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

# Software Assurance Forum for Excellence in Code

Stacy Simpson
March 1, 2011

# Challenge

Individual companies are implementing better methods for developing and delivering more secure software, hardware and services

BUT

Industry lacked a common framework or trusted forum to advance or share these efforts

# Who We Are

The Software Assurance Forum for Excellence in Code (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

Juniper® NETWORKS

symantec™

Microsoft®

NOKIA

SAP®

Adobe®

EMC² ® where information lives®

# Mission

## SAFECode’s Mission

As a center of excellence for vendor software assurance practices, SAFECode unites subject matter experts with unparalleled experience in managing complex global processes for software sourcing, development and delivery to:

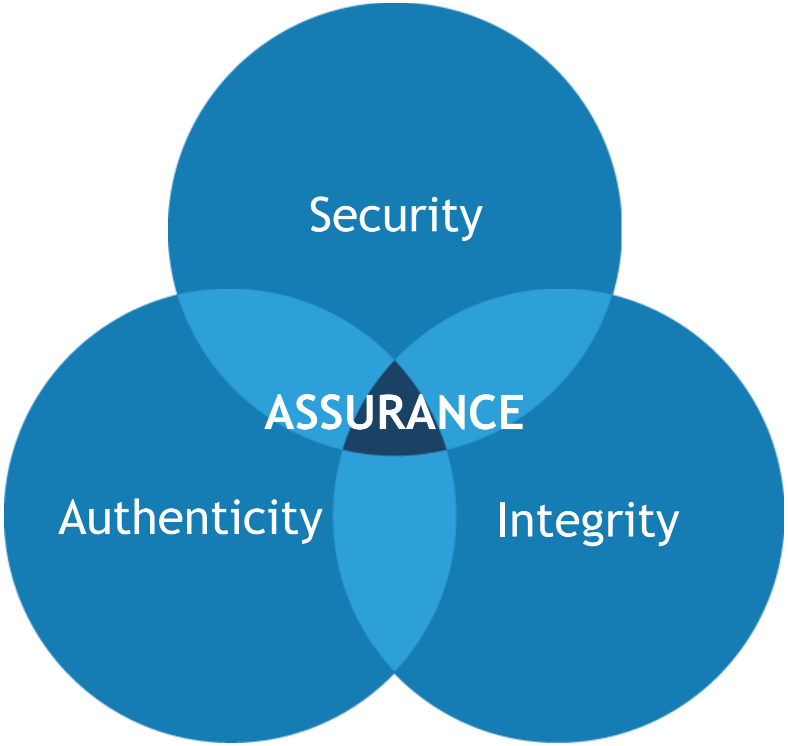
1. Foster a trusted exchange of insights that advance software assurance practices
2. Encourage broad industry adoption of proven software security, integrity and authenticity practices
3. Drive clarity for customers and other key stakeholders on vendor software assurance practices to help empower them to better manage risk

10001 01111 10001 11110 10001 SAFECode Software Assurance Forum for Excellence in Code Driving Security and Integrity

# SAFECode's View of Software Assurance

**Software Assurance:** Confidence that software, hardware and services are free from intentional and unintentional vulnerabilities and that the software functions as intended.

In practice, software vendors take action in three key, overlapping areas to achieve software assurance—security, authenticity and integrity.



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

# Our Work to Date

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

Fundamental Practices for
Secure Software Development

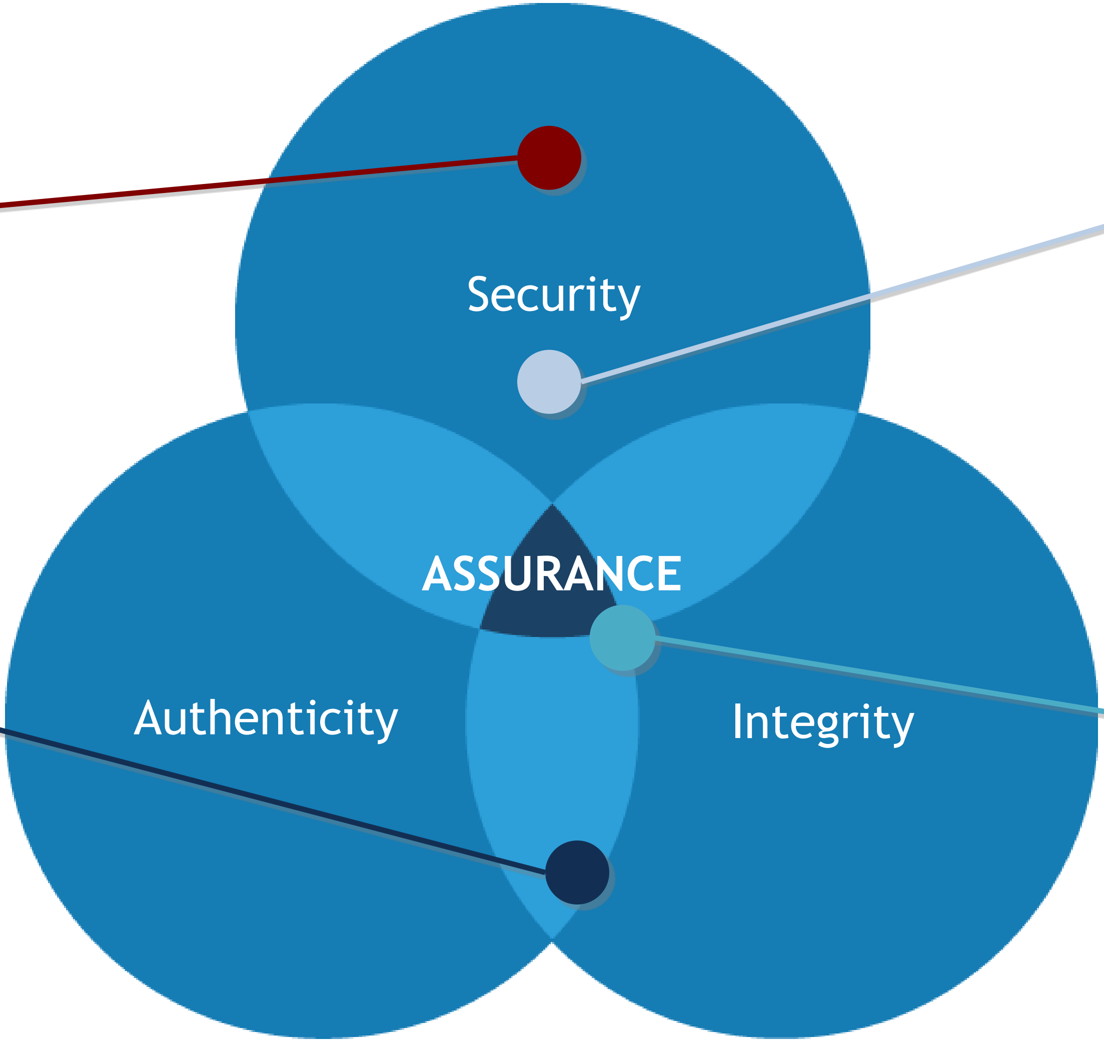
*A Guide to the Most Effective Secure
Development Practices in Use Today*

OCTOBER 8, 2008

EDITOR Stacy Simpson, SAFECode

CONTRIBUTORS
Gunter Bitz, SAP AG
Jerry Cochran, Microsoft Corp.
Matt Coles, EMC Corporation
Danny Dhillon, EMC Corporation
Chris Fagan, Microsoft Corp.
Cassio Goldschmidt, Symantec Corp.
Wesley Higaki, Symantec Corp.
Michael Howard, Microsoft Corp.
Steve Lipner, Microsoft Corp.
Brad Minnis, Juniper Networks, Inc.
Hardik Parekh, EMC Corporation
Dan Reddy, EMC Corporation
Alexandr Seleznyov, Nokia
Reeny Sondhi, EMC Corporation
Janne Uusilehto, Nokia
Antti Vähä-Sipilä, Nokia

Secure Software
Development



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

Security Engineering Training

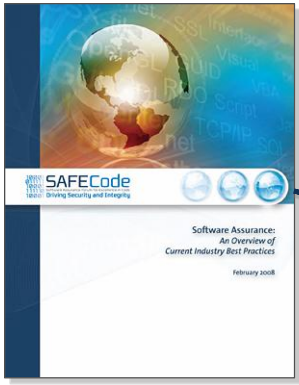
*A Framework for Corporate
Training Programs on the Principles
of Secure Software Development*

April 20, 2009

EDITOR Stacy Simpson, SAFECode

CONTRIBUTORS
Eric Baize, EMC Corporation
Reeny Sondhi, EMC Corporation
Hardik Parekh, EMC Corporation
Dan Reddy, EMC Corporation
Brad Minnis, Juniper Networks, Inc.
Bernie Rosen, Juniper Networks, Inc.
Michael Howard, Microsoft, Corp.
Steve Lipner, Microsoft Corp.
Glenn Pittaway, Microsoft Corp.
Antti Vähä-Sipilä, Nokia
Cassio Goldschmidt, Symantec Corp.
Wesley Higaki, Symantec Corp.
Paul Kurtz, SAFECode

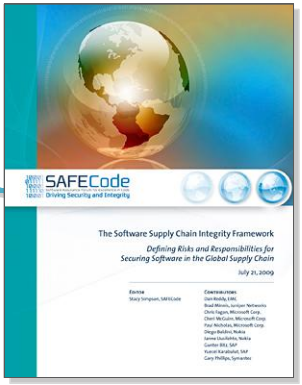
Training


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

Software Assurance:
*An Overview of
Current Industry Best Practices*

February 2008

Software Integrity
Controls


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

The Software Supply Chain Integrity Framework

*Defining Risks and Responsibilities for
Securing Software in the Global Supply Chain*

July 21, 2009

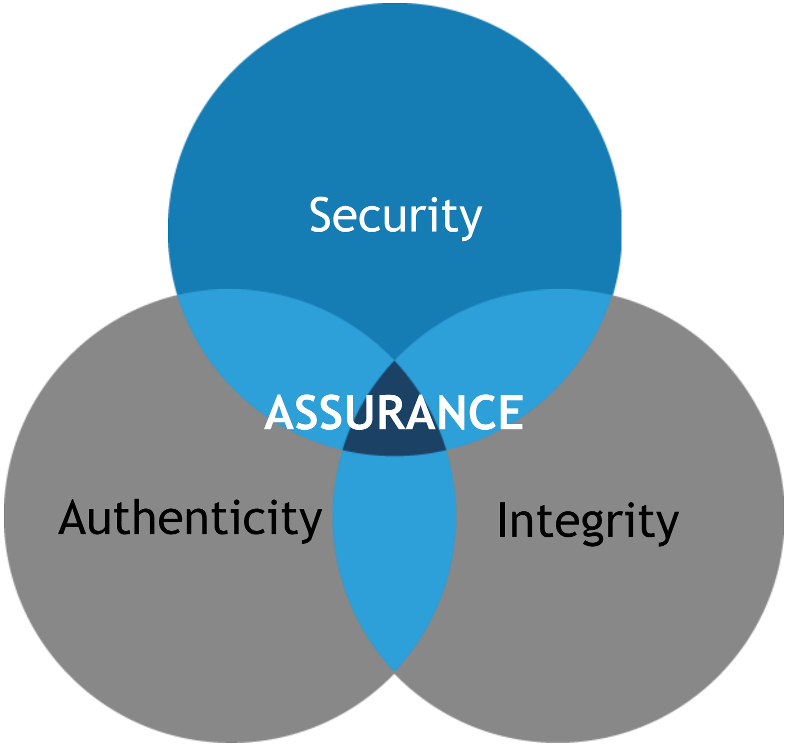
EDITOR
Stacy Simpson, SAFECode

CONTRIBUTORS
Dan Reddy, EMC
Brad Minnis, Juniper Networks
Chris Fagan, Microsoft Corp.
Cheri McGuire, Microsoft Corp.
Paul Nicholas, Microsoft Corp.
Diego Baldini, Nokia
Janne Uusilehto, Nokia
Gunter Bitz, SAP
Yuecel Karabulut, SAP
Gary Phillips, Symantec

Software Integrity
Framework

# Software Assurance: Security

**Security:** Security threats to the software are anticipated and addressed during the software's design, development and testing through secure engineering practices. This requires a focus on code quality and functional requirements to reduce unintentional vulnerabilities in the code.



# Latest Release

Download Today
at
www.safecode.org

- *“Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices in Use Today”*
- The 2nd Edition is here!

# Key Authors

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

# What’s New

- What’s New?
  - It grew from 19 pages to 51 pages!
  - Refined focus to design, development and testing
  - Expanded and updated the guidance and references
  - Added Common Weakness Enumeration (CWE) references
  - Added Verification guidance

# Secure Design Principles

- Secure Design Principles
  - ➢ Threat Modeling
  - ➢ Use Least Privilege
  - ➢ Implement Sandboxing

# Secure Coding Practices

- Secure Coding Practices
  - Minimize Use of Unsafe String and Buffer Functions
  - Validate Input and Output to Mitigate Common Vulnerabilities
  - Use Robust Integer Operations for Dynamic Memory Allocations and Array Offsets
  - Use Anti-Cross Site Scripting (XSS) Libraries
  - Use Canonical Data Formats
  - Avoid String Concatenation for Dynamic SQL Statements
  - Eliminate Weak Cryptography
  - Use Logging and Tracing

# Testing Recommendations

- Testing Recommendations
  - ➢ Determine Attack Surface
  - ➢ Use Appropriate Testing Tools
  - ➢ Perform Fuzz / Robustness Testing
  - ➢ Perform Penetration Testing

# Technology Recommendations

- Technology Recommendations
  - ➢ Use a Current Compiler Toolset
  - ➢ Use Static Analysis Tools

# What’s Next

- What’s Next
  - Community Feedback!
  - Expand – What do you want to know more about?
  - Visit www.safecode.org