Visualization for CPAL-ES Encoding

John Marshall

17 March 2003

Attack on SRP

S A I B T

Malicious Intermediate Node

17 March 2003
Attack on SRP

\[ S \rightarrow A \rightarrow I \rightarrow B \rightarrow T \]

- Source: S
- Target: T
- Q_{req}
- Q_{ip}
- MAC
- S, A

17 March 2003
Attack on SRP

$S \rightarrow A \rightarrow I \rightarrow B \rightarrow T$

$I$ does not append IP-address

<table>
<thead>
<tr>
<th>Source: S</th>
<th>Target: T</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Q_{req}$</td>
<td></td>
</tr>
<tr>
<td>$Q_{ID}$</td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td></td>
</tr>
<tr>
<td>$S,A$</td>
<td></td>
</tr>
</tbody>
</table>

17 March 2003
Attack on SRP

- **target** validates $Q_{seq}$ and $MAC$
- accepts route request packet
- issues route reply packet
Attack on SRP

Again, I does not append IP-address
Attack on SRP

- Check $Q_{seq}$ and $Q_{ID}$ for legitimacy
- Compute and compare $MAC$ using reverse of accumulated route
- Route reply packet accepted
Solution Detecting the Attack

- Detects and mitigates node misbehavior
- *bloodhound*

*bloodhound*

- Node should never receive packet identical to one it sent
- *bloodhound* listens in to overhear identical packets
I does not append IP-address, so I broadcasts **identical** packet.