BSIMM7 Brings Science to Software Security

The seventh iteration of the Building Security In Maturity Model project is a tool you can use as a measuring stick for software security initiatives.

By now, you should have heard about the Building Security In Maturity Model (BSIMM) project, especially if you are a software security person. (No? A good place to start is by taking this software security quiz.) Maybe you've even downloaded a copy of your own to peruse (it's free under the Creative Commons license).

Either way, it's time to get a new copy, because BSIMM7 has just been released. Remember, because BSIMM is completely data driven, the BSIMM7 document is different than what you may have read in the past. That's how science goes.

In this short piece, we're going to focus on BSIMM7 facts and figures. The numbers are about real software security initiatives doing real work to secure the software that you use every day. This is no ephemeral top ten list from the bug parade. This is a set of facts about the real state of commercial software security on planet Earth.

Who is the BSIMM community anyway?

The BSIMM project is spearheaded by three co-authors (the same three who wrote this piece you're reading now). We are directly involved in gathering data in person from each of the BSIMM firms. The data we gather directly through observation describes the work of 95 software security initiatives, from firms including: Adobe, Aetna, ANDA, Autodesk, Axway, Bank of America, Betfair, BMO Financial Group, Black Knight Financial Services, Box, Canadian Imperial Bank of Commerce, Capital One, Cisco, Citigroup, Citizen's Bank, Comerica Bank, Cryptography Research, a division of Rambus, Dell EMC, Depository Trust & Clearing Corporation, Elavon, Ellucian, Epsilon, Experian, F-Secure, Fannie Mae, Fidelity, Freddie Mac, General Electric, Highmark Health Solutions, Horizon Healthcare Services, Inc., HP Fortify, HSBC, Independent Health, iPipeline, JPMorgan Chase & Co., Lenovo, LGE, LinkedIn, Marks and Spencer, McKesson, Morningstar, Navient, NetApp, NetSuite, Neustar, Nokia, NVIDIA, NXP Semiconductors N.V., Principal Financial Group, Qualcomm, Royal Bank of Canada, Siemens, Sony Mobile, Splunk, Symantec, Target, The Advisory Board, The Home Depot, The Vanguard Group, Trainline, U.S. Bank, Visa, Wells Fargo, and Zephyr Health.

Starting with BSIMM6, we lowered this data freshness threshold to 42 months. This requirement caused 26 firms to be removed from the BSIMM data, resulting in the BSIMM6 data set representing 78 firms. For BSIMM7, we removed 13 firms, resulting in a current data pool of 95 firms. As our study progresses, we intend to decrease the freshness window to 36 months to better align with business cycles.

What is the BSIMM?

The BSIMM is a measuring stick for software security. The best way to use the BSIMM is to compare and contrast your own initiative with the data contained in the model, which show what other organizations are doing. You can

then identify goals and objectives of your own and look to the BSIMM to determine which further activities make sense for you.

The BSIMM is not a software security methodology. To make this clear, consider that the BSIMM can be used to measure Microsoft's SDL, but it is by no means for the Microsoft SDL.

BSIMM by the numbers

This table shows how the BSIMM Project has grown over the years. Remember, software security initiatives are ongoing and not a fire-and-forget exercise.

BSIMM NUMBERS OVER TIME

	BSIMM7	BSIMM6	BSIMM-V	BSIMM4	BSIMM3	BSIMM2	BSIMM1
FIRMS	95	78	67	51	42	30	9
MEASUREMENTS	237	202	161	95	81	49	9
2ND MEASURES	30	26	21	13	11	0	0
3RD MEASURES	15	10	4	1	0	0	0
SSG MEMBERS	1,111	1,084	976	978	786	635	370
SATELLITE MEMBERS	3,595	2,111	1,954	2,039	1,750	1,150	710
DEVELOPERS	272,782	287,006	272,358	218,286	185,316	141,175	67,950
APPLICATIONS	87,244	69,750	69,039	58,739	41,157	28,243	3,970
AVG. SSG AGE (IN YRS.)	3.94	3.98	4.28	4.13	4.32	4.49	5.32
SSG AVG. OF AVGS	1.61/100	1.51/100	1.4/100	1.95/100	1.99/100	1.02/100	1.13/100
FINANCIAL SERVICES	42	33	26	19	17	12	4
ISVS	30	27	25	19	15	7	4
HEALTHCARE	15	10					
INTERNET OF THINGS	12	13					
CLOUD	15						
INSURANCE	10						

As you can see, at this stage of the game, BSIMM7 describes the work of 4,706 people working full-time in software security, directly impacting the security efforts of 272,782 developers. They have help from the "satellite," which is made up of developers, architects, and people in the organization directly engaged in and promoting software security, but not as full-time software security group (SSG) members.

Ever wonder how big your firm's SSG should be? We wonder also, but we do know how big the SSGs are at 95 firms. If we average all the ratios of SSG size to Development size, we get an "SSG average of averages" of 11.7 (median 5). The table below contains some additional interesting data.

Real-World Data (95 Firms)	
Initiative age	**Satellite size**
• Average: 3.94 years	• Average: 37.8
• Newest: 0.1	• Smallest: 0
• Oldest: 19	• Largest: 1,400
• Median: 2.5	• Median: 0
SSG size	**Development size**
• Average: 11.7	• Average: 2,871
• Smallest: 1	• Smallest: 20
• Largest: 130	• Largest: 35,000
• Median: 5	• Median: 900

The table on the following page shows just how many firms make use of each of the 113 activities in the BSIMM. Each activity has a label (like SM1.1) and is described in detail in the BSIMM7 report. See, it turns out we do know how to do software security! We even know who is doing what. Now what we need to do is spread adoption of software security to all firms creating software. You can help.

BSIMM7 SCORECARD

GOVERNANCE		INTELLIGENCE		SSDL TOUCHPOINTS		DEPLOYMENT	
ACTIVITY	OBSERVED	ACTIVITY	OBSERVED	ACTIVITY	OBSERVED	ACTIVITY	OBSERVED
[SM1.1]	47	[AM1.2]	63	[AA1.1]	81	[PT1.1]	82
[SM1.2]	48	[AM1.3]	34	[AA1.2]	29	[PT1.2]	58
[SM1.3]	46	[AM1.5]	48	[AA1.3]	23	[PT1.3]	54
[SM1.4]	81	[AM2.1]	8	[AA1.4]	47	[PT2.2]	21
[SM2.1]	41	[AM2.2]	8	[AA2.1]	15	[PT2.3]	16
[SM2.2]	35	[AM2.5]	13	[AA2.2]	12	[PT3.1]	10
[SM2.3]	33	[AM2.6]	9	[AA2.3]	5	[PT3.2]	6
[SM2.5]	19	[AM2.7]	9	[AA3.1]	4		
[SM2.6]	33	[AM3.1]	4	[AA3.2]	0		
[SM3.1]	14	[AM3.2]	2				
[SM3.2]	9						
[CP1.1]	56	[SFD1.1]	74	[CR1.2]	58	[SE1.1]	46
[CP1.2]	84	[SFD1.2]	65	[CR1.4]	63	[SE1.2]	78
[CP1.3]	50	[SFD2.1]	27	[CR1.5]	28	[SE2.2]	27
[CP2.1]	24	[SFD2.2]	40	[CR1.6]	34	[SE2.4]	24
[CP2.2]	31	[SFD3.1]	6	[CR2.5]	22	[SE3.2]	12
[CP2.3]	34	[SFD3.2]	10	[CR2.6]	15	[SE3.3]	3
[CP2.4]	36	[SFD3.3]	1	[CR2.7]	19	[SE3.4]	0
[CP2.5]	38			[CR3.2]	3		
[CP3.1]	19			[CR3.3]	2		
[CP3.2]	13			[CR3.4]	3		
[CP3.3]	5			[CR3.5]	5		
[T1.1]	69	[SR1.1]	60	[ST1.1]	78	[CMVM1.1]	82
[T1.5]	27	[SR1.2]	66	[ST1.3]	72	[CMVM1.2]	84
[T1.6]	17	[SR1.3]	64	[ST2.1]	22	[CMVM2.1]	69
[T1.7]	37	[SR2.2]	28	[ST2.4]	10	[CMVM2.2]	74
[T2.5]	13	[SR2.3]	22	[ST2.5]	7	[CMVM2.3]	41
[T2.6]	14	[SR2.4]	21	[ST2.6]	9	[CMVM3.1]	3
[T2.7]	5	[SR2.5]	22	[ST3.3]	4	[CMVM3.2]	5
[T3.1]	3	[SR2.6]	17	[ST3.4]	2	[CMVM3.3]	8
[T3.2]	5	[SR3.1]	8	[ST3.5]	4	[CMVM3.4]	6
[T3.3]	2	[SR3.2]	11				
[T3.4]	7						
[T3.5]	2						

How does your firm compare?

Here's what happens when you measure a new firm using the BSIMM measuring stick. You can directly compare how your software security initiative stacks up against the other 95 firms in BSIMM7.

Is your firm a financial services institution? Well, we can compare you to 42 other financial services firms. Are you an ISV? We can compare you directly to 30 other ISVs. BSIMM7 also marks the expansion of the healthcare industry with 15 firms. Measurement is a powerful tool that drives both budgets and improvement.

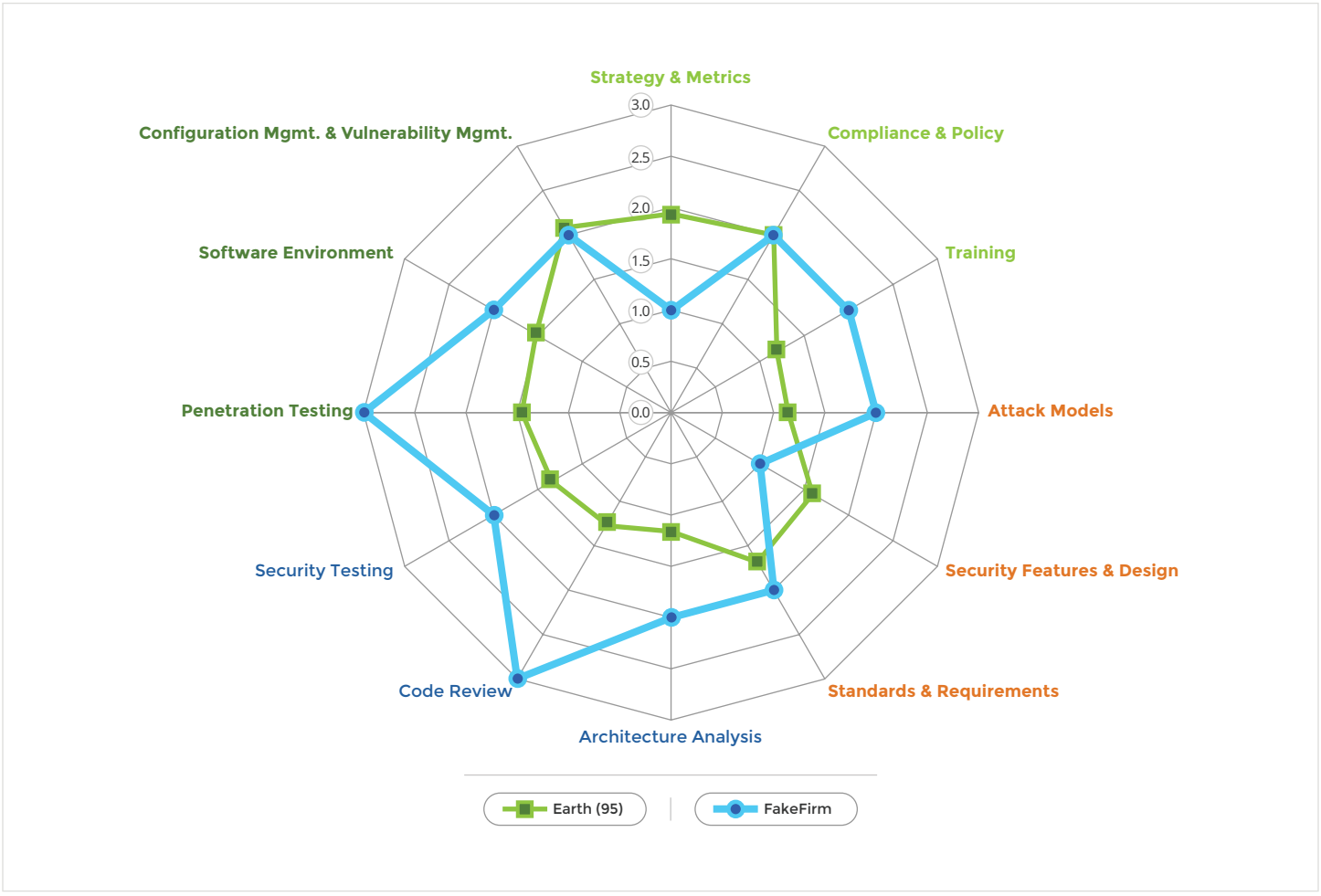
Nobody wants to be the slowest zebra in the zebra pack. Is your firm the slowest zebra? You can get your own scorecard like the one below and do some analysis to find out.

BSIMM7 SCORECARD FOR: FAKEFIRM | OBSERVATIONS: 37

GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM
STRATEGY & METRICS			ATTACK MODELS			ARCHITECTURE ANALYSIS			PENETRATION TESTING		
[SM1.1]	47	1	[AM1.2]	63		[AA1.1]	81	1	[PT1.1]	82	1
[SM1.2]	48		[AM1.3]	34		[AA1.2]	29	1	[PT1.2]	58	1
[SM1.3]	46	1	[AM1.5]	48	1	[AA1.3]	23	1	[PT1.3]	54	
[SM1.4]	81	1	[AM2.1]	8		[AA1.4]	47		[PT2.2]	21	1
[SM2.1]	41		[AM2.2]	8	1	[AA2.1]	15		[PT2.3]	16	
[SM2.2]	35		[AM2.5]	13	1	[AA2.2]	12	1	[PT3.1]	10	1
[SM2.3]	33		[AM2.6]	9	1	[AA2.3]	5		[PT3.2]	6	
[SM2.5]	19		[AM2.7]	9		[AA3.1]	4				
[SM2.6]	33		[AM3.1]	4		[AA3.2]	0				
[SM3.1]	14		[AM3.2]	2							
[SM3.2]	9										
COMPLIANCE & POLICY			SECURITY FEATURES & DESIGN			CODE REVIEW			SOFTWARE ENVIRONMENT		
[CP1.1]	56	1	[SFD1.1]	74		[CR1.2]	58	1	[SE1.1]	46	
[CP1.2]	84		[SFD1.2]	65	1	[CR1.4]	63	1	[SE1.2]	78	1
[CP1.3]	50	1	[SFD2.1]	27		[CR1.5]	28		[SE2.2]	27	1
[CP2.1]	24		[SFD2.2]	40		[CR1.6]	34	1	[SE2.4]	24	
[CP2.2]	31		[SFD3.1]	6		[CR2.5]	22		[SE3.2]	12	
[CP2.3]	34		[SFD3.2]	10		[CR2.6]	15		[SE3.3]	3	
[CP2.4]	36		[SFD3.3]	1		[CR2.7]	19		[SE3.4]	0	
[CP2.5]	38	1				[CR3.2]	3	1			
[CP3.1]	19					[CR3.3]	2				
[CP3.2]	13					[CR3.4]	3				
[CP3.3]	5					[CR3.5]	5				
TRAINING			STANDARDS & REQUIREMENTS			SECURITY TESTING			CONFIG. MGMT & VULN. MGMT		
[T1.1]	69	1	[SR1.1]	60	1	[ST1.1]	78	1	[CMVM1.1]	82	1
[T1.5]	27		[SR1.2]	66		[ST1.3]	72	1	[CMVM1.2]	84	

We also create a spider diagram, as shown below, as a way of visualizing a comparison based on 12 practices. The 113 activities in the model fit directly into the 12 practices.

SPIDER CHART FOR FAKE FIRM



Our spider-graph-yielding "high-water mark" approach (based on three levels per practice) is sufficient to get a low-resolution feel for maturity, especially when working with data from a particular vertical or geography.

One meaningful comparison is to chart your own firm's maturity high-water mark against the averages we have published to see how your initiative compares.

The BSIMM community

The 95 firms participating in BSIMM7 make up the BSIMM community. An exclusive online community with more than 400 members allows SSG leaders participating in the BSIMM to discuss solutions with others who face the same issues, discuss strategy with someone who has already addressed an issue, seek out mentors from those further along a career path, and band together to solve hard problems.

The BSIMM community also hosts annual private conferences in the United States and Europe where representatives from each firm gather together in an off-the-record forum to discuss software security initiatives. Become part of the community today and take advantage of these unique resources. The BSIMM website includes a

credentialed BSIMM community section where information from the conferences, working groups, and mailing-list-initiated studies are posted.

Would you like your firm to be included in the BSIMM community? Give us a shout. BSIMM7 is the latest snapshot of a growing and evolving set of real data about software security. The more data we have, the better off we all are. It's science time.

This was first published in October 2015.

Authors

Sammy Migues
Gary McGraw, Ph.D.
Jacob West

Want to know how your software security initiative stacks up against your peers? Go to www.BSIMM.com to learn more.