Data Mining a Mountain of Zero Day Vulnerabilities
Data Mining a Mountain of Zero Day Vulnerabilities

Joe Brady
Senior Solutions Architect
March 29, 2013
The Data Set

- Applications from over 300 commercial and US government customers
- Scanned 9,910 applications over 18 months
- Ranged in size from 100KB to 6GB
- Included both pre-release and production software
- Internally built, outsourced, open source, and commercial ISV code
Application Metadata
- Industry vertical
- Supplier (internal, third-party, open source, etc.)
- Application type
- Business criticality
- Language
- Platform

Scan Data
- Scan number
- Scan date
- Lines of code

Enterprise Metrics
- Flaw counts
- Flaw percentages
- Application count
- Risk-adjusted rating
- First scan acceptance rate
- Time between scans
- Days to remediation
- Scans to remediation
- Team comparisons
- Custom policies
- PCI-DSS ($)
- CWE/SANS Top25 ($)
- OWASP Top Ten ($)

† Pass/Fail only
Caveats

• Customer base is already security-conscious

• Bias toward business critical applications

• Applications are at inconsistent phases in the SDLC

• Not all flaws are necessarily easy to exploit

• Analysis technology is continuously being improved

• All security testing has False Negatives
THE LATENT VULNERABILITIES VS. THE ATTACKS
While other flaws such as XSS account for a higher volume of findings, SQL injection accounts for 20 percent of hacks.

*Source: WHID*
LET’S TAKE A CLOSER LOOK AT THE NUMBERS
Top Vulnerability Categories
(Percent of Applications Affected for Web Applications)

- Cross-site Scripting (XSS): 68%
- Information Leakage: 66%
- CRLF Injection: 54%
- Cryptographic Issues: 53%
- Directory Traversal: 49%
- SQL Injection: 32%
- Time and State: 30%
- Credentials Management: 27%
- API Abuse: 25%
- Encapsulation: 25%
- Insufficient Input Validation: 24%
- Session Fixation: 21%
- Race Conditions: 13%
- Potential Backdoor: 9%
- OS Command Injection: 9%

Indicate categories that are in the OWASP Top 10
Top Vulnerability Categories
(Percentage of Applications Affected for Non-Web Applications)

- Cryptographic Issues: 46%
- Directory Traversal: 34%
- Error Handling: 24%
- Information Leakage: 23%
- Potential Backdoor: 23%
- Time and State: 19%
- Buffer Management Errors: 17%
- OS Command Injection: 15%
- Credentials Management: 15%
- Buffer Overflow: 14%
- CRLF Injection: 13%
- Numeric Errors: 12%
- SQL Injection: 11%
- Untrusted Search Path: 11%
- Dangerous Functions: 10%

Indicate categories that are in the CWE/SANS Top 25
ARE WE MAKING ANY PROGRESS AT ERADICATING CROSS-SITE SCRIPTING OR SQL INJECTION?
Quarterly Trend for XSS

p-value = 0.124: Statistically, the trend is flat.
Quarterly Trend for SQL Injection

*pvalue = 0.048*: Statistically, the trend is down.
WHAT PERCENTAGE OF WEB APPLICATIONS FAIL THE OWASP TOP TEN?

a) 34%
b) 57%
c) 86%
d) 99%
OWASP Top 10 Compliance by Supplier on First Submission
(Web Applications)

<table>
<thead>
<tr>
<th>Supplier Type</th>
<th>Acceptable</th>
<th>Not Acceptable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally Developed</td>
<td>15%</td>
<td>85%</td>
</tr>
<tr>
<td>Commercial</td>
<td>14%</td>
<td>86%</td>
</tr>
<tr>
<td>Open Source</td>
<td>6%</td>
<td>94%</td>
</tr>
<tr>
<td>Overall</td>
<td>14%</td>
<td>86%</td>
</tr>
</tbody>
</table>
CWE/SANS Top 25 Compliance by Supplier on First Submission
(Non-Web Applications)

<table>
<thead>
<tr>
<th>Supplier Type</th>
<th>Acceptable</th>
<th>Not Acceptable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally Developed</td>
<td>48%</td>
<td>52%</td>
</tr>
<tr>
<td>Commercial</td>
<td>38%</td>
<td>62%</td>
</tr>
<tr>
<td>Open Source</td>
<td>26%</td>
<td>74%</td>
</tr>
<tr>
<td>Overall</td>
<td>42%</td>
<td>58%</td>
</tr>
</tbody>
</table>
HOW LONG DOES IT TAKE APPLICATIONS TO ACHIEVE AN ACCEPTABLE RATING?
Development agility and application security are not mutually exclusive! (or are they...)

**Time to Policy Achievement**

<table>
<thead>
<tr>
<th>Source</th>
<th>0-1 Week</th>
<th>2-3 Weeks</th>
<th>3-4 Weeks</th>
<th>4+ Weeks</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally Developed</td>
<td>82%</td>
<td>3%</td>
<td>3%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>Commercial</td>
<td>79%</td>
<td>3%</td>
<td>7%</td>
<td>11%</td>
<td>11%</td>
</tr>
<tr>
<td>Open Source</td>
<td>98%</td>
<td></td>
<td></td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Outsourced*</td>
<td>100%</td>
<td></td>
<td></td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Overall</td>
<td>82%</td>
<td>3%</td>
<td>4%</td>
<td>11%</td>
<td>11%</td>
</tr>
</tbody>
</table>
GREAT, BUT WHAT ABOUT ALL THE OTHER APPS?
Only about half of companies resubmit more than 90\% of their *most critical* applications!
**Refresher: Whisker Plots**

- **Maximum**
- **Upper Quartile**
- **Median**
- **Lower Quartile**
- **Population Size**
- **Minimum**
Veracode Security Quality Score Trend by Quarter

\textit{pvalue} = 0.543: Statistically, the trend is flat.
WHAT HAPPENS WHEN SOFTWARE VENDORS ARE HELD ACCOUNTABLE?
Compliance with Policies on First Submission

- **Enterprise Policy**
  - Compliant: 38%
  - Out of Compliance: 62%

- **CWE/SANS Top 25**
  - Compliant: 30%
  - Out of Compliance: 70%

- **OWASP Top 10**
  - Compliant: 10%
  - Out of Compliance: 90%
Compliance with Enterprise Policy by Application Purpose on First Submission

- Customer Support: 20% Acceptable, 80% Not Acceptable
- Security: 24% Acceptable, 76% Not Acceptable
- Business and IT Operations: 28% Acceptable, 72% Not Acceptable
- Other: 32% Acceptable, 68% Not Acceptable
- Financial: 41% Acceptable, 59% Not Acceptable
- Web Infrastructure: 65% Acceptable, 35% Not Acceptable
<table>
<thead>
<tr>
<th></th>
<th>Enterprises with an Ad-Hoc Approach</th>
<th>Enterprises with a Programmatic Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average number of vendors participating</td>
<td>4</td>
<td>38</td>
</tr>
<tr>
<td>Average number of applications assessed</td>
<td>7</td>
<td>71</td>
</tr>
<tr>
<td>Percent of applications achieving compliance</td>
<td>34%</td>
<td>52%</td>
</tr>
<tr>
<td>Percent of applications achieving compliance within one week</td>
<td>28%</td>
<td>45%</td>
</tr>
<tr>
<td>Percent of non-compliant applications that are out of compliance for more than six months</td>
<td>39%</td>
<td>20%</td>
</tr>
</tbody>
</table>
**Number of Builds Submitted to Achieve Policy Compliance**

- Enterprises with a Programmatic Approach:
  - 1 Build: 47%
  - 2 Builds: 1%
  - 3 Builds: 1%
  - 4 Builds: 1%
  - 5-10 Builds: 1%

- Enterprises with an Ad-Hoc Approach:
  - 1 Build: 30%
  - 2 Builds: 2%
  - 3 Builds: <1%
  - 4 Builds: 1%
  - 5-10 Builds: <1%

**Time Taken to Achieve Policy Compliance**

- Enterprises with a Programmatic Approach:
  - 0-1 Week: 45%
  - 1-4 Weeks: 3%
  - 4-12 Weeks: 4%

- Enterprises with an Ad-Hoc Approach:
  - 0-1 Week: 28%
  - 1-4 Weeks: 2%
  - 4-12 Weeks: 4%

* *Slight differences between the total percentages in figures are due to rounding.*
Number of Builds Submitted for Non-Compliant Applications*

- Enterprises with a Programmatic Approach:
  - 1 Build: 39%
  - 2 Builds: 7%
  - 3 Builds: 3%
  - 4 Builds: 1%
  - 5-10 Builds: 1%

- Enterprises with an Ad-Hoc Approach:
  - 1 Build: 57%
  - 2 Builds: 6%
  - 3 Builds: 3%
  - 4 Builds: 2%

Time Spent Out of Compliance*

- Enterprises with a Programmatic Approach:
  - 0-1 Week: 1%
  - 1-4 Weeks: 5%
  - 4-12 Weeks: 13%
  - 12-24 Weeks: 9%
  - 24-36 Weeks: 3%
  - 36+ Weeks: 17%

- Enterprises with an Ad-Hoc Approach:
  - 0-1 Week: 2%
  - 1-4 Weeks: 3%
  - 4-12 Weeks: 7%
  - 12-24 Weeks: 16%
  - 24-36 Weeks: 16%
  - 36+ Weeks: 23%

* Slight differences between the total percentages in figures are due to rounding
HOW ABOUT MOBILE APPS?
<table>
<thead>
<tr>
<th>CWE Category</th>
<th>CWE</th>
<th>Percent Applications Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient Entropy</td>
<td>331</td>
<td>61%</td>
</tr>
<tr>
<td>Use of Hard-coded Cryptographic Key</td>
<td>321</td>
<td>42%</td>
</tr>
<tr>
<td>Information Exposure Through Sent Data</td>
<td>201</td>
<td>39%</td>
</tr>
<tr>
<td>Information Exposure Through Error Message</td>
<td>209</td>
<td>6%</td>
</tr>
</tbody>
</table>
State of Software Security Report

The Intractable Problem of Insecure Software

December 7, 2011

http://www.veracode.com/reports

Now Including Mobile App Data! SEE PAGE 37
Enterprise Testing of the Software Supply Chain

Feature Supplement of Veracode’s State of Software Security Report

NOVEMBER 2012

http://www.veracode.com/reports
QUESTIONS?

Speaker
Joe Brady
jbrady@veracode.com

Veracode Colleagues
Andre Gaeta
agaeta@veracode.com
Dave Gerry
dgerry@veracode.com