Policy		
Selector	Processing	Pointer
Dest. IP address Source IP address Dest. Port No. Source Port No.	Bypass / Reject / Apply processing	SA bundle

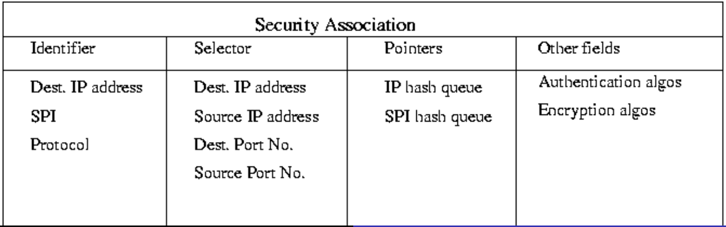
Data structures for SAD and SPD

- Security Policy



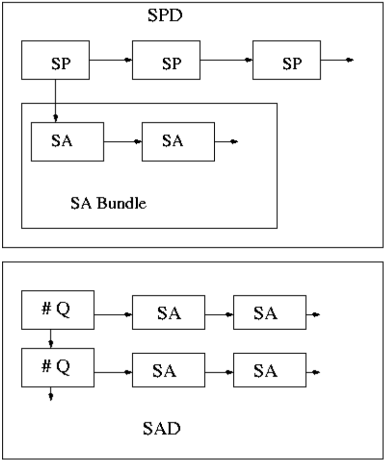
Security Policy		
Selector	Processing	Pointer
Dest. IP address Source IP address Dest. Port No. Source Port No.	Bypass / Reject / Apply processing	SA bundle

- Security Association



Security Association			
Identifier	Selector	Pointers	Other fields
Dest. IP address SPI Protocol	Dest. IP address Source IP address Dest. Port No. Source Port No.	IP hash queue SPI hash queue	Authentication algos Encryption algos

Current organization of these structures



IPSec Packet Processing

- Input
    - IP packet to be sent
    - Refers to SPD for type of processing
    - Follows SA bundle to apply series of transformations.
    - Each transformation adds an IPsec header.

IPSec Packet Processing

- Input
  - IP packet to be sent
  - Refers to SPD for type of processing
  - Follows SA bundle to apply series of transformations.
  - Each transformation adds an IPsec header.
- Output
  - Find the SA in SAD
  - Apply reverse transformation
  - Continue till Transport/IP header is encountered
  - Check from SPD that all reverse transformations have been applied.

Proposed Changes

- What ?
  - Incorporate multiple source/destination addresses into data structures.

Proposed Changes

- What ?
  - Incorporate multiple source/destination addresses into data structures.
- Where ?
  - One SA and SP for each address pair.
  - Modify the address structure itself to include multiple addresses.
  - Modify SA and SP.

Proposed Changes

- What ?
  - Incorporate multiple source/destination addresses into data structures.
- Where ?
  - One SA and SP for each address pair.
  - Modify the address structure itself to include multiple addresses.
  - Modify SA and SP.
- Why ?
  - Changing address structure causes unwanted changes since is used not just in SAD and SPD.
  - Multiple SA's consumes more memory , affects search time , negotiation time.

How proposed changes will affect the management of the data structures

- Functions creating the structures.
- Inserting SA's into hash queues requires multiple insertions in required hash queues.
- Matching selectors should incorporate multiple addresses.

Conclusion

How to extend IPSec support for SCTP.

Methods by which multiple addresses can be negotiated in IPSec have been proposed.

Comparison of these methods.

Future Work

Extraction of SCTP port numbers to use in selectors for SPD.

Extend key negotiation in IKE[3] to negotiate single SA for multiple addresses.

References

beamericonarticle S. Bellovin et. al.
Rfc-3554: On the use of stream control transmission protocol (sctp) with ipsec, 2003.

beamericonarticle S. Kent et. al.
Rfc-2401: Security architecture for the internet protocol, 1998.

beamericonarticle D. Harkins.
Rfc-2409: The internet key exchange (ike), 1998.

beamericonarticle R. Stewart.
Rfc-2960: Stream control transmission protocol, 2000.

Thank you!!!

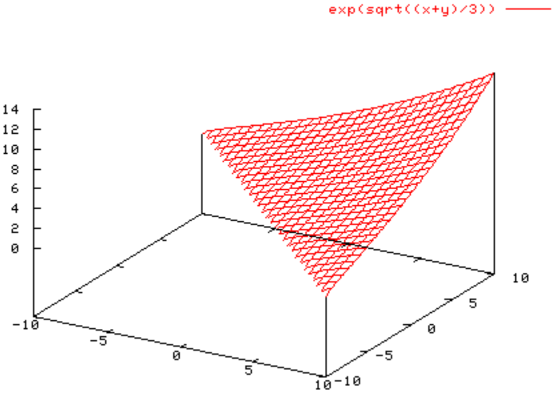
Thank you!!!

Table with 5 colours and multicolumn

Course	Date	Time
Algorithms	23/11/2004	2:30
FSVP	14/11/2004	10:30
Artificial Intelligence	19/11/2004	2:30
Seminar	Hooray! no endsem!!	
Communication Skills	Hooray! endsem over!!	

Graph with gnuplot

Equation: $e^{sin(\sqrt{(x+y)})}$



Simple picture using PGF