Cigital
BUILDING SECURITY IN

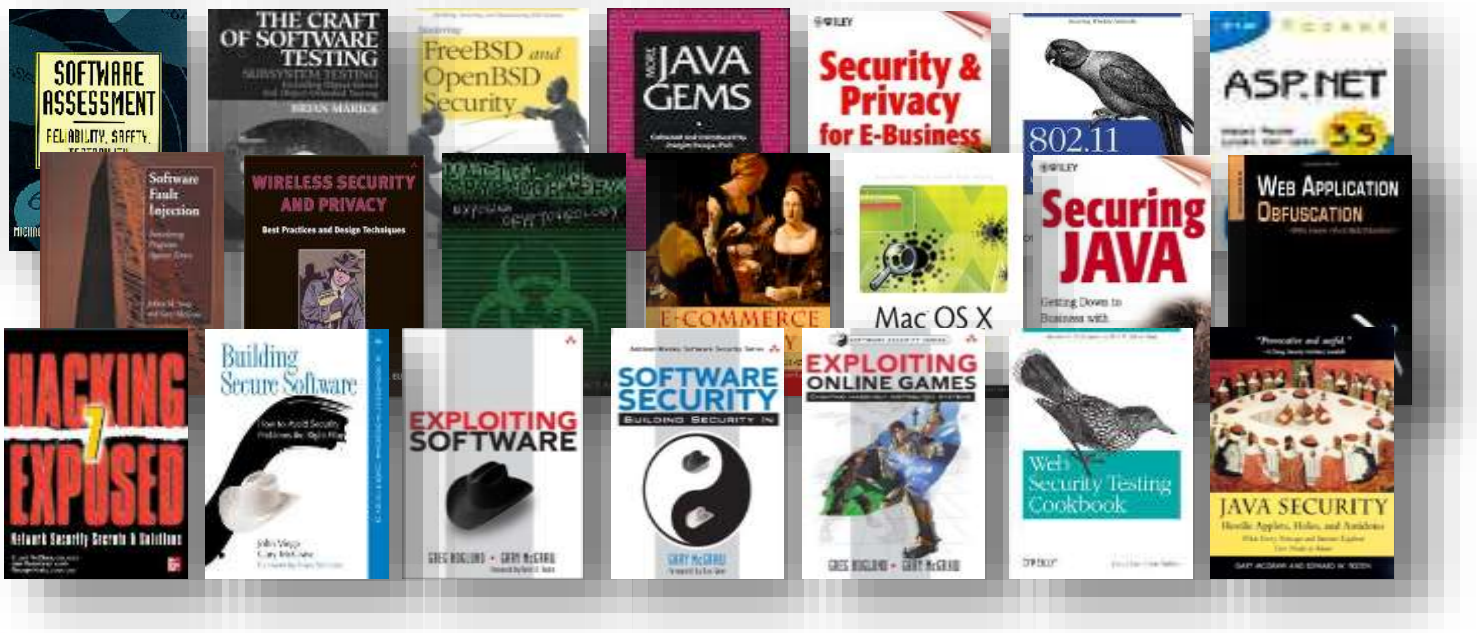
A Brief History of Software, Security, and Software Security: Bits, Bytes, Bugs, and the BSIMM

Gary McGraw, Ph.D.
Chief Technology Officer

@cigitalgem

My Point of View

- Providing software security services since 1992
- Moving armies of developers in global institutions



SOFTWARE AND SECURITY

Software is Everywhere

- Information is the lifeblood of industry
- Software is in our power grid, our cars, our finances, and our communications
- Software is eating the world

- Oh, and most software is broken

Perimeter Security is Failing Us

Today's computer and network security mechanisms are like the walls, moats, and drawbridges of medieval times. At one point, effective for defending against isolated attacks, mounted on horseback. Unfortunately, today's attackers have access to predator drones and laser-guided missiles!

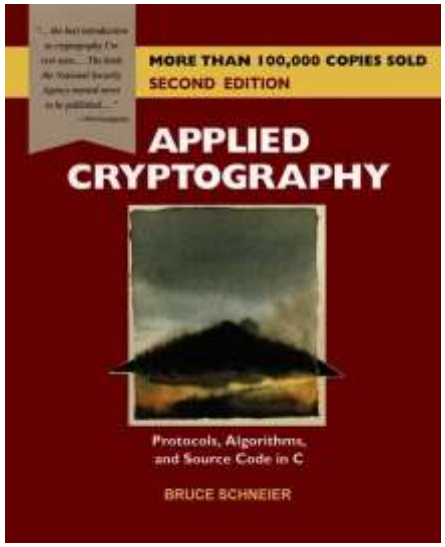
See: "Firewalls, Fairy Dust and Forensics Fail"

http://bit.ly/1kluC7F

Magic Crypto Fairy Dust is not Security

"years ago I wrote another book: Applied Cryptography. I went so far as to write: 'It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics.'

It's just not true. Cryptography can't do any of that."



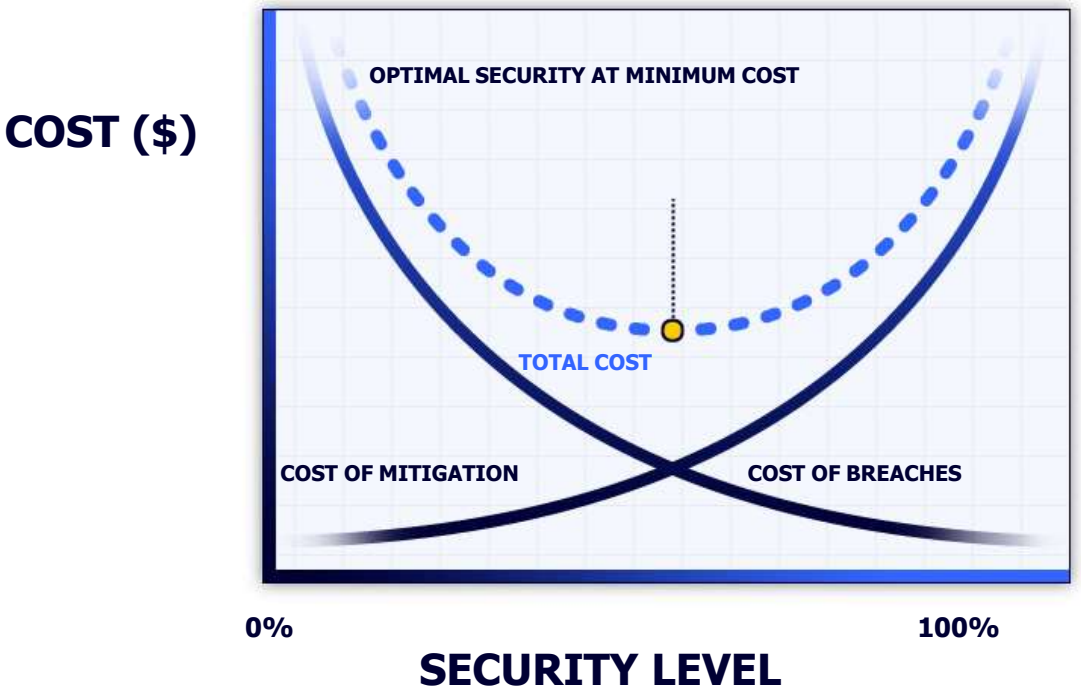
- Bruce Schneier

Security is not a THING

Applied Cryptography
Protocols, Algorithms and Source Code in C
Bruce Schneier
1996 John Wiley & Sons.

Modern Security is Risk Management

- There is no such thing as 100% secure
- Proactive security is about building things properly



SOFTWARE SECURITY BASICS

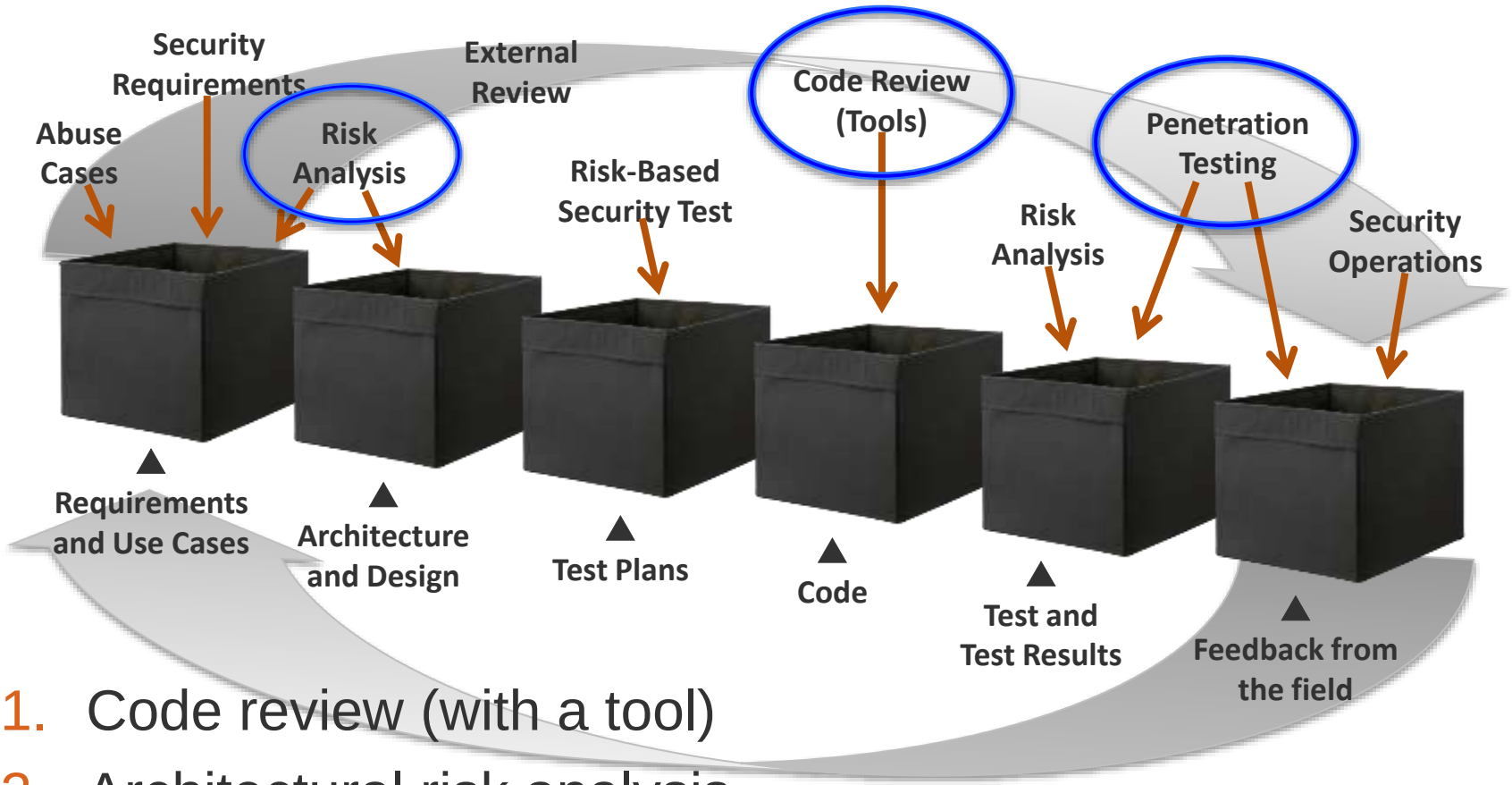
Who should DO software security?

Network security ops guys

NOBODY
IN THE MIDDLE

*Super rad developer **dudes***

Software Security Touchpoints in the SDLC



1. Code review (with a tool)
2. Architectural risk analysis
3. Penetration testing

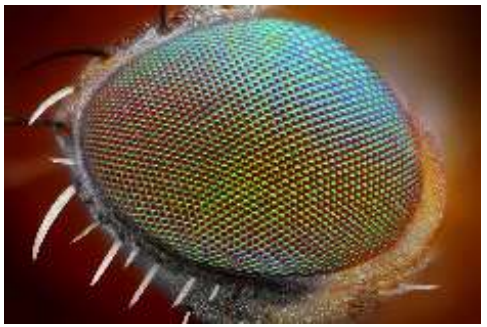
Badness-ometer != security meter

badness-ometer

Fix the Dang Software

- Software security and application security are myopically concerned with finding bugs
- The time has come to stop over focusing on new bugs to add to the (infinite) list
- Work on fixing the bugs (and the other defects too)






Move Past the Bug Parade

- Software security and application security tools over focus on simple bugs
- Design level flaws account for 50% of security defects
- Software security is about fixing design and implementation as code is created

SCIENCE AND THE BSIMM

What is the BSIMM?

- A measurement stick for software security initiatives
- A science project that escaped the lab
- A framework for building and tailoring Software Security Initiatives
- The world's most powerful Community of software security practitioners and executives

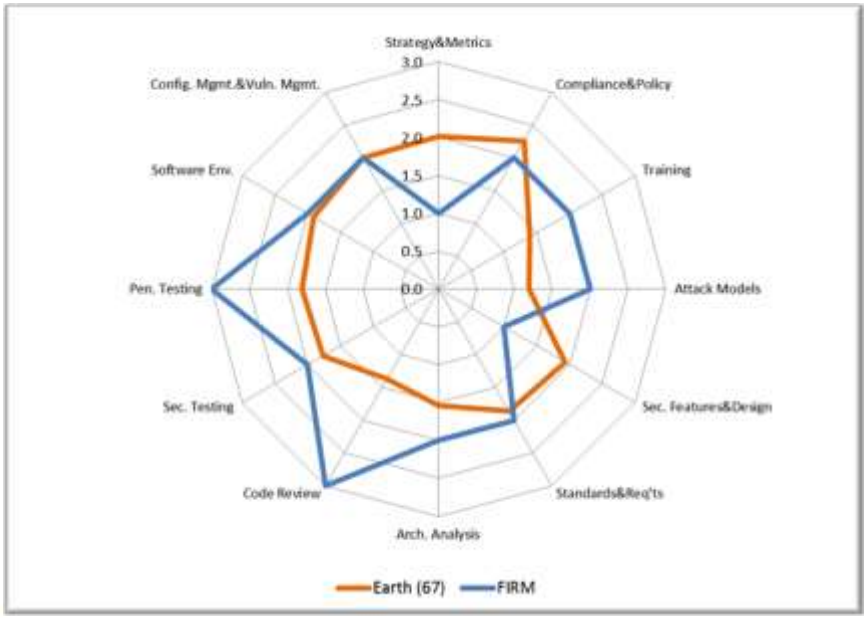
- http://bsimm.com


Adobe
McKESSON
aetna
epsilon
PEARSON
Vanguard
SAP
neustar
FannieMae
QUALCOMM
zynga
SONY
intuit
CapitalOne
NOKIA
Symantec
citi
NETSUITE
MASHERY
Standard Life
PayPal
McAfee
TELECOM ITALIA
salesforce
F-Secure
TOMTOM
Microsoft
vmware
LPS
VISA
Fidelity
THOMSON REUTERS
Intel
HSBC
ComericA Bank
WELLS FARGO
Goldman Sachs
rackspace
EMC²
Nokia Siemens Networks
M&S
JPMORGAN CHASE & CO.
SallieMae
SWIFT

How do you measure software security?

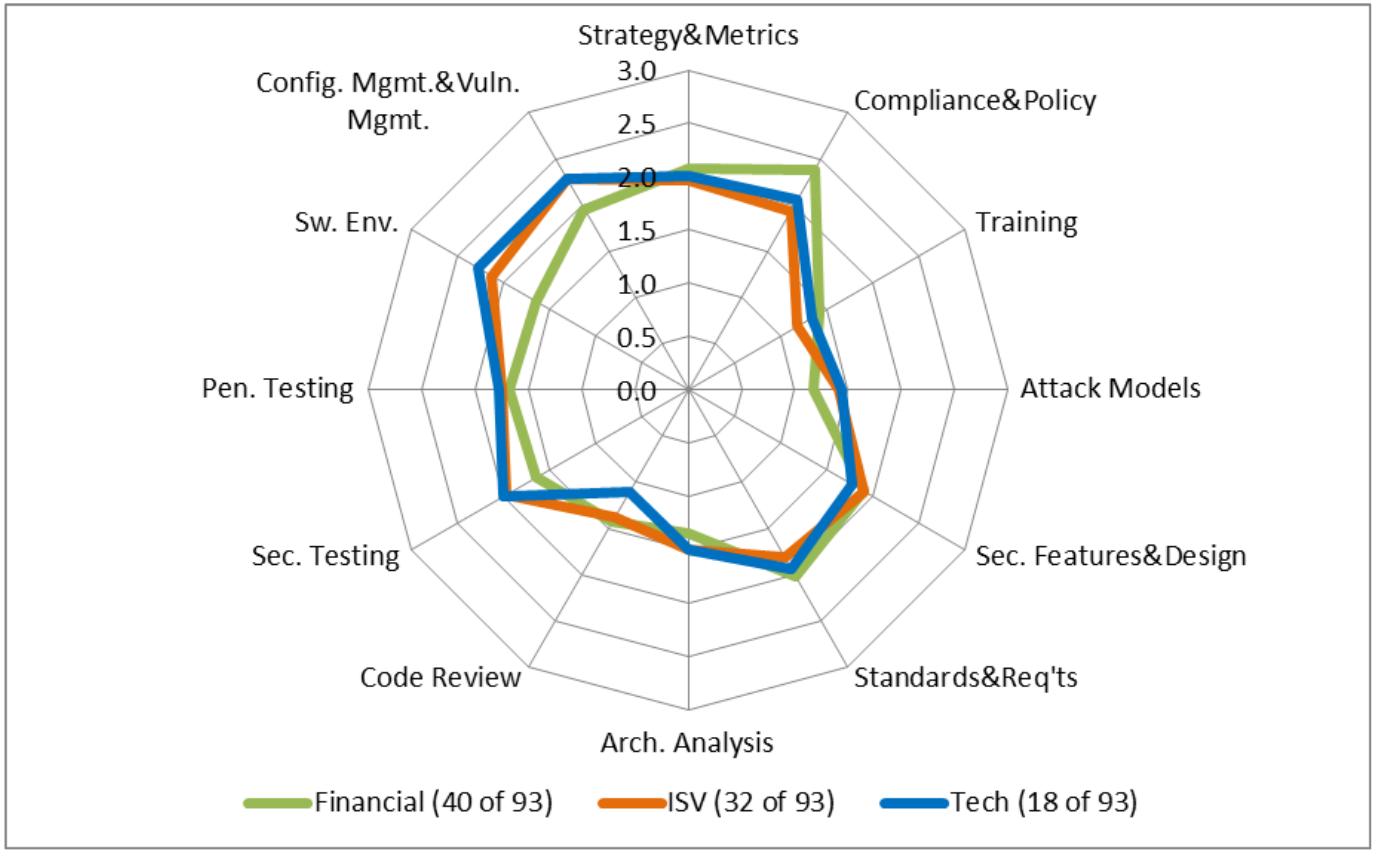
- Badness-ometer != security meter
- A simple tool can’t do it

- Measure the effort in a software security initiative



What good does a BSIMM measurement do?

- Shows a firm where they stand relative to their peers



What good does a BSIMM measurement do?

- Describes observed common activities from the real world
- Demonstrates gaps clearly
- Provides real data and measurement to set SSI strategy
- Shows progress over time

BSIMM-V Scorecard for: FIRM — Raw Score: 37

Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	BSIMM-V Firms	FIRM	Activity	BSIMM-V Firms	FIRM	Activity	BSIMM-V Firms	FIRM	Activity	BSIMM-V Firms	FIRM
[SM1.1]	44	1	[AM1.1]	21	1	[AA1.1]	56	1	[PT1.1]	62	1
[SM1.2]	34		[AM1.2]	43		[AA1.2]	35	1	[PT1.2]	51	1
[SM1.3]	34	1	[AM1.3]	30		[AA1.3]	24	1	[PT1.3]	43	
[SM1.4]	57	1	[AM1.4]	12	1	[AA1.4]	42		[PT2.2]	24	1
[SM1.6]	36		[AM1.5]	42	1	[AA2.1]	10		[PT2.3]	27	
[SM2.1]	26		[AM1.6]	16		[AA2.2]	8	1	[PT3.1]	13	1
[SM2.2]	31		[AM2.1]	7		[AA2.3]	20		[PT3.2]	8	
[SM2.3]	27		[AM2.2]	11	1	[AA3.1]	11				
[SM2.5]	20		[AM3.1]	4		[AA3.2]	4				
[SM3.1]	16		[AM3.2]	6							
[SM3.2]	6										
[CP1.1]	42	1	[SFD1.1]	54		[CR1.1]	24		[SE1.1]	34	
[CP1.2]	52		[SFD1.2]	53	1	[CR1.2]	34	1	[SE1.2]	61	1
[CP1.3]	45	1	[SFD2.1]	26		[CR1.4]	50	1	[SE2.2]	31	1
[CP2.1]	24		[SFD2.2]	29		[CR1.5]	23		[SE2.4]	25	
						[CR1.6]	25	1	[SE3.2]	10	
						[CR2.2]	10		[SE3.3]	9	
						[CR2.5]	15				
						[CR2.6]	18				
						[CR3.2]	4	1			
						[CR3.3]	6				
						[CR3.4]	1				
						[ST1.1]	51	1	[CMVM1.1]	59	1
						[ST1.3]	55	1	[CMVM1.2]	59	
						[ST2.1]	27	1	[CMVM2.1]	50	1
						[ST2.4]	13		[CMVM2.2]	44	
						[ST3.1]	11		[CMVM2.3]	30	
						[ST3.2]	8		[CMVM3.1]	6	
						[ST3.3]	6		[CMVM3.2]	6	
						[ST3.4]	5		[CMVM3.3]	2	
						[ST3.5]	7				
[T3.4]	9										
[T3.5]	5										

[ST1.3] Drive tests with security requirements and security features. Testers target declarative security mechanisms derived from requirements and security features. For example, a tester could try to access administrative functionality as an unprivileged user or verify that a user account becomes locked after some number offailed authentication attempts. For the most part, security features can be tested in a similar fashion to other software features. Security mechanisms based on requirements such as account lockout, transaction limitations, entitlements, and so on are also tested. Of course, software security is not security software, but getting started with features is easy.

Legend:
- Activity — 111 BSIMM-V activities, shown in 4 domains and 12 practices
- BSIMM Firms — count of firms (out of 67) observed performing each activity
- the most common activity within a practice
- a common activity not observed in this assessment
- a common activity observed in this assessment
- a practice where firm's high-water mark score is below the BSIMM-V average

	BSIMM-V+	BSIMM-V	BSIMM4	BSIMM3	BSIMM2	BSIMM1
Firms	**93**	67	51	42	30	9
Measurements	**216**	161	95	81	49	9
2nd Measures	**48**	21	13	11	0	0
3rd Measures	**9**	4	1	0	0	0
SSG Members	**1379**	976	978	786	635	370
Satellite Mem.	**2611**	1954	2039	1750	1150	710
Developers	**363,925**	272,358	218,286	185,316	141,175	67,950
Applications	**93,687**	69,039	58,739	41,157	28,243	3970
Avg SSG Age	**4.24**	4.28	4.13	4.32	4.49	5.32
SSG Avg of Avgs	**1.77 / 100**	1.4 / 100	1.95 / 100	1.99 / 100	1.02 / 100	1.13 / 100
Financials	**40**	26	19	17	12	4
ISVs	**32**	25	19	15	7	4
High Tech	**18**	14	13	10	7	2

LEARNING MORE

Resources

- THANK YOU

- Join the BSIMM Community today http://bsimm.com

http://www.cigital.com/~gem/writings

@cigitalgem