cigital

Software Security and the BSIMM

Gary McGraw, Ph.D.
Chief Technology Officer

Cigital

Providing software security professional services since 1992

World's premiere software security consulting firm

- 250 professional consultants
- Washington, NY, Silicon Valley, Bloomington, Boston, Amsterdam, London, Chicago, Atlanta

Recognized experts in software security

- Widely published in books, white papers, and articles
- Industry thought leaders

Pop quiz

What do wireless devices, cell phones, PDAs, browsers, operating systems, servers, routers, personal computers, cloud computing, public key infrastructure systems, and firewalls have in common?

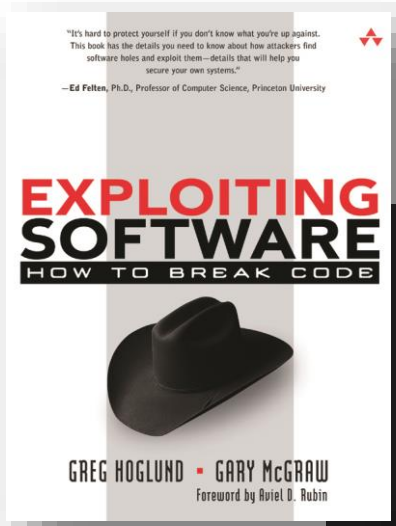
Software

Advocacy

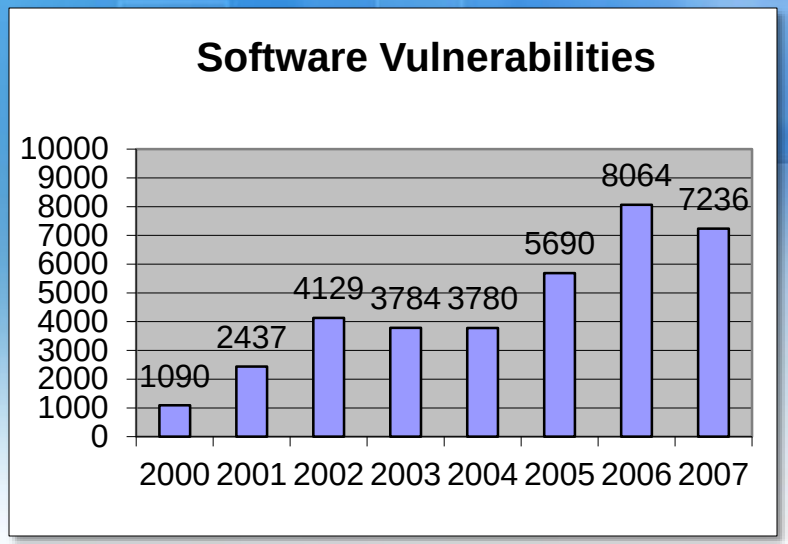
Error 163: ?Type mismatch –or- We’re really sorry

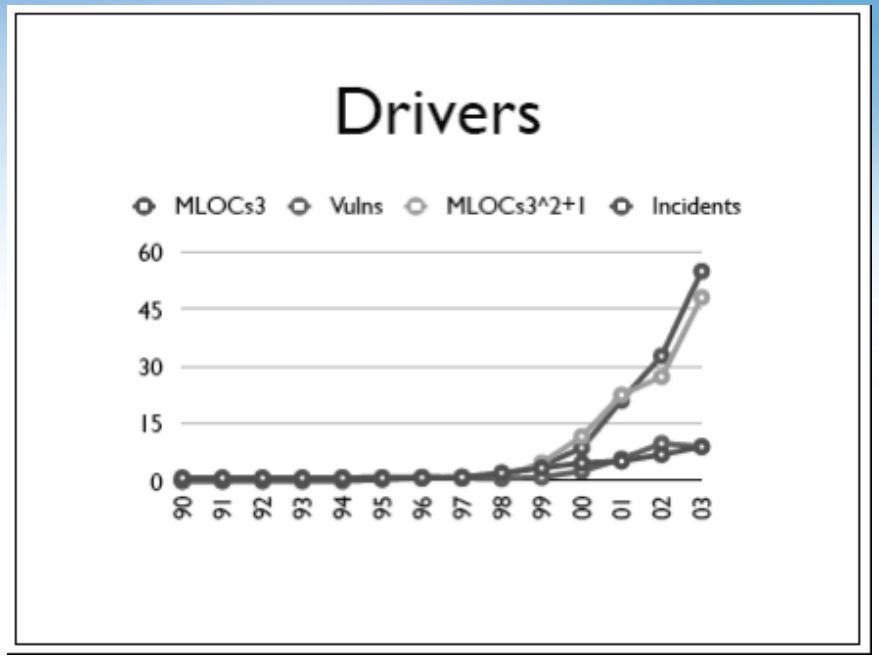
Software is broken (not just Web apps)

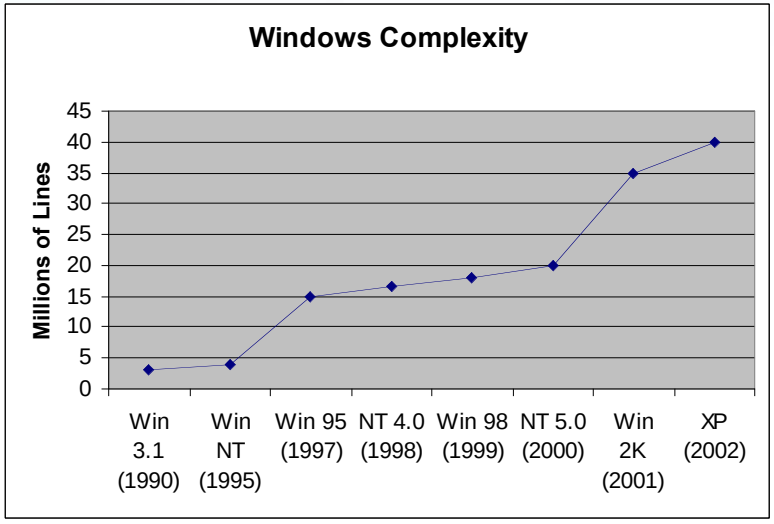
- stuxnet
- firesheep
- <botnet>
- zeus
- nimda



More code, more bugs







cigital

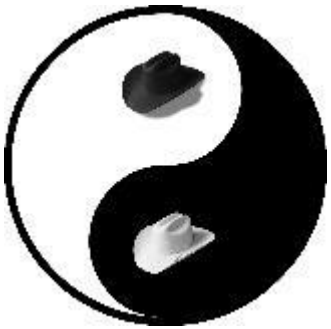
The rise of the software security group (SSG)

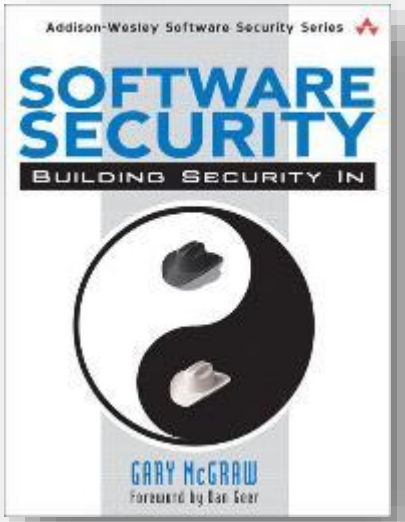
- Cigital SSG turned sixteen in 2013
- Microsoft adopts the Secure Development Lifecycle
- Most firms have a group devoted to software security

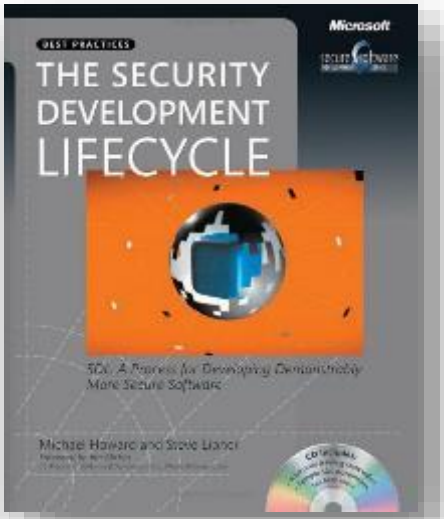
- microsoft
- dtcc
- emc
- fidelity
- adobe
- wells fargo
- goldman sachs
- google
- qualcomm
- morgan stanley
- usaf
- dell
- pershing
- the hartford
- barclays capital
- bank of tokyo
- ups
- bank of montreal
- sterling commerce
- time warner
- cisco
- bank of america
- walmart
- finra
- vanguard
- college board
- oracle
- state street
- omgeo
- motorola
- general electric
- lockheed martin
- intuit
- vmware
- amex
- bank of ny mellon
- harris bank
- paypal
- symantec
- visa europe
- thomson/reuters
- BP
- SAP
- nokia
- ebay
- mckesson
- ABN/amro
- ING
- telecom italia
- swift
- standard life
- cigna
- AON
- coke
- mastercard
- apple
- AOL
- CA

2006: a shift from philosophy to HOW TO

- Integrating best practices into large organizations' SDLC (that is, an SSDL)
  - Microsoft's SDL
  - Cigital's Touchpoints
  - OWASP CLASP







BSIMM: Software Security Measurement

- Real data from (62) real initiatives
- 122 measurements
- 18 (21) over time
- McGraw, Migues, & West

cigital

FORTIFY An HP Company

PlexLogic

Minded security

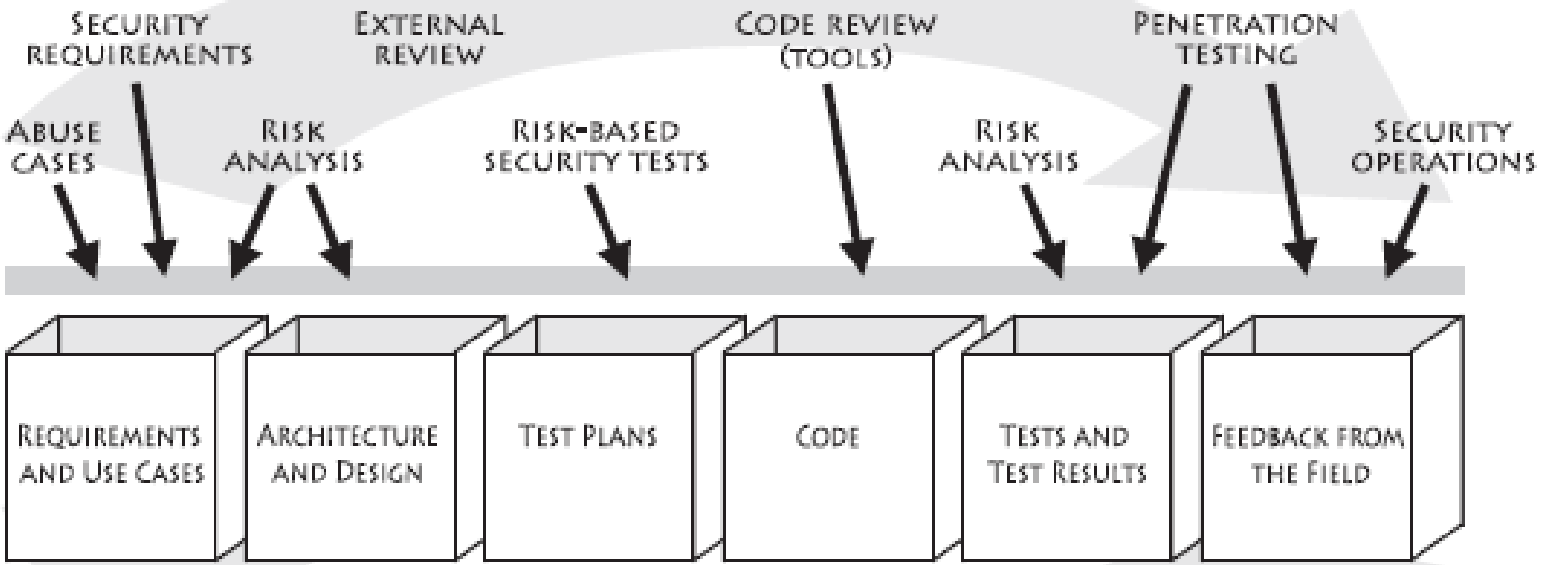
VIRTUALFORGE we harden your software

Software security touchpoints

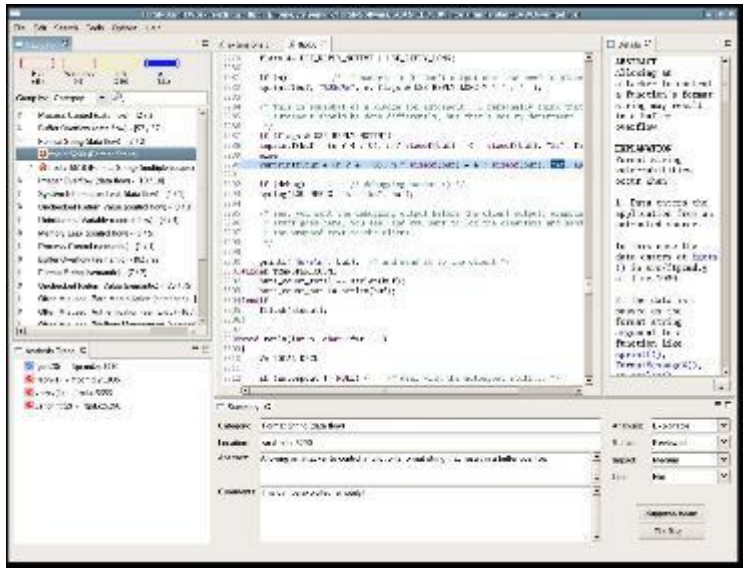
badness-ometer != security meter

badness-ometer

Software security touchpoints



Touchpoint: Code review (with a tool)



FORTIFY

coverity

OUNCE LABS

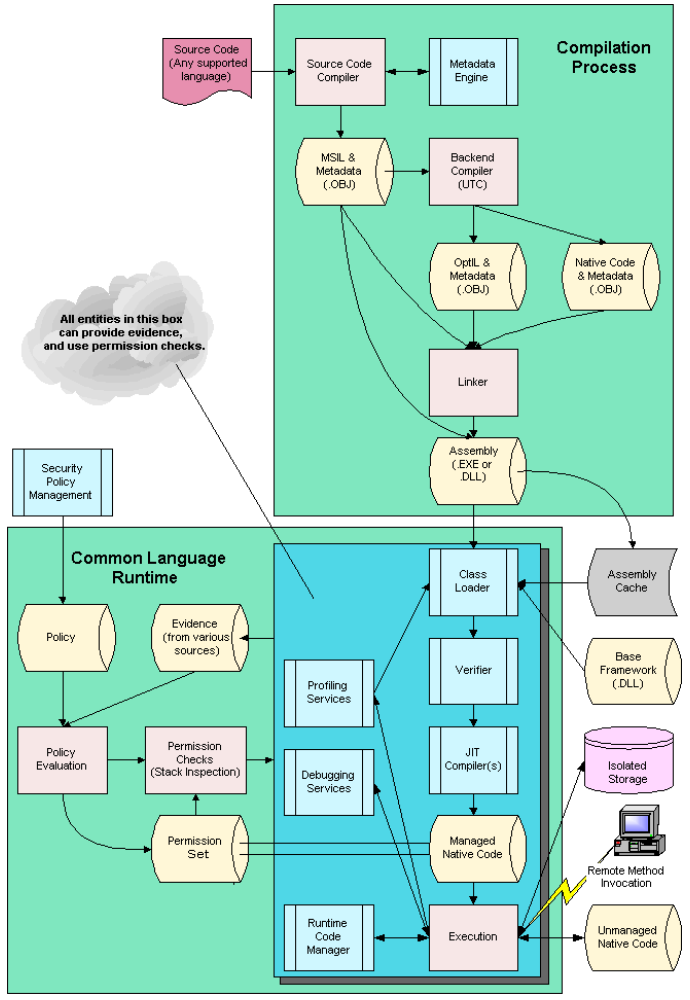
- Code scanning catches on
  - Demand for manual services up
  - Tool adoption proceeding apace (being measured)
- Tools (finally) handle large code bases
  - Don't fail to grep()
  - Simple enforcement is no longer useful
- Customization pays off royally
  - Fidelity
- Training courses about bugs and tools widespread

cigital

Touchpoint: Architecture risk analysis

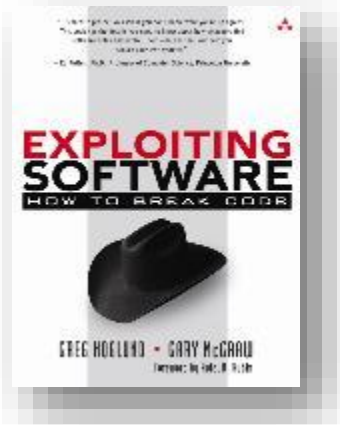
- More common to find customers with a handle on software architecture
- Widespread use of common components
  - Spring
  - Hibernate
  - Log4J
  - OpenSSL
  - "ripple effect"
- Design patterns help

- High-expertise work is still hard to teach
- Training courses about ARA being widely adopted



Touchpoint: Penetration testing

- Penetration testing finds its place
  - Badnessometer (helpful for booting program)
  - Solutions more important than finding problems
- Focus on final software environment
  - Configuration
  - Context
- Clients no longer rely on pen tests exclusively



Fix the dang software

- Software security and application security today are about finding bugs
- The time has come to stop looking for new bugs to add to the list
- Which bugs in this pile should I fix?




The BSIMM

BSIMM: Software Security Measurement

- Real data from (62) real initiatives
- 122 measurements
- 18 (21) over time
- McGraw, Migues, & West

cigital

FORTIFY An HP Company

PlexLogic

Minded security

VIRTUALFORGE we harden your software

51 firms in the BSIMM community

Monkeys eat bananas

- BSIMM is not about good or bad ways to eat bananas or banana best practices
- BSIMM is about observations
- BSIMM is descriptive, not prescriptive
- BSIMM describes and measures multiple prescriptive approaches

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://bsimm.com

Architecture Analysis practice skeleton

SSDL TOUCHPOINTS: ARCHITECTURE ANALYSIS

Capturing software architecture diagrams, applying lists of risks and threats, adopting a process for review, building an assessment and remediation plan.

	Objective	Activity	Level
[AA1.1]	get started with AA	perform security feature review	1
[AA1.2]	demonstrate value of AA with real data	perform design review for high-risk applications	
[AA1.3]	build internal capability on security architecture	have SSG lead review efforts	
[AA1.4]	have a lightweight approach to risk classification and prioritization	use risk questionnaire to rank apps	
[AA2.1]	model objects	define/use AA process	2
[AA2.2]	promote a common language for describing architecture	standardize architectural descriptions (include data flow)	
[AA2.3]	build capability organization-wide	make SSG available as AA resource/mentor	
[AA3.1]	build capabilities organization-wide	have software architects lead review efforts	3
[AA3.2]	build proactive security architecture	drive analysis results into standard architectural patterns (T: sec features/design)	

Example activity

[AA1.2] **Perform design review for high-risk applications.** The organization learns about the benefits of architecture analysis by seeing real results for a few high-risk, high-profile applications. If the software security group (SSG) is not yet equipped to perform an in-depth architecture analysis, it uses consultants to do this work. Ad hoc review paradigms that rely heavily on expertise may be used here, though in the long run they do not scale.

Real-world Data (62 firms)

- Initiative age
  - Average: 5.8 years
  - Newest: 0.1
  - Oldest: 17.4
  - Median: 5.4
- SSG size
  - Average: 17.6
  - Smallest: 1
  - Largest: 100
  - Median: 7.5
- Satellite size
  - Average: 35.9
  - Smallest: 0
  - Largest: 350
  - Median: 6
- Dev size
  - Average: 4097
  - Smallest: 11
  - Largest: 30,000
  - Median: 1400

Average SSG size: 1.75% of dev group size

BSIMM by the Numbers

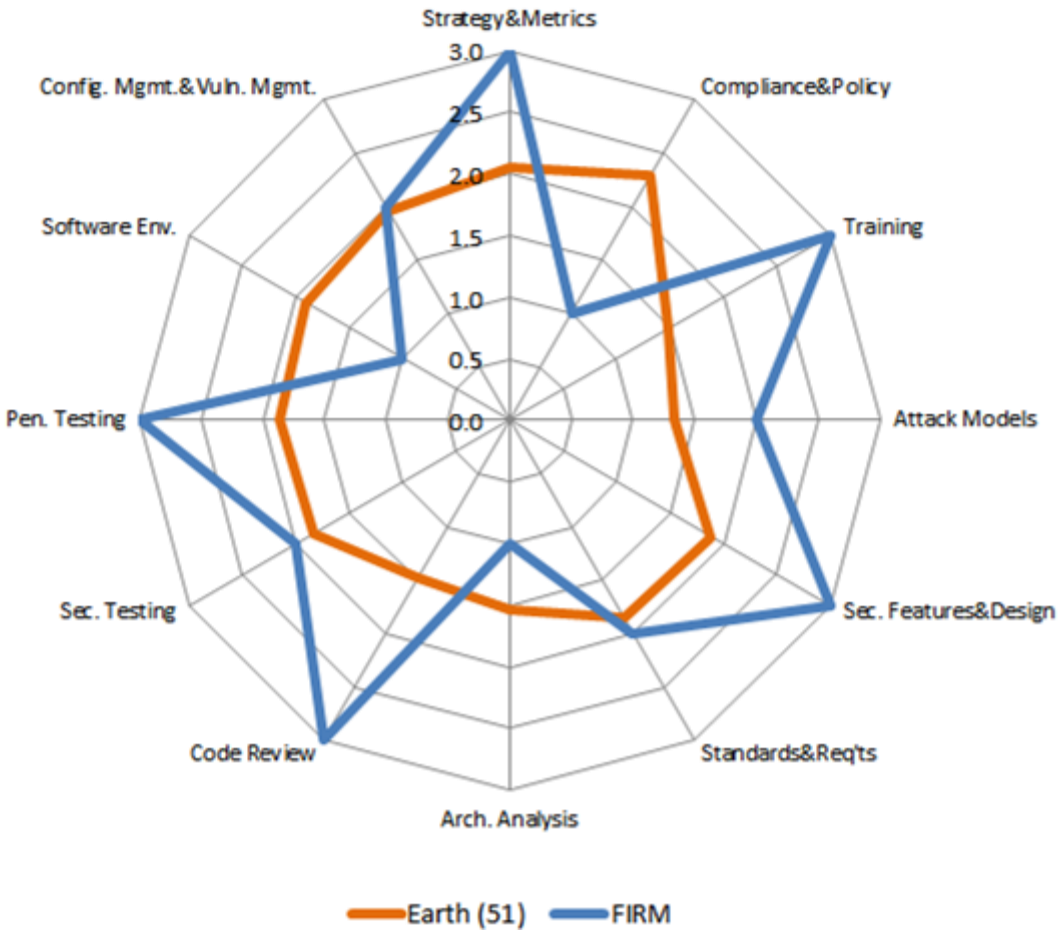
	BSIMM1	BSIMM2	BSIMM3	BSIMM4	BSIMM4+
Firms	9	30	42	51	61
Measurements	9	49	81	95	122
2nd Measurements	0	0	11	13	15
3rd Measurements	0	0	0	1	1
SSG Members	370	635	786	978	1053
Satellite Members	710	1150	1750	2039	2152
Developers	67,950	141,175	185,316	218,286	241,766
Applications	3970	28,243	41,157	58,739	68,572
Avg SSG Age	5.32	4.49	4.32	4.13	4.0
SSG Avg of Avgs	1.13 / 100	1.02 / 100	1.99 / 100	1.95 / 100	1.75 / 100
Financials	4	12	17	19	23
ISVs	4	7	15	19	23
High Tech	2	7	10	13	15

BSIMM4+ Scorecard

Governance		Intelligence		SSDL Touchpoints		Deployment	
Activity	**Observed**	**Activity**	**Observed**	**Activity**	**Observed**	**Activity**	**Observed**
[SM1.1]	39	[AM1.1]	19	[AA1.1]	47	[PT1.1]	53
[SM1.2]	32	[AM1.2]	37	[AA1.2]	36	[PT1.2]	44
[SM1.3]	35	[AM1.3]	28	[AA1.3]	29	[PT1.3]	41
[SM1.4]	50	[AM1.4]	14	[AA1.4]	37	[PT2.2]	22
[SM1.6]	37	[AM1.5]	38	[AA2.1]	9	[PT2.3]	26
[SM2.1]	21	[AM1.6]	17	[AA2.2]	7	[PT3.1]	11
[SM2.2]	27	[AM2.1]	12	[AA2.3]	18	[PT3.2]	10
[SM2.3]	29	[AM2.2]	13	[AA3.1]	9		
[SM2.5]	21	[AM3.1]	3	[AA3.2]	4		
[SM3.1]	15	[AM3.2]	5				
[SM3.2]	7						
[CP1.1]	43	[SFD1.1]	49	[CR1.1]	24	[SE1.1]	26
[CP1.2]	49	[SFD1.2]	43	[CR1.2]	24	[SE1.2]	53
[CP1.3]	39	[SFD2.1]	27	[CR1.4]	38	[SE2.2]	26
[CP2.1]	23	[SFD2.2]	21	[CR1.5]	23	[SE2.4]	25
[CP2.2]	30	[SFD2.3]	15	[CR1.6]	22	[SE3.2]	12
[CP2.3]	28	[SFD3.1]	10	[CR2.2]	13	[SE3.3]	7
[CP2.4]	21	[SFD3.2]	11	[CR2.5]	11		
[CP2.5]	36			[CR3.1]	13		
[CP3.1]	9			[CR3.2]	3		
[CP3.2]	13			[CR3.3]	6		
[CP3.3]	8			[CR3.4]	1		
[T1.1]	42	[SR1.1]	43	[ST1.1]	43	[CMVM1.1]	48
[T1.5]	21	[SR1.2]	31	[ST1.3]	44	[CMVM1.2]	52
[T1.6]	22	[SR1.3]	39	[ST2.1]	24	[CMVM2.1]	44
[T1.7]	26	[SR1.4]	24	[ST2.3]	8	[CMVM2.2]	38
[T2.5]	11	[SR2.1]	12	[ST2.4]	13	[CMVM2.3]	26
[T2.6]	13	[SR2.2]	21	[ST3.1]	11	[CMVM3.1]	4
[T2.7]	11	[SR2.3]	19	[ST3.2]	11	[CMVM3.2]	6
[T3.1]	5	[SR2.4]	20	[ST3.3]	5	[CMVM3.3]	0
[T3.2]	5	[SR2.5]	20	[ST3.4]	6		
[T3.3]	9	[SR3.1]	8				
[T3.4]	6						
[T3.5]	6						

BSIMM4 as a Measuring Stick

- Compare a firm with peers using the high water mark view
- Compare business units
- Chart an SSI over time



BSIMM4 scorecard with FAKE firm data

BSIMM4 Scorecard for: FIRM — Raw Score: 41

Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	BSIMM Firms	FIRM	Activity	BSIMM Firms	FIRM	Activity	BSIMM Firms	FIRM	Activity	BSIMM Firms	FIRM
[SM1.1]	35	1	[AM1.1]	15	1	[AA1.1]	39		[PT1.1]	47	1
[SM1.2]	30		[AM1.2]	31		[AA1.2]	35	1	[PT1.2]	40	1
[SM1.3]	33		[AM1.3]	25		[AA1.3]	27	1	[PT1.3]	35	
[SM1.4]	44	1	[AM1.4]	13	1	[AA1.4]	32		[PT2.2]	20	
[SM1.6]	35		[AM1.5]	32	1	[AA2.1]	10		[PT2.3]	24	1
[SM2.1]	21		[AM1.6]	17	1	[AA2.2]	7		[PT3.1]	11	
[SM2.2]	26		[AM2.1]	12		[AA2.3]	17		[PT3.2]	8	
[SM2.3]	26		[AM2.2]	13		[AA3.1]	9				
[SM2.5]	22	1	[AM3.1]	3		[AA3.2]	4				
[SM3.1]	15	1	[AM3.2]	5							
[SM3.2]	6										
[CP1.1]	40	1	[SFD1.1]	44	1	[CR1.1]	23	1	[SE1.1]	21	1
[CP1.2]	45		[SFD1.2]	37	1	[CR1.2]	20	1	[SE1.2]	47	
[CP1.3]	36	1	[SFD2.1]	25		[CR1.4]	33	1	[SE2.2]	21	
[CP2.1]	21		[SFD2.2]	19		[CR1.5]	22		[SE2.4]	23	
[CP2.2]	28		[SFD2.3]	15	1	[CR1.6]	21		[SE3.2]	11	
[CP2.3]	25		[SFD3.1]	8	1	[CR2.2]	13		[SE3.3]	7	1
[CP2.4]	22		[SFD3.2]	9		[CR2.5]	12				
[CP2.5]	31					[CR3.1]	13	1			
[CP3.1]	7					[CR3.2]	3				
[CP3.2]	12					[CR3.3]	4	1			
[CP3.3]	8					[CR3.4]	TBD				
[T1.1]	38		[SR1.1]	38	1	[ST1.1]	38	1	[CMVM1.1]	40	1
[T1.5]	19	1	[SR1.2]	27		[ST1.3]	37	1	[CMVM1.2]	44	1
[T1.6]	21	1	[SR1.3]	34	1	[ST2.1]	24	1	[CMVM2.1]	37	1
[T1.7]	23		[SR1.4]	21		[ST2.3]	8		[CMVM2.2]	31	
[T2.5]	10		[SR2.1]	12	1	[ST2.4]	12		[CMVM2.3]	23	1
[T2.6]	12	1	[SR2.2]	20		[ST3.1]	9		[CMVM3.1]	5	
[T2.7]	11		[SR2.3]	18		[ST3.2]	11		[CMVM3.2]	6	
[T3.1]	5	1	[SR2.4]	19		[ST3.3]	5		[CMVM3.3]	TBD	
[T3.2]	5		[SR2.5]	21	1	[ST3.4]	6				
[T3.3]	8		[SR3.1]	8							
[T3.4]	6										
[T3.5]	6										

Legend:
- Activity — 111 BSIMM4 activities, shown in 4 domains and 12 practices
- BSIMM Firms — count of firms (out of 51) observed performing each activity
- the most common activity within a practice
- a most common activity not observed in this assessment
- a most common activity observed in this assessment
- a practice where the firm's high-water mark score is below the average of the 51 firms

- Top 12 activities
  - purple = good?
  - red = bad?
- "Blue shift" practices to emphasize

BSIMM4 to BSIMM-V

- BSIMM4 released September 2012 under creative commons
  - http://bsimm.com
  - Italian and German translations available, Spanish soon
- BSIMM is a yardstick
  - Use it to see where you stand
  - Use it to figure out what your peers do
- BSIMM4→BSIMM-V
  - BSIMM is growing
  - Target of 75 firms

Where to learn more

SearchSecurity + Justice League

TechTarget

SearchSecurity

www.searchsecurity.com

No-nonsense monthly security column by Gary McGraw

www.cigital.com/~gem/writing

www.cigital.com/justiceleague

In-depth thought leadership blog from the Cigital Principals

- Scott Matsumoto
- Gary McGraw
- Sammy Migues
- John Steven
- Paco Hope

cigital

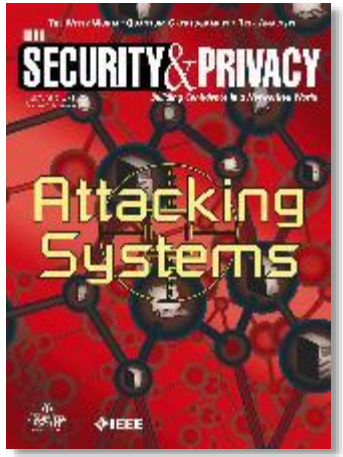
silver bullet + IEEE security & privacy

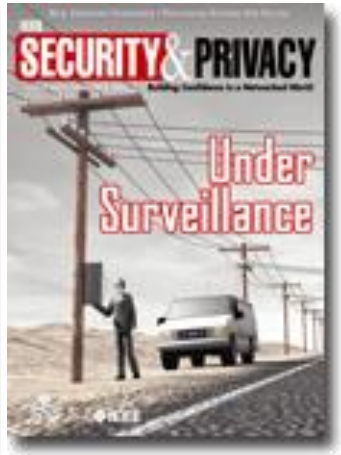
www.cigital.com/silverbullet

Building Security In

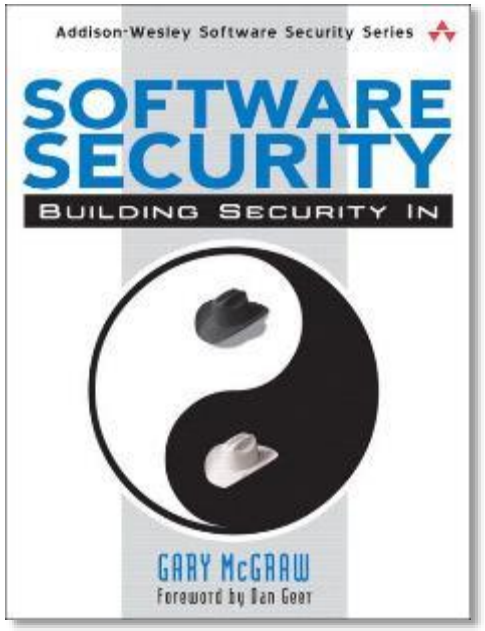
Software Security Best Practices column

www.computer.org/security/bsisub/





The book



How to DO software security

- Best practices
- Tools
- Knowledge

Cornerstone of the Addison-Wesley Software Security Series

www.swsec.com

Addison Wesley

cigital

Build security in

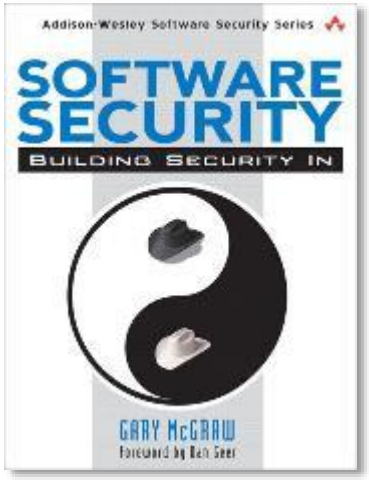
cigital

http://bsimm.com

WE NEED GREAT PEOPLE

Read the Addison-Wesley Software Security series

Send e-mail: gem@cigital.com



Addison Wesley