SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Interpreting the BSIMM: A SAFECode Perspective on Leveraging Descriptive Software Security Initiatives

NOVEMBER 10, 2011

Introduction

As the practice of software security has matured, a number of new initiatives aimed at supporting its continued development have been undertaken. One such effort is the Building Security In Maturity Model (BSIMM), led by software security experts from Cigital, Inc., a software security consulting firm, and Fortify, an HP Company specializing in software security assurance tools.

There are a number of similarities between our work at the Software Assurance Forum for Excellence in Code (SAFECode) and the BSIMM effort. Both SAFECode and the BSIMM are focused on improving software security. Both have published documents[1] about software security practices that offer approaches to advancing secure software development. And both the SAFECode and BSIMM papers can be used as part of efforts to plan, implement and measure a software security program. Given these similarities, it is not surprising that there has been confusion about how to best interpret and apply the information provided by SAFECode and the BSIMM.

To address this confusion, this paper aims to clarify similarities and differences between the SAFECode and BSIMM papers. It offers guidance for software security practitioners on how to use each document for its appropriate purpose.

SAFECode's Fundamental Secure Development Practices

SAFECode's *Fundamental Practices for Secure Software Development* paper is currently in its second edition and represents an ongoing, collaborative effort by SAFECode to identify secure development activities that have been shown to be effective at improving software security in real-world implementations by SAFECode members. The goal of the Fundamental Practices paper is to help other development organizations initiate or improve their own software security programs and to encourage the industry-wide adoption of secure development methods.

[1] Fundamental Practices for Secure Software Development 2nd Edition: A Guide to the Most Effective Secure Development Practices in Use Today; Feb. 8, 2011; http://www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf

Building Security In Maturity Model (BSIMM3); September 2011; http://www.bsimm.com/download/

To develop this *Fundamental Practices* paper, SAFECode member companies conducted an intensive analysis of existing security development practices in their organizations. These analyses recorded the security activities in use during all phases of the software development lifecycle. SAFECode then used subjective and objective data to identify a foundational set of secure development practices that were not only common across its members, but also demonstrated a positive impact on efforts to improve software security. As noted in the paper, these practices have proven to be both effective and implementable even when different product requirements and development methodologies are taken into account.

SAFECode's *Fundamental Practices* paper not only offers implementation advice, but also describes methods and tools for verifying that development teams correctly followed prescribed security practices. This is an area of continuing work for SAFECode.

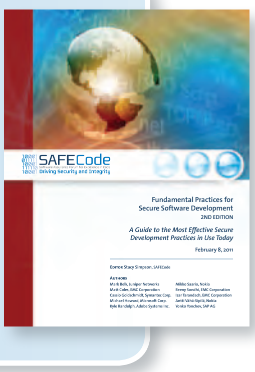
Building Security In Maturity Model

The Building Security In Maturity Model (BSIMM) is an inventory of existing security practices from over 40 large-scale, IT dependent organizations across seven business vertical categories. The BSIMM team has recently published its third update to the BSIMM – incorporating more inventory data from a larger set of organizations.

The BSIMM consists of 109 different activities grouped into four major categories: Governance, Intelligence, SSDL Touchpoints and Deployment. These categories encompass a broad spectrum of activities within an enterprise, including corporate strategy, internal marketing, standards and regulatory compliance, design and development and post-development operational security.

Fundamental Practices for Secure Software Development 2nd Edition: A Guide to the Most Effective Secure Development Practices in Use Today

www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf



10001
011111
10001
111110
10001 SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Fundamental Practices for
Secure Software Development
2ND EDITION

A Guide to the Most Effective Secure
Development Practices in Use Today

February 8, 2011

EDITOR Stacy Simpson, SAFECode

AUTHORS

Mark Belk, Juniper Networks	Mikko Saario, Nokia
Matt Coles, EMC Corporation	Reeny Sondhi, EMC Corporation
Cassio Goldschmidt, Symantec Corp.	Izar Tarandach, EMC Corporation
Michael Howard, Microsoft Corp.	Antti Vähä-Sipilä, Nokia
Kyle Randolph, Adobe Systems Inc.	Yonko Yonchev, SAP AG

The BSIMM was created by a team of software security professionals from Cigital and Fortify who conducted interviews at the 42 participating organizations using a common framework and scorecard approach.

Prescriptive vs. Descriptive Models of Security

Both the SAFECode *Fundamental Practices* paper and the BSIMM focus on secure development methodologies; however, there are important differences in their respective approaches and conclusions.

SAFECode has chosen a prescriptive approach that emphasizes the use of security practices and techniques that have proven to be effective at each of the SAFECode member organizations. It makes deliberate value judgments regarding security practices and prioritizes those that were recognized by SAFECode member experts as having the most impact – regardless of organization size, resources or computing platform.

The BSIMM employs a descriptive approach to development security and does not (by design) seek to measure the effectiveness of security processes.

Its authors' intention is simply to observe and report on the frequency of use of particular security practices within a set of firms – and thus allow readers to form their own conclusions about what constitutes effective security development practice. The BSIMM process can be characterized as a "second order metric" – it doesn't measure the result (e.g., more secure software), but rather the process. In the words of its authors, BSIMM "is useful for comparing software security activities observed in a target firm to those activities observed among the thirty [40] firms (or various subsets of the thirty [40] firms)."[2]

The BSIMM's open ended "here's what everybody else is doing" approach may help organizations identify blank spots in their development security landscape or assist them in picking activities, while the SAFECode *Fundamental Practices* paper offers detailed advice on recommended security practices for software design, coding and testing.

Selection of Secure Software Development Practices

Threats to software have been increasing over the last two decades and stories of exploited software and computing systems are all too common. Generally speaking, business and technical decision makers in IT organizations understand the need for secure software development. Thus, there is an increasing demand for practical guidance on how to implement software security.

As noted above, there is no right or wrong answer regarding which approach to use. However, given the differences in the two models (prescriptive and descriptive), it is useful to clearly illustrate their intended goals to allow organizations and individuals to form their own conclusions about applicability.

Choosing the Right Stuff

SAFECode is composed of technology providers and thus our recommendations and efforts speak from a provider perspective and focus on the needs of similar organizations and their customers. In this spirit, it is important to note that SAFECode is focused on secure development best practices. In contrast, the BSIMM participants span a number of industry verticals beyond technology providers, such as financial services, media and energy firms, and the BSIMM covers a much broader range of IT security practice areas beyond secure software development.

While some of the development activities in the BSIMM inventory may be applicable in organizations of varying business sector and size, there are a significant number of observed activities that are realistic only within the confines of a large enterprise, or that are not part of software development activities.

Being the result of real-world observations, the BSIMM provides an organizational "snapshot in time" of the most and least common practices in use today. Unfortunately, the adoption of specific practices is often driven by compliance and regulation, not risk. For example, the BSIMM's Compliance and Policy (CP) activities are among the twelve groups with the highest observed average. CP 1.1 is related to regulatory or compliance drivers such as FFIEC, GLBA, OCC, PCI DSS, SOX, SAS 70, HIPAA and others. CP 1.2 is related to personally identifiable information (PII) obligations. Relying on policy to ensure software assurance is not a fool-proof

[2] *InformIT,* "Software [In]security: BSIMM3"; Gary McGraw, Brian Chess, Sammy Migues; Sept. 27, 2011; http://www.informit.com/articles/article.aspx?p=1755416

solution. In fact, companies may race to become compliant, but not necessarily secure, if they choose to emulate the most observed BSIMM activities.

Thus, a strict adoption of the practices that the BSIMM reports as most prevalent would not address what SAFECode considers the root cause of the problem: poor secure coding practices. In fact, comparing the most commonly practiced activities reported by the BSIMM against what SAFECode believes to be core security activities shows almost a perfect inverse relation. While SAFECode members are well represented in the BSIMM data, none of the SAFECode members uses the BSIMM as an arbiter of proper security development practice.

Finally, in contrast to the SAFECode approach, the BSIMM lacks comprehensive verification requirements – to ensure that security activities have been correctly and comprehensively implemented.

Historical Versus Emerging Practices

Neither SAFECode nor the BSIMM makes statements about what practice is most important or which practices an organization should adopt first. In fact, SAFECode members have found that the importance of practices tends to shift over time as a security initiative matures.

Security tools, processes and defense mechanisms constantly become outdated and are replaced by updated practices. Prescriptive documents tend to

Strengths and Weaknesses of SAFECode and the BSIMM

SAFECode

Strengths

- Focused on technology providers
- Emphasis on preventing software vulnerabilities, not meeting compliance requirements
- Manageable set of real-world practices shown to get results

Weaknesses

- Focused on technology providers
- Narrower set of guidance
- Recommendations based largely on qualitative experience

BSIMM

Strengths

- Diverse set of 40 companies surveyed
- Covers a broad set of practice areas beyond secure engineering
- Provides quantifiable data on current state of practice

Weaknesses

- Weighted toward compliance and general security activities as opposed to preventing software vulnerabilities
- Lacks identification of verification activities
- Emphasis on scoring can lead readers to treat list of activities as a checklist
- Reports on frequency of activities performed, not the effectiveness of those practices
- May not reflect emerging best practices
- Some activities only make sense within very large enterprises

highlight these trends and put more emphasis on such shifts. The BSIMM will capture these changes, but recognition of such changes can only be achieved using historical data. SAFECode companies in many cases are in the forefront of application security. Some of the practices employed by this group and are both leading edge and uncommon, such as having an entire department dedicated to security research. Some other practices conducted within SAFECode members are not even part of the BSIMM framework yet. With time, the successful practices tend to become industry best practices and may eventually result in changes to the BSIMM framework.

SAFECode Members and the BSIMM

Not all organizations need to achieve the same level of security. However, since SAFECode represents leading technology providers that provide software to millions of users, its guidance is supported by the significant software security efforts undertaken by each of its members, many of which are on the leading edge of software security program development. While SAFECode believes the BSIMM's limitations reduce its ability to serve as an accurate measurement tool, it did compare its participating members to the larger BSIMM community to see what the existing data revealed. The average score of the six SAFECode members that participated in the BSIMM either matches or exceeds the BSIMM score of the top 10 participants in all but one of the 12 BSIMM domains. This "SAFECode Index" (the average of all SAFECode practices) is probably an indicator of the depth of real-world experience SAFECode members bring to the organization's guidance and may provide some insight into the effectiveness of prescriptive approaches to software security.

Summary

Practitioners involved in the creation of a software security initiative will find value from both the SAFECode guidance and the BSIMM when reviewing or selecting their security processes. Both papers make positive contributions to the ongoing effort to improve software security.

The prescriptive and detailed nature of SAFECode publications provides a better starting point for implementation. In addition, SAFECode's second edition of *Fundamental Practices for Secure Software Development* offers ways for practitioners to verify that development organizations are actually following the provided security guidance.

The BSIMM provides data across a broader range of practice areas that are largely outside the core focus of security and development professionals. Further, its quantitative approach is useful for organizations wishing to see how their approach aligns with the rest of their industry.

While both SAFECode and the BSIMM take different approaches, their work should be viewed as complementary and not conflicting. SAFECode's technology provider-focused, prescriptive approach supports software security practitioners by providing a blueprint for engineering best practices for software security. The BSIMM's descriptive approach provides the software security practitioner with a non-judgmental lens into a broad spectrum of security activities whose scope extends beyond software development security, across a broad spectrum of organizations.

PRIMARY AUTHORS

Cassio Goldschmidt, Symantec Corp.
Frank Koehntopp, SAP AG
David Ladd, Microsoft Corporation
Niall O'Donoghue, Nokia
Kyle Randolph, Adobe Systems Incorporated
Stacy Simpson, SAFECode
Reeny Sondhi, EMC Corporation

CONTRIBUTORS

Brad Arkin, Adobe Systems Incorporated
Eric Baize, EMC Corporation
Gunter Bitz, SAP AG
Robert Dix, Juniper Networks, Inc.
Marc French, EMC Corporation
Steve Lipner, Microsoft Corporation
Frances Paulisch, Siemens AG
Gary Phillips, Symantec Corp.
Janne Uusilehto, Nokia

About SAFECode

The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Its members include Adobe Systems Incorporated, EMC Corporation, Juniper Networks, Inc., Microsoft Corporation, Nokia, SAP AG, Siemens AG and Symantec Corp.

For more information, please visit www.safecode.org.

Product and service names mentioned herein are the trademarks of their respective owners.

SAFECode
2101 Wilson Boulevard Suite 1000
Arlington, VA 22201
(p) 703.812.9199 (f) 703.812.9350
stacy.simpson@goodharbor.net
www.safecode.org