Security Fatigue? Shift Your Paradigm

Gary McGraw, *Cigital*

Software security is the fastest growing paradigm in the IT security field, and the Building Security in Maturity Model (BSIMM) project offers real-world measurements for assessment.

Computer security is currently all over the news, and mostly for all the wrong reasons. Retailers such as Target, Neiman Marcus, and Michaels have admitted exposing tens of millions of consumers' personal data, including credit card numbers and PINs, through poor computer security practices. We've learned that for years the NSA has been indiscriminately vacuuming up massive collections of data about American citizens by exploiting the inherent insecurity of mobile devices, email, and social media. A recent attack reveals the Internet of Things to be a collection of insecure devices plopped directly on the Net, naked (see "Hackers Conduct First Internet of Things Attack" in this issue's News Briefs). For all of the money spent on IT security to date, cybersecurity problems only seem to be growing. What is going on?

CONCERN OVER CURRENT SECURITY APPROACHES

In its 2014 CIO agenda report (www.gartner.com/imagesrv/cio/pdf/cio_agenda_insights2014.pdf), international tech advisory firm Gartner pointed out that CIOs are beginning to express serious concern over our current collective approach to computer security—the "cleanup on aisle seven" approach, as I like to call it, with a broad emphasis on network security and failed perimeter controls, followed immediately by forensics, system cleanup, and much hand wringing.

Since its earliest days, network security has focused on protecting the broken stuff from the bad guys by putting a "thing" in between the two (a firewall of some kind). Sadly, this method is failing. Simply put, the notion of real-time monitoring and blocking of network traffic is just as expensive as it is reactive, and it does not make much sense for massively distributed modern systems. All this has led to immensely entertaining news stories about "advanced persistent threats" and "insidious foreign spy rings" and the occasional "spectacular forensics investigation," but such press coverage merely revels in the computer security problem without pointing to solutions.

Fortunately, a relatively new paradigm in computer security—software security—promises some relief. What makes software security different is a focus on security engineering as systems are designed and constructed. The idea of "building security in" makes for technology that is, by design, harder to exploit and creates an economic situation that is much cheaper than "penetrate and patch."

But how quickly is this new paradigm catching on? And what measures are available to quantify software security?

GROWTH IN SOFTWARE SECURITY

Despite its reactive, "clean up on aisle seven" problems, IT security is growing at a steady clip. International Data Corporation (IDC), in its *Revenue by Segment and Revenue by Delivery Platform Breakdowns for 2010*, reports an 8.9 percent compound annual growth rate (CAGR) for IT security products. At Cigital, we estimate the 2013 worldwide

0018-9162/14/$31.00 © 2014 IEEE Published by the IEEE Computer Society

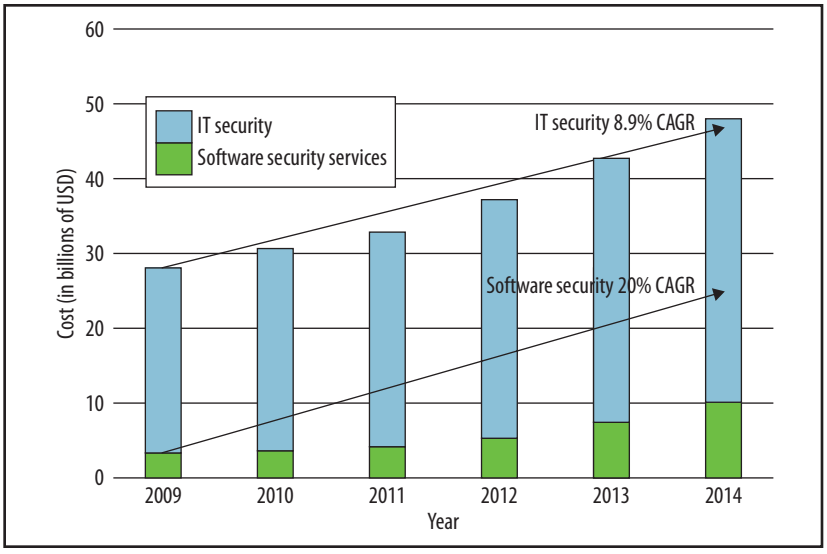

Figure 1. Growth in IT security versus growth in software security (sources: Cigital, IDC). CAGR, compound annual growth rate.

market for goods and services in IT security at somewhere between US$30 and $45 billion. Not bad in a world economy still in slow recovery from the Great Recession of 2009.

Software security, a submarket of IT security, is growing more than twice as fast, with a CAGR of 20 percent. And in 2013, the software security market accounted for approximately 10 percent of all IT security revenue, as Figure 1 illustrates.

If this kind of growth holds up, we can expect software security to play a much larger role in IT security in the future. In other words, the new paradigm *is* catching on—and quickly.

BSIMM: MEASURING SOFTWARE SECURITY THROUGH OBSERVATION

Five years ago, we initiated the Building Security in Maturity Model (BSIMM, pronounced "bee sim") project to measure and assess real-world software security protocols including Microsoft's Trustworthy Computing initiative. The idea was simple—describe through direct observation exactly what real firms are doing to build secure software. Collective data from the BSIMM, available for free under Creative Commons licenses, can be downloaded at http://bsimm.com.

The BSIMM project is spearheaded by scientists from Cigital and HP Fortify. We are directly involved in gathering data *in person*, through extensive interviews and artifact observation. The project has grown impressively since its inception and now receives input from the software security initiatives of 67 participating firms, including Adobe, Aetna, Bank of America, Box, Capital One, Citi, Comerica Bank, EMC, Epsilon, F-Secure, Fannie Mae, Fidelity, HSBC, Intel, Intuit, JPMorgan Chase & Co., Lender Processing Services Inc., Marks and Spencer, Mashery, McAfee, McKesson, Microsoft, NetSuite, Neustar, Nokia, Nokia Siemens Networks, PayPal, Pearson Learning Technologies, QUALCOMM, Rackspace, Salesforce, Sallie Mae, SAP, Sony Mobile, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, TomTom, Vanguard, Visa, VMware, Wells Fargo, and Zynga. Table 1 suggests the growth of the project; its most recent reporting, BSIMM-V, describes the work of 2,930 full-time software security professionals working directly with 272,358 developers.

It's important to understand that the BSIMM is a measuring stick for software security, not a software security methodology: the BSIMM can be used to measure Microsoft's software development lifecycle (SDL), for example, but it is by no means a replacement for the Microsoft SDL. The best way for IT security professionals to use the BSIMM is as a basis for comparison, to evaluate how their own company's software security initiative stacks up against those of the 67 firms in BSIMM-V using data in the model about what these other organizations are doing. They can then identify goals and objectives of their own and look to the BSIMM to determine which further activities make sense.

Is your firm a financial services institution? The BSIMM can directly compare your firm to 26 other financial services firms. Are you an independent software vendor (ISV)? The BSIMM can compare you directly to 25 other ISVs. Measurement is a powerful tool that drives both budgets and improvement.

Figure 2 shows a sample spider diagram we have created for purposes of "high water mark" measurement comparison. It suggests a way to visualize a low-resolution comparison between a hypothetical firm's software security maturity and the BSIMM community's collective measurement based on 12 software security practices described by the model. The 12 practices make up the 12 spokes in the spider diagram. (Note that 112 particular software security activities described in the model fit directly into these 12 practices. A high-resolution activities-based visualization is possible too.)

Among the current 67 participants of the BSIMM community, a moderated private mailing list made up of over 200 members allows participating software security group (SSG) leaders to discuss strategies and solutions with others who face or have already addressed the same issues,

Table 1. BSIMM by the numbers since the project's inception.					
	BSIMM1	BSIMM2	BSIMM3	BSIMM4	BSIMM-V
Firms	9	30	42	51	67
Measurements	9	49	81	95	161
Second measurements	0	0	11	13	21
Third measurements	0	0	0	1	4
Software security group (SSG) members	370	635	786	974	976
Satellite members	710	1,150	1,750	2,039	1,954
Developers	67,950	141,175	185,316	218,286	272,358
Applications	3,970	28,243	41,157	58,739	69,039
Average SSG age	5.32	4.49	4.32	4.13	4.28
SSG average of averages	1.13/100	1.02/100	1.99/100	1.95/100	1.4/100
Financials	4	12	17	19	26
Independent software vendors	4	7	15	19	25
High tech	2	7	10	13	14

seek out mentors from those farther along a career path, and band together to solve hard problems.

The BSIMM community also hosts annual private conferences where up to three representatives from member firms gather in an off-the-record forum to discuss software security initiatives. In fall 2013, more than 100 people from 35 firms participated in the fourth annual BSIMM Community Conference in Dulles, Virginia, and earlier that year, 10 of 15 firms with a presence in the EU participated in the second annual BSIMM Europe Community Conference in London.

We know that the fastest growing new paradigm in IT security is software security, and we know how to build and measure a software security initiative. Now we just need to do it. With the participation of security professionals, the BSIMM can help.

Gary McGraw is Cigital's chief technology officer. Contact him via Twitter @cigitalgem.

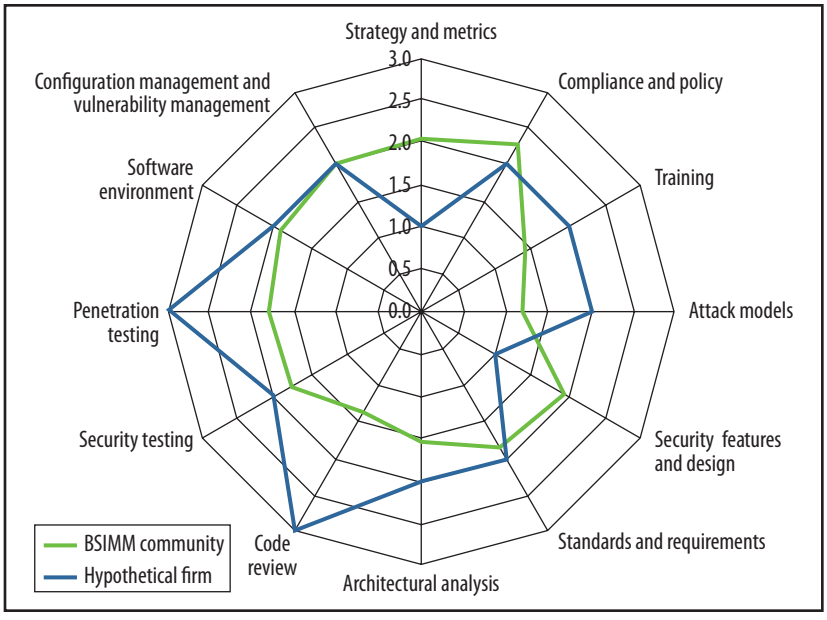

Figure 2. The BSIMM spider graph offers a "high water mark" measurement to provide firms with a low-resolution visualization of their software security maturity compared to that of the 67-firm BSIMM community.