TRUSTWAVE PRESENTS
SPIDERLABS
10¢

SpiderLabs
Worst of the Best of
the Best

Kevin Stadmeyer
Garrett Held
Worst of the Best of the Best
Agenda

• Motives
• Goals
• Awards Overview
• Example of Serious Flaws in the System
• Lies, Damned Lies, and Awards
• What Awards Really Mean
• Better Ways
Motives and Goals
Motives

• Yes, it’s obvious this is about marketing

• Any product will probably contain vulnerabilities

• Awarding dangerous security practices is much worse

• Public records give an incomplete picture
Goals

- Highlight a product that’s an example of this problem, and why vulnerability statistics do not accurately reflect product security

- Attempt to use publicly available statistics that come up with a model that does work
## Awards Overview

<table>
<thead>
<tr>
<th>Name</th>
<th>Nomination</th>
<th>Choosing A Winner</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC Magazine</td>
<td>Unknown</td>
<td>Popular vote</td>
</tr>
<tr>
<td>Techworld.com</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>Information Security Magazine</td>
<td>Editor Chosen</td>
<td>Popular vote</td>
</tr>
</tbody>
</table>
Product X and Vendor Y

Why public statistics aren’t a complete picture
Product X

It’s a Secret shhh! Hi Lawyers!

• Provides a web service/interface on a network appliance
Product X: Findings

- A manual application security review was performed on the device without access to the source code.
- The following vulnerabilities were found:
  - Eight high-risk issues
  - Six medium-risk issues
  - Nine low-risk issues
Product X: Serious Findings

This is a subset of the High and Medium risk issues found:

- **Systemic Cross-Site Scripting**
  - Almost any variable was vulnerable, including variables stored by the application (Persistent Cross-Site Scripting)

- **Privilege Escalation**
  - Browser-supplied user ID while in a valid session could be changed, using an easily predictable method, for privilege escalation.

- **Custom Web Server**
  - Re-inventing the wheel and introducing bugs such as arbitrary system file access, including the password file.
Product X: Serious Findings (Cont.)

- **Session Hijacking**
  - Poor implementation resulted in users able to steal sessions of users logging in around the same time of day.

- **Custom, Weak Session ID Algorithm**
  - Without getting into details that would give it away:
Product X: Reaction

So What?
Vendor Y

- Major software vendor
- Two independently discovered vulnerabilities, medium or higher
- One occurs on their own servers (still)

Vendor Response: *Crickets*
Lies, Statistics, and Awards
What Awards Really Mean

Problems with gathering statistics

- FUD
- Sources
- Lack of History
Sample Statistics

Methodology

• Three Categories
• Two Awards
• Competitors
• Variety of Sources
# Awards: Anti-Malware

<table>
<thead>
<tr>
<th>Award</th>
<th>Product</th>
<th>Highs</th>
<th>Mediums</th>
<th>Lows</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC Magazine</td>
<td>Symantec End-Point Protection</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Info Security Products Guide</td>
<td>CoreTrace - Bouncer 4.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Nod32 Anti-Virus</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Proventia Network Scanner</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Radware Defense Pro</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Vipre</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Websense</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
## Awards: Endpoint Security

<table>
<thead>
<tr>
<th>Award</th>
<th>Product</th>
<th>Highs</th>
<th>Mediums</th>
<th>Lows</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC Magazine</td>
<td>McAfee Security Center</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Info Security Products Guide</td>
<td>Parity v4.0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Checkpoint for Endpoint Security</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Cisco NAC</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>F5 Firepass Remote Access Solutions</td>
<td>5</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Protection</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Awards: IPSec/SSL VPN

<table>
<thead>
<tr>
<th>Award</th>
<th>Product</th>
<th>Highs</th>
<th>Mediums</th>
<th>Lows</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC Magazine</td>
<td>Cisco ASA 5500</td>
<td>3</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Info Security Products Guide</td>
<td>NCP Secure Enterprise Solution</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Checkpoint Connectra</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Citrix Access Gateway</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>F5 Firepass Remote Access Solutions</td>
<td>5</td>
<td>2</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Stonesoft Stonegate VPN</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
What Awards Really Mean
What Awards Really Mean

Awards Are Marketing

- Unclear
- Too Many
- Press Releases
- Pointless
Better Ways
Better Ways

Credible Award Requirements

- Open Process
- Established Products
- Audit Product Patch Process
- Relevant Criteria
Better Ways

Alternative Evaluation Criteria

- References
- History of Security
- Talk to Developers
Questions?