Building Security In Maturity Model

Gary McGraw, Ph.D.
Chief Technology Officer, Cigital
Brian Chess, Ph.D.
Chief Scientist, Fortify Software

August 2009
We hold these truths to be self-evident

- 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
- Bugs and flaws are 50/50
- Security is an emergent property of the entire system (just like quality)
- Getting security right requires building security in
A shift from philosophy to HOW TO

- Integrating best practices into large organizations
  - Microsoft’s SDL
  - Cigital’s touchpoints
  - OWASP adopts CLASP
Breaking new ground

- Building Security In Maturity Model
- Real data from real initiatives
- McGraw, Chess, & Migues
46 software security initiatives

- 26 Financial
- 7 ISV
- 6 Tech
- 2 Defense
- 3 Retail
- 1 Oil
- 1 Behemoth

- visa europe
- thomson/reuters
- BP
- SAP
- nokia
- ABN/amro
- ING
- telecomm italia
- swift
- standard life
- microsoft
- dtcc
- emc
- fidelity
- adobe
- wells fargo
- goldman sachs
- google
- qualcomm
- morgan stanley
- usaf
- dell
- pershing
- the h bank
- Barclay's Capital
- bank of tokyo
- ups
- bank of mont real
- cisco
- bank of america
- walmart
- finra
- vanguard
- college board
- oracle
- state street
- omgeo
- motorola
- general electric
- lockheed martin
- intuit
- vmware
- amex
- bank of ny mellon
- harris bank
- paypal

© 2009 Cigital Inc.
The nine

Two more unnamed financial services firms
Building BSIMM

- Big idea: Build a maturity model from actual data gathered from 9 of 35 known large-scale software security initiatives

- Create a software security framework
- Nine 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”
A Software Security Framework

The Software Security Framework (SSF)

<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>

- Four domains
- Twelve practices
- An “archeology grid”
- See informIT article at [http://bsi-mm.com](http://bsi-mm.com)
Monkeys eat bananas

- BSIMM is not about good or bad ways to eat bananas or banana best practices
- BSIMM is about observations
Real-world data: the nine

- Initiative age: 5yrs 4months avg.
  - Newest: 2.5
  - Oldest: 10
- SSG size: 41
  - Smallest: 12
  - Largest: 100
  - Median: 35
- Satellite size: 79
  - Smallest: 0
  - Largest: 300
  - Median: 20
- Dev size: 7750
  - Smallest: 450
  - Largest: 30,000
  - Median: 5000

Average SSG size: 1% of dev
Ten surprising things

1. Bad metrics hurt
2. Secure-by default frameworks
3. Nobody uses WAFs
4. QA can’t do software security
5. Evangelize over audit
6. ARA is hard
7. Practitioners don’t talk attacks
8. Training is advanced
9. Pen testing is diminishing
10. Fuzz testing

InformIT article on BSIMM website http://bsi-mm.com
BSIMM basics

- Software security framework
- Top-down presentation through GOALS and OBJECTIVES
- 110 activities with examples
- Three levels of maturity
- Discussion of how to use the model
A 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>

- Four domains
- Twelve practices
- See informIT article on BSIMM website
  http://bsi-mm.com

© 2009 Cigital Inc.
## GOVERNANCE: TRAINING

<table>
<thead>
<tr>
<th>Objective</th>
<th>Activity</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>[T1.1] promote culture of security throughout the organization</td>
<td>provide awareness training</td>
<td>1</td>
</tr>
<tr>
<td>[T1.2] ensure new hires enhance culture</td>
<td>include security resources in onboarding</td>
<td></td>
</tr>
<tr>
<td>[T1.3] act as informal resource to leverage teachable moments</td>
<td>establish SSG office hours</td>
<td></td>
</tr>
<tr>
<td>[T1.4] create social network tied into dev</td>
<td>identify satellite during training</td>
<td></td>
</tr>
<tr>
<td>[T2.1] build capabilities beyond awareness</td>
<td>offer role-specific advanced curriculum (tools, technology stacks, bug parade)</td>
<td>2</td>
</tr>
<tr>
<td>[T2.2] see yourself in the problem</td>
<td>create/use material specific to company history</td>
<td></td>
</tr>
<tr>
<td>[T2.3] keep staff up-to-date and address turnover</td>
<td>require annual refresher</td>
<td></td>
</tr>
<tr>
<td>[T2.4] reduce impact on training targets and delivery staff</td>
<td>offer on-demand individual training</td>
<td></td>
</tr>
<tr>
<td>[T2.5] educate/strengthen social network</td>
<td>hold satellite training/events</td>
<td></td>
</tr>
<tr>
<td>[T3.1] align security culture with career path</td>
<td>reward progression through curriculum (certification or HR)</td>
<td>3</td>
</tr>
<tr>
<td>[T3.2] spread security culture to providers</td>
<td>provide training for vendors or outsource workers</td>
<td></td>
</tr>
<tr>
<td>[T3.3] market security culture as differentiator</td>
<td>host external software security events</td>
<td></td>
</tr>
</tbody>
</table>
Example activity

[T1.3] Establish SSG office hours. The SSG offers help to any and all comers during an advertised lab period or regularly scheduled office hours. By acting as an informal resource for people who want to solve security problems, the SSG leverages teachable moments and emphasizes the carrot over the stick. Office hours might be held one afternoon per week in the office of a senior SSG member.
Ten things everybody does

- Activities that ALL do
  - evangelist role
  - policy
  - awareness training
  - history in training
  - security features
  - SSG does ARA
  - code review tools
  - black box tools
  - external pen testing
  - good network security
Top 10 things
- green = good?
- red = bad?

Blue shift practices to emphasize
- activities you should maybe think about in blue
We are a special snowflake (NOT)

- ISV results are similar to financial services
- You do the same things
- You can demand the same results
Using BSIMM

- BSIMM released March 2009 under creative commons
  - http://bsi-mm.com
- BSIMM is a yardstick
  - Use it to see where you stand
  - Use it to figure out what should you do next
- BSIMM is evolving
  - More BSIMM victims (8 and counting)
  - BSIMM Europe
  - BSIMM lite
  - Statistics
  - Correlations
Where to Learn More
“So now, when we face a choice between adding features and resolving security issues, we need to choose security.”

-Bill Gates