Many connections have holes, but little buffer required.
Adversary can fill the entire buffer with just a single connection!  
**Policy 1:** Restrict per-connection buffer to threshold (say 20KB)
- Adversary can create *multiple* connections to exhaust the buffer!

- **Policy 2:** Do not allow a single host to create two connections with holes

<table>
<thead>
<tr>
<th></th>
<th>Univ$_{sub}$</th>
<th>Univ$_{19}$</th>
<th>Lab$_{lo}$</th>
<th>Lab$_2$</th>
<th>Super</th>
<th>T3</th>
<th>Munich</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraction of holes that overlap hole on another connection of same <em>external</em> host</td>
<td>0.5%</td>
<td>0.02%</td>
<td>0.06%</td>
<td>0.06%</td>
<td>0%</td>
<td>0.46%</td>
<td>0.02%</td>
</tr>
</tbody>
</table>
• Adversary attacks from distributed hosts! (zombies)
  – No connection can be isolated as adversary’s… all of them look good

• **Policy 3:** Upon buffer exhaustion …
  – … Evict one buffer page *randomly*
    and reallocate it to new packet
  – **Kill** the connection of the evicted page (mod details)

• If the buffer is **large**, then *most evicted connections belong to the adversary*
  – They fight an uphill battle!
• Suppose total 512 MB, 2KB page, 25KB/conn

Avg. Legitimate Buffer = 30 KB
On another trace, ratio is only 1.2:1
On still another, *this* ratio flips to 1:2!

And *this* is almost as bad as Snort-[FV01]