Transport-Level Denial-of-Service

- Recall TCP’s 3-way connection establishment handshake
  - Goal: agree on initial sequence numbers
  - Starting sequence numbers are based on clock random
  
Client (initiator)

SYN, SeqNum = x

SYN and ACK, SeqNum = y, Ack = x + 1

ACK, Ack = y + 1

Server

Server creates state associated with connection here
to prevent attacker from guessing them to establish connections using spoofed source addresses
Flooding Defense: SYN Cookies

- Server: when SYN arrives, **encode** connection state entirely within SYN-ACK’s sequence # y
  
  \[ y = \text{SHA-1}(\text{client\_addr}, \text{client\_port}, \text{ISN} \ x, \text{server\_secret}) \]

- When ACK of SYN-ACK arrives, server only creates state *if* seq # y in it agrees with hash

![Diagram showing SYN, SYN and ACK, and ACK packets with sequence numbers and acknowledgments. The server only creates state if the sequence number and hash match.]
SYN Cookies: Discussion

• Illustrates general strategy: rather than holding state, encode it so that it is returned when needed.

• For SYN cookies, attacker must complete 3-way handshake in order to burden the server.
  – Can’t use spoofed source addresses.

• Note #1: strategy requires that you have enough bits to encode all the state.
  – This is just barely the case for SYN cookies:
    o 24 bit hash + 5-bit timestamp + 3 bits to remember MSS
    o Can’t remember any TCP options …

• Note #2: if it’s expensive to generate or check the cookie, then it’s not a win.
Click 3 pictures of kittens to submit

The KittenAuth system. Source: ThePCSpy.com.
<table>
<thead>
<tr>
<th>Служба</th>
<th>Кол-во акков</th>
<th>Цена за 1К акков</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail.ru</td>
<td>3046</td>
<td>до 10К: $10</td>
</tr>
<tr>
<td>Pochta.ru (+ FTP)</td>
<td>35</td>
<td>до 10К: $8</td>
</tr>
<tr>
<td>Yandex.ru (+ Narod.ru)</td>
<td>0</td>
<td>до 10К: $9</td>
</tr>
<tr>
<td>Gmail.com</td>
<td>134670</td>
<td>до 10К: $6</td>
</tr>
<tr>
<td>Hotmail.com</td>
<td>42893</td>
<td>до 10К: $7</td>
</tr>
<tr>
<td>Yahoo.com</td>
<td>10847</td>
<td>до 10К: $9</td>
</tr>
</tbody>
</table>

КУПИТЬ: 100K Gmail.com OK