4/12/07

IPsec

TCP | Data | - End to end

IP

S Connectionless R

IPsec - Provide security in the network.

Solution for Network Security
IPsec

1. Authentication
2. Confidentiality
3. Key Management
1) Authentication Header

AH

2) ESP - Encapsulating Security Payload

<table>
<thead>
<tr>
<th>AH</th>
<th>ESP (Encrypt)</th>
<th>ESP (Encrypt + Authentication)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Comm Integrity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data origination authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Replayed attack determined</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Confidentiality

Limited traffic flow

Confidentiality

Confidentiality
Replayed attack

32 bit sequence no.

Receiver Window

N-W+1

N
Architecture

- ESP
  - Encryption Algorithm

- AH
  - Authentication Algorithm

- DOI (Domain of Interpretation)

  - Key Management
Database
Security Association Database (SA)
Transmit IPsec to destination X

S - how to transmit,
Security parameters Index
Key, the algorithm, seq no.

Security Policy Database
AH:

IPv 4 and IPv 6

(1) Transport Mode
(2) Tunnel Mode.

<table>
<thead>
<tr>
<th>TCP</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>TCP</td>
</tr>
</tbody>
</table>

AH

| IP | AH | TCP | Data |

AH - Next Header
Payload Length - AH in terms of 32 bit word
SPI
Sequence no.
MAC, ICV
Tunnel Mode

ESP

Transport Mode

HMAC: $\{\text{MD5, SHA-1}\}$ - 96 bits