



Building Security In Maturity Model

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

August 2009



Software Confidence. Achieved.

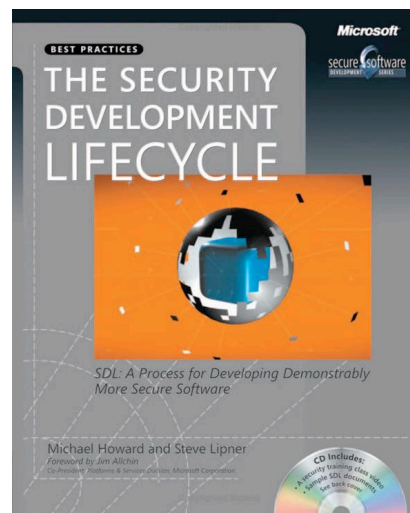
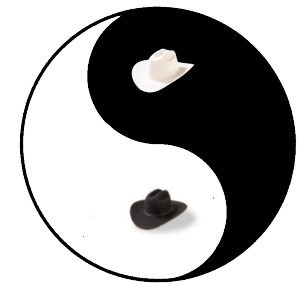


We hold these truths to be self-evident

- 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, & Miguez



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 hartford

- barclays capital

- bank of tokyo

- ups

- bank of montreal

- 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



The nine



*The Depository Trust &
Clearing Corporation*



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)			
Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

- Four domains
- Twelve practices
- An “archeology grid”
- See informIT article at <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](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

The Software Security Framework (SSF)			
Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

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

Training practice skeleton

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

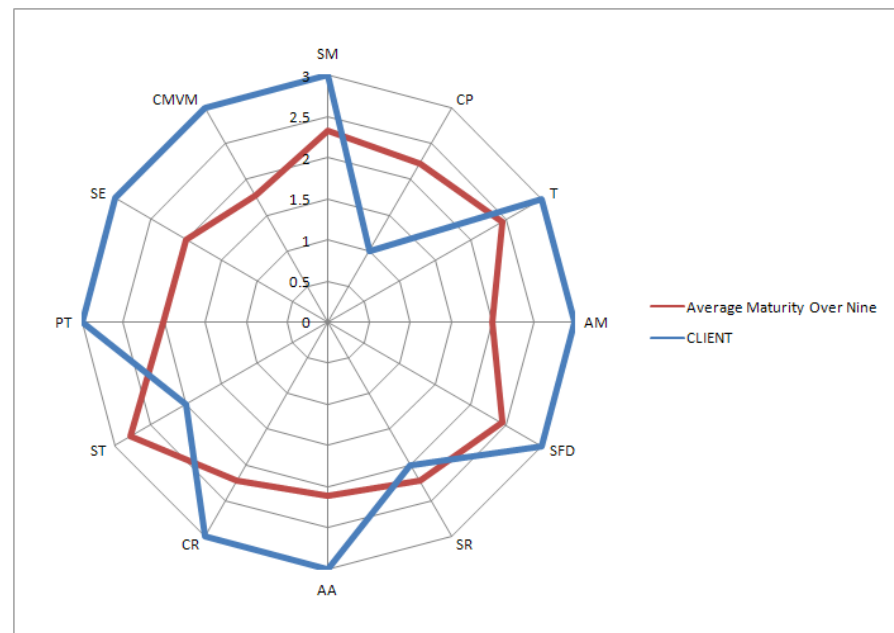
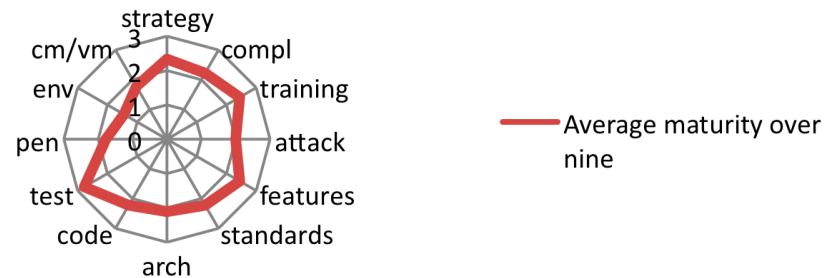
Example activity

[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

Average maturity over nine

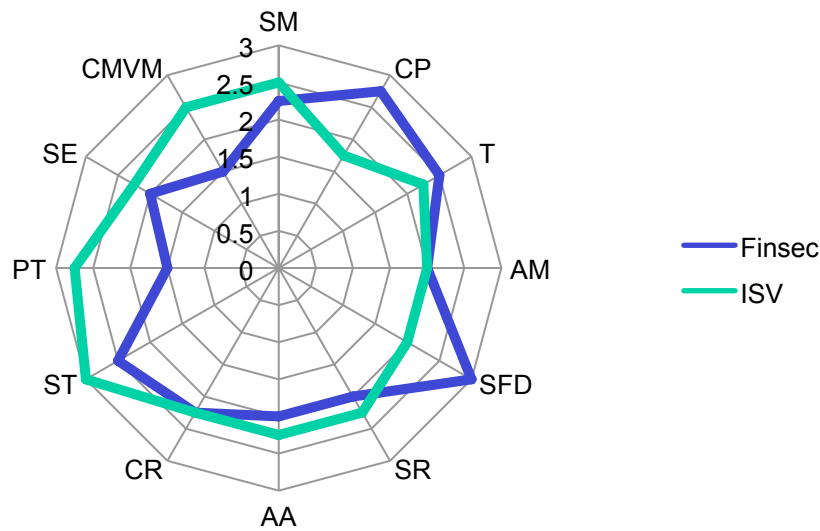


BSIMM Scorecard

Governance			Intelligence			SDL Touchpoints			Deployment		
Activity	Observed	CLIENT	Activity	Observed	CLIENT	Activity	Observed	CLIENT	Activity	Observed	CLIENT
[SM1.1]	4	1	[AM1.1]	5	1	[AA1.1]	5		[PT1.1]	9	
[SM1.2]	8	1	[AM1.2]	6		[AA1.2]	4		[PT1.2]	2	
[SM1.3]	6	1	[AM1.3]	2		[AA1.3]	8	1	[PT2.1]	3	1
[SM1.4]	7	1	[AM1.4]	7		[AA1.4]	3		[PT2.2]	2	
[SM1.5]	7	1	[AM2.1]	3		[AA2.1]	4		[PT2.3]	1	
[SM2.1]	7	1	[AM2.2]	6		[AA2.2]	2	1	[PT3.1]	2	1
[SM2.2]	4	1	[AM2.3]	5		[AA2.3]	5		[PT3.2]	2	
[SM2.3]	7	1	[AM2.4]	5		[AA3.1]	2				
[SM2.4]	4	1	[AM3.1]	1		[AA3.2]	1	1			
[SM3.1]	3	1	[AM3.2]	1	1						
[SM3.2]	1	1									
[CP1.1]	6	1	[SFD1.1]	9	1	[CR1.1]	3	1	[SE1.1]	2	1
[CP1.2]	6		[SFD1.2]	6	1	[CR1.2]	7	1	[SE1.2]	9	1
[CP1.3]	9	1	[SFD2.1]	6	1	[CR1.3]	3	1	[SE2.1]	1	1
[CP2.1]	3		[SFD2.2]	5	1	[CR2.1]	7	1	[SE2.2]	4	1
[CP2.2]	4		[SFD2.3]	4	1	[CR2.2]	5	1	[SE2.3]	2	1
[CP2.3]	5		[SFD3.1]	1	1	[CR2.3]	4	1	[SE3.1]	3	1
[CP2.4]	3		[SFD3.2]	5	1	[CR2.4]	5	1			
[CP2.5]	5					[CR2.5]	5	1			
[CP3.1]	1					[CR3.1]	2	1			
[CP3.2]	2					[CR3.2]	1	1			
[CP3.3]	2					[CR3.3]	1	1			
[T1.1]	9		[SR1.1]	5	1	[ST1.1]	5	1	[CMVM1.1]	4	1
[T1.2]	5		[SR1.2]	3		[ST1.2]	5		[CMVM1.2]	6	
[T1.3]	5	1	[SR1.3]	3	1	[ST2.1]	9	1	[CMVM2.1]	6	1
[T1.4]	7		[SR1.4]	4		[ST2.2]	2		[CMVM2.2]	4	
[T2.1]	6		[SR2.1]	3	1	[ST2.3]	3	1	[CMVM2.3]	2	1
[T2.2]	8	1	[SR2.2]	1		[ST3.1]	5		[CMVM3.1]	1	
[T2.3]	1		[SR2.3]	4	1	[ST3.2]	7		[CMVM3.2]	2	1
[T2.4]	6		[SR2.4]	5		[ST3.3]	2				
[T2.5]	4	1	[SR2.5]	4	1	[ST3.4]	2				
[T3.1]	2		[SR3.1]	3							
[T3.2]	1										
[T3.3]	1	1									

- 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)

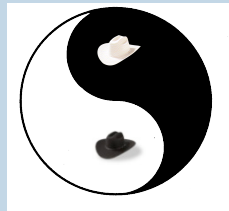


- ISV results are similar to financial services
- You do the same things
- You can demand the same results

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

For more on BSIMM

- <http://bsi-mm.com>
- See the Addison-Wesley Software Security series
- Send e-mail: gem@cigital.com
chess@fortify.com

“So now, when we face a choice between adding features and resolving security issues, we need to choose security.”

-Bill Gates

