IPsec ESP Attacks

CS 470
Introduction to Applied Cryptography
Ali Aydin Selçuk

Attacks on ESP Encryption


Attack model:
- Host-pair keying
- ESP encryption without authentication
- CBC mode of encryption

TCP Header

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

UDP Header

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
Due to CBC, only first block of the pasted packet will be corrupted. (Can be avoided if IV is copied as well)

Padding may be added to re-injected packet if needed to make lengths match

If IPv6 in use, UDP checksum mandatory. 2^16 trials are needed on average to pass validation.

If \( L_A, L_B \) are using UDP, attack is easier:
- Wait till session ends
- Allocate \( L_A \)'s UDP port to \( X_B \)
- Replay all packets

|                    Options                    |    Padding    |
|                    Destination Address                        |
|                       Source Address                          |

|  Time to Live |       Protocol   |         Header Checksum       |
|         Identification        |Flags|      Fragment Offset    |

Reading Encrypted Data

\( L_A, L_B \): Legitimate user accounts on hosts A, B

\( X_A, X_B \): Attacker’s accounts on A and B

Monitored data:

\[
L_A \rightarrow L_B: \begin{array}{c} IP \ \ ESP_x \ \ TCP \ \ \ \ \ \ \ \ secret \end{array}
\]

\[
X_A \rightarrow X_B: \begin{array}{c} IP \ \ ESP_x \ \ UDP \ \ \ \ any \end{array}
\]

Re-injected data:

\[
X_A \rightarrow X_B: \begin{array}{c} IP \ \ ESP_x \ \ UDP \ \ TCP \ \ secret \end{array}
\]

Session Hijacking

Monitored data:

\[
L_A \rightarrow L_B: \begin{array}{c} IP \ \ ESP_x \ \ TCP \ \ \ \ \ \ data \end{array}
\]

\[
X_A \rightarrow X_B: \begin{array}{c} IP \ \ ESP_x \ \ UDP \ \ CBC \ \ pad \ \ m-rf \ / \end{array}
\]

Re-injected data:

\[
L_A \rightarrow L_B: \begin{array}{c} IP \ \ ESP_x \ \ TCP \ \ CBC \ \ pad \ \ m-rf / \ \ ckfix \end{array}
\]
Session Hijacking (cont’d)

- Due to CBC, the first pasted block will be corrupted; the “CBC pad”.
- Some extra bytes may be needed to restore to a known state (e.g., shell prompt)
- “ckfix” is to fix the checksum; takes on average $2^{16}$ trials.
- Attack can work without having logins $X_A$, $X_B$. (e.g., with SMTP-level source routing)

IV Attacks

- IV is sent in the payload; subject to modification
- By modifying IV, the first plaintext block can be modified in controllable manner:
  $$P_1 = D_K(C_1) \oplus IV$$
- Attacks have further impact: First block includes the upper-layer header!!!
- Checksums, if present, may be fixed by modifying insensitive fields in the first block

IV Attacks on TCP

- Fields in first 64 bits: Source Port, Destination Port, Seq.No.
  Fields in bits 65-128: Window Size, Ack.No., Offset, flags
- Attacks on Destination Port: Decrypted packets delivered to $X_B$.
- Other attacks: Seq.No. (reordering), Window Size (flooding/stalling)
- Checksum fixing: by “reserved” or Ack.No.

IV Attacks on UDP

- Fields in first 64 bits: Source Port, Destination Port, Length, Checksum
  Bits 65-128: Data payload
- Dest. Port: Decrypted packets delivered to $X_B$.
- Length: Packets can be truncated.
- Checksum can be fixed directly.
- With a 128-bit cipher, the first 64 bits of the payload can be modified.
Conclusion

- Encryption without integrity protection can be all but useless.
- Authentication is better made mandatory in IPsec (and other security protocols).
- Moral of the story: It is safe to always use authentication/integrity protection, even if only confidentiality is the purpose. (Besides, the extra cost of MAC is marginal.)