Update Management for Control Systems

Kevin Sullivan
Sr. Security Strategist
Microsoft
# Common Security Challenges

<table>
<thead>
<tr>
<th></th>
<th>Networked OS 1999</th>
<th>Control Systems 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubiquitous connectivity</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Use of commodity software</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Fast growing deployed base</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Focus of attackers</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Media coverage</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Application Layer Attacks

Vulnerabilities:
Major Operating Systems versus Application Layer

~90% are remotely exploitable
~60% are in web applications

Source: Microsoft Security Intelligence Report 2007

Critical Infrastructure Protection
**Update Philosophy**

- Plan for updates to the entire infrastructure stack:
  - Network
  - Operating System
  - Database
  - Application

- Architect your systems for updates:
  - Redundancy
  - Virtualization

Updates should be manageable and predictable.
Critical Infrastructure Protection

Update Mechanics

1. Assess
2. Identify
3. Evaluate & Plan
4. Deploy

Security Response
Advance Notification
Security Update Validation Program
Bulletin Release
Responsible Disclosure
Secure Development

Microsoft
Critical Infrastructure Protection
Update Innovations

- **Exploitability Index**
  - 1 = Consistent Exploit Code Likely
  - 2 = Inconsistent Exploit Code Likely
  - 3 = Functioning Exploit Code Unlikely

- **Windows Server 2008 - Server Core**
  - Reduced attack surface
  - Infrastructure roles only
  - Limited GUI

Customer Goal:
- Prioritize Updates
- Fewer Updates