2011: Web Application Security Metrics Landscape

Actionable Software Security Metrics that Clarify instead of Confuse

Arian Evans
VP Operations, R&D
WhiteHat Security

SANS AppSec 2011 Summit
3.8.2011
The Speaker is

Arian Evans, VP, Operations, R&D, WhiteHat Security

- Runs the WhiteHat TRC (Threat Research Center) assessing 3100+ websites weekly using the Whitehat Sentinel Website Security platform.

- 12 years in ecommerce and enterprise Web application security.

- Incident response on organized crime hacking for the CIS, NIST, FBI, Secret Service, and commercial organizations.

- Researches and discloses new attack techniques and vulnerabilities in Web application software.

- Arian is a frequent speaker at industry conferences including Black Hat, OWASP, RSA, WASC, SANS, and international software developer conferences & events.

- Contributing author of "Hacking Exposed: Web Applications."
WhiteHat Security Overview

400+ enterprise customers
  • Start-ups to Fortune 500

Flagship offering “WhiteHat Sentinel Service”
  • 3100+ websites assessed weekly

Recognized leader in website security
  • Quoted thousands of times by the mainstream press
285 MILLION RECORDS WERE COMPROMISED IN 2008.

A study conducted by the Verizon Business RISK Team

2009 Data Breach Investigations Report
### Attack Pathways

**Figure 22.** Attack pathways by percent of breaches within Hacking and percent of records

<table>
<thead>
<tr>
<th>Attack Pathway</th>
<th>Breaches</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web application</td>
<td>54%</td>
<td>92%</td>
</tr>
<tr>
<td>Remote access and control services/software</td>
<td>34%</td>
<td>2%</td>
</tr>
<tr>
<td>Backdoor or control channel</td>
<td>23%</td>
<td>5%</td>
</tr>
<tr>
<td>Network file/resource sharing services</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>Physical access or connection</td>
<td>2%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Wireless network</td>
<td>2%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Unknown</td>
<td>7%</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>

**54% of breaches occur in 92% of records**

Web applications now reign supreme in both the number of breaches and the amount of data compromised through this vector. Both Verizon and USSS cases show the same trend...

**Source:** 2010 Data Breach Investigations Report, page 30
KPI: Number of *serious new vulnerabilities introduced per website annually:

- Overall: 230
- Banking: 30
- Education: 80
- Financial Services: 266
- Healthcare: 33
- Insurance: 80
- IT: 111
- Manufacturing: 35
- Retail: 404
- Social Networking: 71
- Telecommunications: 215
Avg. # of Serious* Vulnerabilities per website aggregated*

(Sorted by Industry)

* Serious Vulnerabilities: Those vulnerabilities with a **HIGH**, **CRITICAL**, or **URGENT** severity as defined by PCI-DSS naming conventions. Exploitation could lead to breach or data loss.

* Aggregated by location (form/cgi/path) by class, which results in a 20-to-1 collapse vs. industry standard practice of reporting individual attack-vectors per-parameter
Time-to-Fix (Days)

- Cross-Site Scripting: 67 days
- Information Leakage: 78 days
- Content Spoofing: 87 days
- Insufficient Authorization: 57 days
- SQL Injection: 62 days
- Pred. Res. Loc.: 30 days
- Cross-Site Request Forgery: 93 days
- Session Fixation: 106 days
- HTTP Response Splitting: 75 days
- Abuse of Functionality: 54 days
Software Security Challenges..

Application Security Standards…
- Are vague or too broad (OWASP, BITS)
- Are too detailed & myopic (CWE – 828 weaknesses)
- Lack pragmatic guidance on metrics
- Ignore current Threat Landscape (WHID)

AppSec Program Metrics
- Confuse Risk with */KLOC
- Disenfranchise developers
- Fail to clearly communicate:
  - Impact and Loss to Business
  - Savings (remediation, lost opportunity cost)
  - Positive progress over time (ROI)
You are not alone with your software security challenges….

Common strategic goals for metrics:
• Do not get hacked.
• Do not get into the WSJ (in hacked-company articles).
• Keep my job.
• Protect my organizations assets/profits/reputation.
• Show the business ROI on securing software.
• Hackers will find my applications, sooner or later. *I want to be ready for them.*
Metrics Challenge

- Web software constantly growing and changing
- Need ongoing metrics to reflect rapid rate of change
- Business wants Risk (Impact | Loss) - not Avg Defect rates
- Normalize high volume of defects from Appsec Tools into Risk
- Enable Disenfranchised Developer
- Am I “getting better” – over time, new code, etc.
- Am I “less exploitable” than yesterday?
- Am I saving the business money?
Six Key AppSec Metrics

• Discoverability (Exposure)
• Exploitability (Threat)
• Impact Severity (Risk)
• Vulnerability~Input (Pulse)
• Window of Annual Exposure Rate (Frequency)
• Reduce Remediation Cost per Defect (Savings)
Example Discoverability Classes:

**Fully Targeted (APT)**
- Customize their own tools
- Focused on business logic
- Profit or goal driven ($$$)

**Directed Opportunistic**
- Commercial and Open Source Tools
- Authentication
- Scans Multi-step processes (forms)

**Random Opportunistic**
- Fully automated scripts
- Unauthenticated scans
- Targets chosen indiscriminately

It’s NOT about WHAT vulnerabilities you look for, but HOW and WHY that’s important.
KPI: Windows of Exposure

Number of days [in a year] a website is exposed to at least one serious* reported vulnerability.

Most websites were exposed to at least one serious* vulnerability every single day of 2010, or nearly so (9-12 months of the year). Only 16% of websites were vulnerable less than 30 days of the year overall.
## 2010: Windows of Exposure Summarized

<table>
<thead>
<tr>
<th>Industry</th>
<th>Number of Vulns</th>
<th>Std. Dev</th>
<th>Remediation Rate</th>
<th>Std. Dev</th>
<th>Window of Exposure (Days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>230</td>
<td>1652</td>
<td>53%</td>
<td>40%</td>
<td>233</td>
</tr>
<tr>
<td>Banking</td>
<td>30</td>
<td>54</td>
<td>71%</td>
<td>41%</td>
<td>74</td>
</tr>
<tr>
<td>Education</td>
<td>80</td>
<td>144</td>
<td>40%</td>
<td>36%</td>
<td>164</td>
</tr>
<tr>
<td>Financial Services</td>
<td>266</td>
<td>1935</td>
<td>41%</td>
<td>40%</td>
<td>184</td>
</tr>
<tr>
<td>Healthcare</td>
<td>33</td>
<td>87</td>
<td>48%</td>
<td>40%</td>
<td>133</td>
</tr>
<tr>
<td>Insurance</td>
<td>80</td>
<td>204</td>
<td>46%</td>
<td>37%</td>
<td>236</td>
</tr>
<tr>
<td>IT</td>
<td>111</td>
<td>313</td>
<td>50%</td>
<td>40%</td>
<td>221</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>35</td>
<td>111</td>
<td>47%</td>
<td>40%</td>
<td>123</td>
</tr>
<tr>
<td>Retail</td>
<td>404</td>
<td>2275</td>
<td>66%</td>
<td>36%</td>
<td>328</td>
</tr>
<tr>
<td>Social Networking</td>
<td>71</td>
<td>116</td>
<td>47%</td>
<td>34%</td>
<td>159</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>215</td>
<td>437</td>
<td>63%</td>
<td>40%</td>
<td>260</td>
</tr>
</tbody>
</table>
Six Key AppSec Metrics

• Discoverability (Exposure)
• Exploitability (Threat)
• Impact Severity (Risk)
• Vulnerability~Input (Pulse)
• Window of Annual Exposure Rate (Frequency)
• Reduce Remediation Cost per Defect (Savings)
Website Security By the Numbers

To learn more about the state of website security and how to enhance your organization’s software security initiatives – please read the WhiteHat Security the WhiteHat Security Website Security Statistics Reports:

Measuring Website Security: Windows of Exposure

Industry Benchmarks
http://www.whitehatsec.com/home/assets/WPstats_fall10_10th.pdf

Which Web programming languages are most secure?
http://www.whitehatsec.com/home/assets/WPstats_spring10_9th.pdf
Time for Questions

Arian Evans
VP Operations, R&D
arian@whitehatsec.com
www.whitehatsec.com

SANS AppSec 2011 Summit
3.8.2011
Remediation Rate

*(Percentage of Websites within Remediation Rate Ranges Sorted by Industry)*

<table>
<thead>
<tr>
<th>Industry</th>
<th>0 - 20%</th>
<th>21% - 40%</th>
<th>41% - 60%</th>
<th>61% - 80%</th>
<th>81% - 100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>28</td>
<td>10</td>
<td>10</td>
<td>13</td>
<td>39</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>22</td>
<td>6</td>
<td>11</td>
<td>6</td>
<td>56</td>
</tr>
<tr>
<td>Social Networking</td>
<td>24</td>
<td>12</td>
<td>10</td>
<td>18</td>
<td>35</td>
</tr>
<tr>
<td>Retail</td>
<td>24</td>
<td>10</td>
<td>9</td>
<td>16</td>
<td>41</td>
</tr>
<tr>
<td>IT</td>
<td>41</td>
<td>17</td>
<td>9</td>
<td>11</td>
<td>22</td>
</tr>
<tr>
<td>Insurance</td>
<td>43</td>
<td>17</td>
<td>13</td>
<td>3</td>
<td>23</td>
</tr>
<tr>
<td>Healthcare</td>
<td>32</td>
<td>5</td>
<td>10</td>
<td>11</td>
<td>42</td>
</tr>
<tr>
<td>Financial Services</td>
<td>27</td>
<td>11</td>
<td>10</td>
<td>12</td>
<td>38</td>
</tr>
<tr>
<td>Education</td>
<td>31</td>
<td>11</td>
<td>14</td>
<td>14</td>
<td>29</td>
</tr>
<tr>
<td>Banking</td>
<td>21</td>
<td>8</td>
<td>8</td>
<td>2</td>
<td>62</td>
</tr>
</tbody>
</table>