IP vulnerabilities

Password sniffing

IP Spoofing
- host rename (LAN)
- DNS
- source routing
- TCP sequence number guessing / splicing

Session hijacking

Denial of service
- ICMP bombing, redirects, unreachable
- application(ftp, mail, echo) bombing
- TCP SYN flooding

Port probes

AT&T attacks Feb/Mar '92

guest/demo/visitor logins  296
rlogins                      62
FTP passwd fetches           27
NNTP                         16
portmapper                   11
whois                       10
SNMP                        9
X11                          8
TFTP                         5
systat                       2
NFS                          2

Number of evil sites 95
IPv6

next generation TCP/IP

- Larger addresses (128 bits)
- Improved performance
  - expanded routing
  - header format simplification
  - flow labeling
  - priority (QoS)
- Security
- Interoperability with IPv4

IPv6 Header

<table>
<thead>
<tr>
<th>40 octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
</tr>
<tr>
<td>Payload length</td>
</tr>
<tr>
<td>Source Address</td>
</tr>
<tr>
<td>Destination Address</td>
</tr>
</tbody>
</table>

V. (4bit) : 6
T. C.(8bit) : distinguish between different classes or priorities of IPv6 packet (under study)
F. L.(20bit) : used by a host to label packet for special handling
P. L.(16bit) : length of remainder of IPv6 packet following the header
N. H.(8bit) : Identify the type of header immediately following IPv6 packet
H. L.(8bit) : remaining number of allowable hops for this packet
S.A. (128bit) , D.A(128bit)
IPv6 Extension Headers

- Hop-by-hop Options header: define special options that require hop-by-hop processing consisting of Next Header (8bit), Header Extension Length (8bit), and Options
- Routing Header: Provides extended routing
- Fragment Header: Contains fragmentation and reassembly information
- Authentication Header: Provides packet integrity and authentication
- Encapsulating Security Payload: provides integrity and privacy
- Destination Option Header: contain optional information to be examined by the destination node

IPv6 Packet with Extension Headers (containing TCP Segment)

<table>
<thead>
<tr>
<th>Octets</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 header</td>
<td>40</td>
</tr>
<tr>
<td>Hop-by-hop Options header</td>
<td>Variable</td>
</tr>
<tr>
<td>Routing header</td>
<td>Variable</td>
</tr>
<tr>
<td>Fragment Header</td>
<td>8</td>
</tr>
<tr>
<td>Destination Options Header</td>
<td>Variable</td>
</tr>
<tr>
<td>TCP header</td>
<td>20 (optional variable part)</td>
</tr>
<tr>
<td>Application data</td>
<td>Variable</td>
</tr>
</tbody>
</table>

: next header field
Architecture of IPSec(II)

Overview of IPSec protocol

(c)Kwangjo Kim
Applications of IPSec

- Secure branch office connectivity over the Internet: VPN
- Secure remote access over the Internet via ISP
- Establishing extranet and intranet connectivity with partners: +SSL
- Enhancing electronic commerce security: SET

IPSec Document

- RFC1825: Security architecture for the Internet Protocol
- RFC1826: IP Authentication Header
- RFC1827: IP Encapsulating Security Payload
- RFC1828: IP Authentication using Keyed MD5
- RFC1829: The ESP DES-CBC Transform
- RFC1851: The ESP Triple DES Transform
- RFC1852: IP Authentication using Keyed SHA
- RFC2085: HMAC-MD5 IP Authentication with Replay Prevention
- RFC2104: HMAC: Keyed-hashing for Message Authentication
- I-D: Internet Security Association and Key Management Protocol (ISAKMP) etc 23 documents
IPSec Document Overview(I)

- Architecture
  - ESP Protocol
  - AH Protocol
    - Encryption Algorithm
    - Authentication Algorithm
    - DOI
    - Key Management

DOI : Domain of Interpretation

(c)Kwangjo Kim

13

IPSec document overview(II)

- Architecture: general concepts, security req't, definitions and mechanisms defining IPsec tech.
- Encapsulating Security Payload (ESP): covers packet format and general issues for packet encryption
- Authentication Header (AH): packet authentication
- Encryption Algorithm: various algorithms for ESP
- Authentication Algorithm: various algorithms for AU
- Key Management: key management
- Domain of Interpretation (DOI): values for the other documents to relate to each other

(c)Kwangjo Kim

14
Security Association(I)

- Sender/receiver security info
- SA for each direction
- Maintained by kernel
- Uniquely identify
  - SPI (Security Parameter Index)
  - IP destination address
  - Security Protocol Identifier
- Specifies
  - encryption key, IV, algorithm
  - authentication algorithm
  - key lifetimes
  - SA lifetime
  - security labels

Security Association(II)

<table>
<thead>
<tr>
<th>Security Parameter</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPI(Security Parameter Index)</td>
<td>2916</td>
</tr>
<tr>
<td>AH Algorithm</td>
<td>MD5</td>
</tr>
<tr>
<td>AH Algorithm Mode</td>
<td>Keyed</td>
</tr>
<tr>
<td>AH Transform</td>
<td>RFC1828</td>
</tr>
<tr>
<td>AH Key(s)</td>
<td>a 128 bit MD5 Key</td>
</tr>
<tr>
<td>AH Mode</td>
<td>Entire Datagram</td>
</tr>
<tr>
<td>ESP Algorithm</td>
<td>DES</td>
</tr>
<tr>
<td>ESP Algorithm Mode</td>
<td>CBC</td>
</tr>
<tr>
<td>ESP Transform</td>
<td>RFC1829</td>
</tr>
<tr>
<td>ESP Key(s)</td>
<td>a 56 bit DES key</td>
</tr>
<tr>
<td>ESP Mode</td>
<td>Transport</td>
</tr>
<tr>
<td>ESP Synch/Init. Vector Size</td>
<td>64</td>
</tr>
<tr>
<td>Lifetime</td>
<td>an absolute time in Unix time format</td>
</tr>
</tbody>
</table>
Security Policy Record

<table>
<thead>
<tr>
<th>Security Parameter</th>
<th>Example Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPI (Security Parameter Index)</td>
<td>2916</td>
</tr>
<tr>
<td>IP Destination Address</td>
<td>128 bit IPv6 address value</td>
</tr>
<tr>
<td>IP Source Address</td>
<td>128 bit IPv6 address value</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>TCP/UDP Destination Port</td>
<td>23</td>
</tr>
<tr>
<td>TCP/UDP Source Port</td>
<td>1234</td>
</tr>
<tr>
<td>UserID</td>
<td>Unix UID or other credentials</td>
</tr>
</tbody>
</table>

AH format

### Inbound datagram

<table>
<thead>
<tr>
<th>IPv6 Header</th>
<th>Hop-by-Hop/Routing</th>
<th>Others</th>
<th>Upper Protocol (e.g. TCP, UDP)</th>
</tr>
</thead>
</table>

### AH calculation

<table>
<thead>
<tr>
<th>IPv6 Header</th>
<th>Hop-by-Hop/Routing</th>
<th>Auth Header</th>
<th>Others</th>
<th>Upper Protocol (e.g. TCP, UDP)</th>
</tr>
</thead>
</table>

### AH Syntax

- **Next Header**: length of next payload after Authentication payload
- **Length**: length of authentication data in 32 bit word
- **RESERVED**: 16 bit reserved field
- **Security Parameters Index**: 32 bit SPI: SA of this datagram
- **Authentication Data (variable number of 32-bit words)**: variable length depending on specification of auth. transform
ESP format

<table>
<thead>
<tr>
<th>Bit 0</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.N.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P.D.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conf.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conf.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SPI (32bit): Identifies SA
S.N. (32 bit) : decreasing counter values
P.D. (var.) : transport-level segment (transport m.) or IP packet (tunnel m.)
P. : for encryption of CBC mode

Algorithms

- Confidentiality and authentication
  - 3DES
  - RC5
  - IDEA
  - CAST
  - Blowfish
- MIC (Message Integrity Check)
  - HMAC-MD5-96
  - HMAC-SHA-1-96
**Modes(I)**

- **Transport Mode**
  - protection for upper-layer protocol like TCP, UDP or ICMP packet
  - end-to-end btw 2 hosts (e.g. C/S, or 2 W/S)

- **Tunnel Mode**
  - protect entire IP packet
  - host-to-subnet or subnet-to-subnet

**Modes(II)**

**AH Transformation**

1. **(1) transport mode**
   - IP Header → TCP/UDP Header → Upper Layer Payload
   - IP Header → AH Header → TCP/UDP Header → Upper Layer Payload
   - Authenticated

2. **(2) tunnel mode**
   - IP Header → AH Header → IP Header → TCP/UDP Header → Upper Layer Payload
   - Authenticated
**Modes(III)**

ESP transformation

1. **Transport mode**
   - IP Header
   - ESP Header
   - TCP/UDP Header
   - Upper Layer Payload
   - ESP Trailer
   - ESP Auth

2. **Tunnel mode**
   - IP Header
   - ESP Header
   - IP Header
   - TCP/UDP Header
   - Upper Layer Payload
   - ESP Trailer
   - ESP Auth

(c) Kwangjo Kim

**Modes(IV)**

<table>
<thead>
<tr>
<th></th>
<th>Transport Mode SA</th>
<th>Tunnel Mode SA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AH</strong></td>
<td>Authenticates IP payload and selected portions of IP header and IPv6 extension headers.</td>
<td>Authenticate entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer.</td>
</tr>
<tr>
<td><strong>ESP</strong></td>
<td>Encrypts IP payload and any IPv6 extension headers following the ESP header.</td>
<td>IPv6 extension headers. Encrypts inner IP packets</td>
</tr>
</tbody>
</table>

(c) Kwangjo Kim
IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection for replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality

<table>
<thead>
<tr>
<th></th>
<th>AH</th>
<th>ESP (e. only)</th>
<th>ESP (e. + a.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Connectionless Integrity</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data origin authentication</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rejection of replayed packets</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Confidentiality</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Limited Traffic flow confidentiality</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
IP Sec benefits

- Implemented in firewall/router, provides strong security
- Traffic can’t bypass firewall with IPsec
- Below transport layer (TCP, UDP) and transparent to applications
- Transparent to end users
- Provide security for individual users if needed.

Limitations

- Don’t provide traffic analysis
- Don’t provide non-repudiation
- Don’t provide denial-of-service attack
key/SA management

- active research, not standard
- manual keying
- proposals (SKIP, ISAKMP, Photuris)
  - SKIP (Simple Key Interchange Protocol)
    - light-weight
    - in-band
    - Diffie-Hellman (signed public keys)
  - ISAKMP (Internet Security Association and Key Management Protocol)
    - out-of band, daemon
    - negotiate (Oakley)
    - Diffie-Hellman, public keys

Group key parameter by Oakley

- Modular exp. (a=2) with p
  - 768bit
  - 1024bit
- Elliptic curves over
  - $2^{155}$
  - $2^{185}$
**Features of Oakley**

- employ mechanism known as cookies* to thwart clogging attack
- enable 2 parties to negotiate a group
- use nonces to ensure against replay attack
- enable to exchange DH public key values
- authenticate DH exchange to thwart man-in-the-middle attack

*cookie*: low level ID carrying in each packet to drive classification or electronic tags placed on your computer by web site.

---

**Example of Oakley(I)**

\[
\begin{align*}
I \rightarrow R : & \text{ CKY}_I, \text{ OK_KEYX}, \text{ GRP}, g^I, \text{ EHAO}, N_I, I_D, R_D, N_R, S_{SK}_I[I_D || I_R || N_I || GRP || g^I || \text{EHAO}] \\
R \rightarrow I : & \text{ CKY}_R, \text{ CKY}_I, \text{ OK_KEYX}, \text{ GRP}, g^R, \text{ EHAS}, N_I, I_D, R_D, N_R, S_{SK}_R[I_R || I_D || N_R || GRP || g^R || g^I || \text{EHAS}] \\
I \rightarrow R : & \text{ CKY}_I, \text{ CKY}_R, \text{ OK_KEYX}, \text{ GRP}, g^I, \text{ EHAS}, N_I, I_D, R_D, N_R, S_{SK}_I[I_D || I_R || N_I || GRP || g^I || \text{EHAS}] \\
I : & \text{ Initiator, } R: \text{ Responder} \\
\text{CKY}_I, \text{ CKY}_R : & \text{ Initiator, responder cookies, OK_KEYX : Key exchange message type} \\
\text{GRP} : & \text{ Name of DH group for this exchange} \\
\text{EHAO, EHAS} : & \text{ Encryption, hash, authentication functions, offered and selected} \\
NIDP : & \text{ Indicates encryption is not used for remainder of this message} \\
I_D, R_D : & \text{ Identifier for initiator, responder} \\
N_I, N_R : & \text{ Random nonce supplied by initiator, responder for this exchange} \\
S_{SK}(X), S_{SK}(X) : & \text{ Indicates the signature over } X \text{ using private key (signing key) of initiator, responder}
\end{align*}
\]
Example of Oakley(II)

- (step 1) transmit cookie, group to be used, I’s public key and others
- (step 2) R verifies signature using I’s public key and echoing adding signature
- (step 3) verifies R’s signature, check nonce against replay attack
- (step 4) complete the exchange, I send message back to R to verify that I have received R’s public key
SSL(II)

- **Handshake Protocol**
  - (Step 1) Selection of algorithm, distribution of master key, authentication of server
  - (Step 2) Authentication of client if necessary

- **Record Protocol**
  - If no use session ID, no need authentication of client
  - If use of Session ID, no need authentication of client
  - If use of Session ID, need authentication of client

---

SSL(III)

- **Confidentiality** : Fortezza, IDEA, RC2-40, RC4-40, DES, 3DES
- **Anti-traffic attack**
- **Message Authentication** : HMAC-MD5
## Comparison of IPv6 and SSL

<table>
<thead>
<tr>
<th>Classification</th>
<th>IPv6</th>
<th>SSL</th>
</tr>
</thead>
</table>
| Layer          | • Network layer  
• Applicable to transport layer                                   | • Transport layer  
• Limited privacy and authentication services                         |
| Style of usage | • host-to-host  
• host-to-subnet  
• subnet-to-subnet                                                   | host-to-host                                                     |
| Key exchange   | • IKMP  
• Hard to define exchange mechanism for large network                | • Server key exchange message  
• Client key exchange message  
• secure WWW-based                                                        |
| Privacy        | • No limitation  
• DES, 3DES, IDEA, Blowfish, RC5                                     | • No limitation  
• Fortezza, IDEA, RC2, RC4, DES, 3DES                                 |
| Authentication  | • Keyed MD5, SHA-1  
• packet authentication on network layer  
• origin and destination address                                        | • MD5  
• Packet authentication on transport layer                               |
| Integrity      | • Tunnel mode ESP  
• Transparent mode ESP                                                 | • Protocol (HTTP, NNTP, SMTP) dependent                              |

## Security Facilities in TCP/IP

<table>
<thead>
<tr>
<th>HTTP</th>
<th>FTP</th>
<th>SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HTTP</th>
<th>FTP</th>
<th>SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>TLS</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>S/MIME</th>
<th>PGP</th>
<th>SET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos</td>
<td>SMTP</td>
<td>HTTP</td>
</tr>
<tr>
<td>UDP</td>
<td>TCP</td>
<td>IP</td>
</tr>
</tbody>
</table>

(a) Network level  
(a) transport level  
(c) application level