BSIMM: A Software Security Maturity Model

Brian Chess
Chief Scientist
Fortify Software

Joint work with Gary McGraw and Sammy Migues from Cigital

OWASP-Day III
Centro di Competenza ICT-Puglia - Dipartimento di Informatica
Università degli Studi di Bari

23rd February 2009 - Bari (Italy)
About Fortify

- Founded in 2002 on premise that security must be built in; reactive security doesn't work.
- Fortify sells products and services for creating secure code and for defending deployed applications. (Free product license for university research.)
Data loss

244,928,681
Number of data records reported compromised from Feb 2005 – Sept 2008
Source: Privacy Rights Clearinghouse www.privacyrights.org

45%
Percentage of IT, security and business executive respondents that did not know what types of attacks have occurred on their system

+106%
Increase in reported breaches due to 3rd parties, such as outsourcers, contractors and consultants since 2006
Source: Ponemon Institute, 2007

40%
Percentage of IT, security and business executive respondents that did not know the number of security incidents experienced in 2007
Software security common sense

Software security is more than a set of security functions
  - Not magic crypto fairy dust
  - Not silver-bullet security mechanisms
Non-functional aspects of design are essential
Must address both bugs in code and flaws in design
Security is an emergent property (just like quality)
To end up with secure software, you have to build security in
Technology is cool

- Find vulnerabilities
- Protect against attack
- Harness dev horsepower
- Manage vulnerabilities
Security in the Development Lifecycle
More Questions than Answers

- Same activities for all software project?
- How to get budget / internal support?
- Which vulnerabilities do I have to fix?
- What about outsourcing?
- How to handle open source?
- Who does the work?
Objective: describe what works

BSIMM
- Building Security In Maturity Model
- Real data from real initiatives
The process

- Big idea: Build a maturity model from actual data gathered from 9 large-scale initiatives
- Create software security framework
- In-person executive interviews
- Build bullet lists (one per practice)
- Bucketize the lists to identify activities
- Create levels
  - Objectives → Activities
  - 110 activities supported by real data
  - Three levels of “maturity”
Seven of the nine
Real world data

- **Age**
  - Avg 5.25 yrs
  - Newest 2.5
  - Oldest 10

- **SSG Size**
  - Avg 41
  - Smallest 12
  - Largest 100
  - Median 35

- **Satellite size**
  - Avg 49
  - Smallest 0
  - Largest 300
  - Median 20

- **Dev size**
  - Avg 7750
  - Smallest 450
  - Largest 30,000
  - Median 5000
# Software Security Framework

<table>
<thead>
<tr>
<th>Governance</th>
<th>Intelligence</th>
<th>SSDL Touchpoints</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy and Metrics</td>
<td>Attack Models</td>
<td>Architecture Analysis</td>
<td>Penetration Testing</td>
</tr>
<tr>
<td>Compliance and Policy</td>
<td>Security Features and Design</td>
<td>Code Review</td>
<td>Software Environment</td>
</tr>
<tr>
<td>Training</td>
<td>Standards and Requirements</td>
<td>Security Testing</td>
<td>Configuration Management and Vulnerability Management</td>
</tr>
</tbody>
</table>
Common ground

- **Everyone** has a software security group (SSG)
- SSG is roughly 1% size of dev team
- Ten activities that ALL do
  - evangelist role
  - policy
  - awareness training
  - history in training
  - security features
  - static analysis
  - SSG does ARA
  - black box tools
  - external pen testing
  - good network security
Ten surprising things

1. Bad metrics hurt
2. Secure-by default frameworks
3. WAF Myth
4. QA can’t do security
5. Evangelize over audit
6. ARA is hard
7. Practitioners don’t talk attacks
8. Training is advanced
9. Decline of Pen Testing
10. Fuzz testing
BSIMM

- Release March 10
- Top-down presentation through GOALS and OBJECTIVES
- 110 activities with examples
- Three levels of maturity
- Creative commons

- How to use the model
- Where do you stand?
- What should you do next?
Report Card

Average maturity over nine

- Strategy
- CM/VM
- Environment
- Penetration testing
- Code
- Architecture
- Compliance
- Training
- Features
- Standards

Average maturity over nine

- Company 1
- Avg
Learn more

Nine Things Everybody Does

Top 10 Surprises

A Software Security Framework

Coming March 10
http://www.bsa-mm.com
BSIMM: A Software Security Maturity Model

Brian Chess
Chief Scientist
Fortify Software

Joint work with Gary McGraw and Sammy Migues from Cigital

OWASP-Day III
Centro di Competenza ICT-Puglia - Dipartimento di Informatica
Università degli Studi di Bari
23rd February 2009 - Bari (Italy)

The OWASP Foundation
http://www.owasp.org