Security Scoreboard in the Sky

OWASP AppSec Research
June 24, 2010
Bio

- **Chris Eng**
  - Senior Director of Research at Veracode
  - Responsible for incorporating security intelligence into Veracode’s offerings

- **Previously**
  - Technical Manager at Symantec (through acquisition)
  - Technical Director and Consultant at @stake
  - Security Researcher, etc. at NSA

- **Industry Involvement**
  - Frequent speaker at security conferences
  - Contributor to various CWE, OWASP, WASC initiatives
  - Advisor, program committee for SOURCE Conferences (BOS, BCN)
  - Developed @stake WebProxy (any old timers out there?)
Application Risk Management Services Platform: Automating Security Acceptance Testing

1. SET SECURITY POLICY
2. SCAN APPLICATION
3. REMEDIATE FLAWS
4. ACHIEVE COMPLIANCE WITH POLICY

- Static Binary
- Dynamic
- Manual

UPLOAD BINARY OR SPECIFY URL

MAKE INFORMED DECISIONS
Purchase/Deploy/Accept
Data Set and Available Metrics

Application Data
- Industry vertical
- Application supplier (internal, purchased, outsourced, open source)
- Application type
- Assurance level
- 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
- Mean time between scans
- Days to remediation
- Scans to remediation
- PCI-DSS (pass/fail)
- CWE/SANS Top25 (pass/fail)
- OWASP Top Ten (pass/fail)
State of Software Security, Volume 1

State of Software Security Report
The Intractable Problem of Insecure Software
March 1, 2010

VERACODE
Software Security Simplified
Statistically Significant Sample Size

- Sample size this large enable us to report findings with a reasonable degree of confidence:

- Type I Error
  - Probability of stating that something is FALSE when it is in fact TRUE: < 5%

- Type II Error
  - Probability of stating that something is TRUE when it is in fact FALSE: < 20%

- Margins of error for estimates of various metrics:
  - Flaw count: 10%
  - First scan acceptance rate: 15%
  - Veracode risk-adjusted rating: 10%
  - Remediation time: 10%

1. Most software is indeed very insecure
2. Third-party software is a significant percentage of the enterprise software infrastructure, and third-party components are a significant percentage of most applications
3. Open source projects have comparable security, faster remediation times, and fewer Potential Backdoors than Commercial or Outsourced software
4. A significant amount of Commercial and Open Source software is written in C/C++ making it disproportionately susceptible to vulnerabilities that allow attackers to gain control of systems
5. The pervasiveness of easily remedied vulnerabilities indicates a lack of developer education on secure coding
6. Software of all types from Finance and Government sectors was relatively more secure on first submission to Veracode for testing
7. Outsourced software is assessed the least, suggesting the absence of contractual security acceptance criteria
Most Software is Insecure

42%

58%
# Veracode Risk-Adjusted Ratings

<table>
<thead>
<tr>
<th>Assurance Level</th>
<th>Rating Based on Analysis Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VERY HIGH</strong> (AL5)</td>
<td>90-100 (no VH, H, M) 80-89 (no VH, H) 70-79 (no VH) 60-69</td>
</tr>
<tr>
<td><strong>HIGH</strong> (AL4)</td>
<td>80-100 (no VH, H) 70-79 (no VH) 60-69 50-59</td>
</tr>
<tr>
<td><strong>MEDIUM</strong> (AL3)</td>
<td>70-100 (no VH) 60-69 50-59 40-49</td>
</tr>
<tr>
<td><strong>LOW</strong> (AL2)</td>
<td>60-100 50-59 40-49 30-39</td>
</tr>
</tbody>
</table>
Most Software is Insecure

Supplier Performance on First Submission (Adjusted for Business Criticality)

- **Outsourced**: 43% Acceptable, 57% Not Acceptable
- **Open Source**: 41% Acceptable, 59% Not Acceptable
- **Internally Developed**: 49% Acceptable, 51% Not Acceptable
- **Commercial**: 29% Acceptable, 71% Not Acceptable
Most Software is Insecure

OWASP Top 10 Compliance by Supplier on First Submission  (2007 List)

- Outsourced: 4% Acceptable, 96% Not Acceptable
- Open Source: 53% Acceptable, 47% Not Acceptable
- Internally Developed: 12% Acceptable, 88% Not Acceptable
- Commercial: 37% Acceptable, 63% Not Acceptable

CWE/SANS Top 25 Compliance by Supplier on First Submission  (2009 List)

- Outsourced: 6% Acceptable, 94% Not Acceptable
- Open Source: 39% Acceptable, 61% Not Acceptable
- Internally Developed: 30% Acceptable, 70% Not Acceptable
- Commercial: 38% Acceptable, 62% Not Acceptable
Third-Party Software Cannot Be Ignored

- Commercial: 30%
- Internally Developed: 60%
- Open Source: 8%
- Outsourced: 2%
Third-Party Software Cannot Be Ignored

Development Process
- Company Employees
- Contractors
- Enterprise Employees
- Foreign Contractors
- Foreign Sub-Contractors
- US Dev. Center A
- Open Source
- 3rd Party Libraries
- Reuse
- US Dev. Center B
- Developed In-house

Procurement Process
- ISV Employees
- Foreign Contractor
- License 3rd Party Libraries
- Open Source
- ISV (COTS)
- Outsource Partner A
- Outsourcer Employees
- Indian Contractor
- Chinese Contractor
- License 3rd Party Libraries
Third-Party Software Cannot Be Ignored

Development Process:
- Company Employees
- Contractors
- US Dev. Center A
  - Open Source
  - Developed In-house
  - 3rd Party Libraries
  - Reuse
  - US Dev. Center B
- Foreign Contractors
- Foreign Sub-Contractors
- Enterprise Employees

Procurement Process:
- ISV Employees
- Foreign Contractor
  - License 3rd Party Libraries
  - Open Source
- Outsource Partner A
- Outsource Partner B
  - Outsourcer Employees
  - Indian Contractor
  - Chinese Contractor
  - License 3rd Party Libraries
ISVs Slowest to Remediate; Open Source Fastest

Remediation Performance by Supplier

- Internally Developed
- Commercial
- Open Source
- Overall

Average Days to Remediate:
- Internally Developed: 48
- Commercial: 82
- Open Source: 36
- Overall: 59

Average Remediation Submissions to Pass:
- Internally Developed: 1.42
- Commercial: 1.26
- Open Source: 1.11
- Overall: 1.36
C/C++ Less Prevalent in Enterprises

<table>
<thead>
<tr>
<th>Supplier Application Profiles</th>
<th>C/C++</th>
<th>Java</th>
<th>.NET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally Developed</td>
<td>22%</td>
<td>53%</td>
<td>25%</td>
</tr>
<tr>
<td>Commercial</td>
<td>44%</td>
<td>35%</td>
<td>21%</td>
</tr>
<tr>
<td>Open Source</td>
<td>45%</td>
<td>54%</td>
<td>1%</td>
</tr>
<tr>
<td>Outsourced* (Low sample size)</td>
<td>0%</td>
<td>67%</td>
<td>33%</td>
</tr>
</tbody>
</table>
Easily Remedied Vulnerabilities Remain Pervasive

Top Vulnerability Categories (Overall Prevalence)

- Cross-site Scripting (XSS): 33%
- Information Leakage: 22%
- CRLF Injection: 8%
- Cryptographic Issues: 8%
- Buffer Overflow: 6%
- Numeric Errors: 6%
- Directory Traversal: 5%
- Error Handling: 4%
- SQL Injection: 3%
- Time and State: 2%
- Buffer Management Errors: 2%
- Potential Backdoor: 1%
- Credentials Management: 1%
- Encapsulation: 1%
- API Abuse: 1%
Easily Remedied Vulnerabilities Remain Pervasive

Top Vulnerability Categories (Percent of Application Affected)

- Cryptographic Issues: 44%
- Information Leakage: 37%
- Cross-site Scripting (XSS): 33%
- Directory Traversal: 29%
- CRLF Injection: 25%
- Time and State: 23%
- SQL Injection: 20%
- Credentials Management: 18%
- Numeric Errors: 15%
- Error Handling: 15%
- API Abuse: 13%
- Buffer Overflow: 13%
- Encapsulation: 8%
- Buffer Management Errors: 8%
- Insufficient Input Validation: 7%

Legend: Indicate categories that are in the OWASP Top 10 or CWE/SANS Top 25.
Finance and Government are Better

Application Performance by Industry on First Submission (Adjusted for Business Criticality)

- All Industries: 42% Acceptable, 58% Not Acceptable
- Finance-related: 50% Acceptable, 50% Not Acceptable
- Government: 52% Acceptable, 48% Not Acceptable
- Software-related: 34% Acceptable, 66% Not Acceptable
- Other: 40% Acceptable, 60% Not Acceptable
Finance and Government are Better?!

<table>
<thead>
<tr>
<th>Vulnerability Distribution by Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Finance-related</strong></td>
</tr>
<tr>
<td>Cross-site Scripting (XSS)</td>
</tr>
<tr>
<td>Information Leakage</td>
</tr>
<tr>
<td>CRLF Injection</td>
</tr>
<tr>
<td>Cryptographic Issues</td>
</tr>
<tr>
<td>Directory Traversal</td>
</tr>
</tbody>
</table>

35% | 19% | 53%
21% | 17% | 12%
5%  | 11% | 6%
5%  | 8%  | 4%
3%  | 6%  | 3%
Outsourced Software is Assessed the Least

Development Process

- Company Employees
- Contractors
- US Dev. Center A
- Open Source
- Developed In-house
- 3rd Party Libraries
- Reuse
- US Dev. Center B
- Enterprise Employees
- Foreign Contractors
- Foreign Sub-Contractors

Procurement Process

- ISV Employees
- Foreign Contractor
- License 3rd Party Libraries
- Open Source
- Purchased
- Outsource Partner A
- Outsource Employees
- Indian Contractor
- Chinese Contractor
- License 3rd Party Libraries
More Resources

- Download the report, plus other whitepapers, webcasts, and educational resources
  - [http://veracode.com/resources](http://veracode.com/resources)
  - Volume 2 due out in July/August timeframe

- Veracode ZeroDay Labs Blog
  - [http://veracode.com/blog](http://veracode.com/blog)

- Contact info
  - Email: ceng@veracode.com
  - Twitter: @chriseng
  - Phone: 781.425.6040