## 1 day of “crud” seen at ICSI (155K times)

<table>
<thead>
<tr>
<th>Issue Description</th>
<th>Related Problem</th>
<th>Issue Description</th>
<th>Related Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>active-connection-reuse</td>
<td>DNS-label-len-gt-pkt</td>
<td>HTTP-chunked-multipart</td>
<td>possible-split-routing</td>
</tr>
<tr>
<td>bad-Ident-reply</td>
<td>DNS-label-too-long</td>
<td>HTTP-version-mismatch</td>
<td>SYN-after-close</td>
</tr>
<tr>
<td>bad-RPC</td>
<td>DNS-RR-length-mismatch</td>
<td>illegal-%-at-end-of-URI</td>
<td>SYN-after-reset</td>
</tr>
<tr>
<td>bad-SYN-ack</td>
<td>DNS-RR-unknown-type</td>
<td>inappropriate-FIN</td>
<td>SYN-inside-connection</td>
</tr>
<tr>
<td>bad-TCP-header-len</td>
<td>DNS-truncated-answer</td>
<td>IRC-invalid-line</td>
<td>SYN-seq-jump</td>
</tr>
<tr>
<td>base64-illegal-encoding</td>
<td>DNS-len-lt-hdr-len</td>
<td>line-terminated-with-single-CR</td>
<td>truncated-NTP</td>
</tr>
<tr>
<td>connection-originator-SYN-ack</td>
<td>DNS-truncated-RR-rdlength</td>
<td>malformed-SSH-identification</td>
<td>unescaped-%-in-URI</td>
</tr>
<tr>
<td>data-after-reset</td>
<td>double-%-in-URI</td>
<td>no-login-prompt</td>
<td>unescaped-special-URI-char</td>
</tr>
<tr>
<td>data-before-established</td>
<td>excess-RPC</td>
<td>NUL-in-line</td>
<td>unmatched-HTTP-reply</td>
</tr>
<tr>
<td>too-many-DNS-queries</td>
<td>FIN-advanced-last-seq</td>
<td>POP3-server-sending-client-commands</td>
<td>window-recision</td>
</tr>
<tr>
<td>DNS-label-forward-compress-offset</td>
<td>fragment-with-DF</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Ohio State Says Hackers Breached Data on 760,000

By TAMAR LEWIN

Ohio State University is notifying about 760,000 people whose personal information was stored in the university’s computer server that a data breach could put them at risk for identity theft.

The university, located in Columbus, began sending letters on Wednesday to current and former faculty and staff members, students and applicants, telling them that hackers had broken into the server that stored their names, Social Security numbers, dates of birth and addresses.

The university said that although there was no evidence that the information had been used for identity theft, it was nonetheless offering a year of free credit protection to everyone whose data was on the server.

“We regret that this has occurred and are exercising an abundance of caution in choosing to notify those affected,” Joseph A. Alutto, the university provost, said in a news release.
- 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 (= ?)
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
Cisco IPS Architecture
Intelligent Detection and Precision Response

- Cisco Threat Intelligence Services
- Signature Updates
- Engine Updates
- Context Data
- Network Context Information

**Normalizer Module**
- Layer 3–7 normalization of traffic to remove attempts to hide an attack

**Modular Inspection Engines**
- Vulnerability
- Exploit
- Behavioral anomaly
- Protocol anomaly
- Universal engines

**On-Box Correlation Engine**
- Meta event generator for event correlation

**Risk-Based Policy Control**
- Calibrated “risk rating” computed for each event
- Event action policy based on risk levels
- Filters for known benign triggers

**Virtual Sensor Selection**
- Traffic directed to appropriate virtual sensor by interface or VLAN

**Forensics Capture**
- Before attack
- During attack
- After attack

**Mitigation and Alarm**
- “Threat rating” of event indicates level of residual risk