

10001
01111
10001
11110
10001

SAFECode

Software Assurance Forum for Excellence in Code
Driving Security and Integrity

An Overview of SAFECode & Best Practices for Secure Development

Wes Higaki (whigaki@symantec.com)

Michael Howard (mikehow@microsoft.com)

Why the Focus on Software Assurance?

- As the global dependence on ICT has grown, users have become increasingly concerned over its integrity, security and reliability
- The need to reduce vulnerabilities, improve resistance to attack, and protect supply chain integrity has never been more important than in today's increasingly complex and dynamic threat environment
- There is a growing desire to know more about the processes used to design, engineer, develop and deliver software/hardware/services

Managing the threats we face today in cyberspace requires a layered system of security...

- Vendors building more secure software
- Integrators ensuring that the software is installed correctly
- Operators maintaining the system properly
- End users using the products in a safe and secure manner

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

- 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 effort

- The Software Assurance Forum for Excellence in Code (SAFECode) was announced on 23rd October 2007
- SAFECode is the first global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services

- SAFECode unites subject matter experts with unparalleled experience in managing complex global processes for software development, integrity controls and supply chain security.
- The goal is not to establish one way but to identify methods that work and can be effectively leveraged in a rational way by governments and enterprises.



- Increase understanding of the secure development methods and integrity controls used by vendors
- Promote proven software assurance practices among vendors and customers to foster a more trusted ecosystem
- Identify opportunities to leverage vendor software assurance practices to better manage enterprise risks
- Foster essential university curriculum changes needed to support the cyber ecosystem
- Catalyze action on key research and development initiatives in the area of software assurance

- Vendors who have implemented these best practices have seen dramatic improvements in software product assurance and security
- SAFECode encourages software developers and vendors to consider, tailor and adopt these practices into their own development environments
- High-level best practices provide a solid foundation, but more work to be done

Strong Development Processes:

- Developers implement processes that are demonstrated to be effective at improving security
- Developers have a clear roadmap for beginning the process of building robust software assurance programs

- Individual companies need to commit to software assurance best practices at every level of their organization
- Industry needs to lead effort to build upon positive work of individual companies and promote and advance the art of software assurance
- SAFECode is one forum for subject matter experts to come together to identify different approaches that have been proven to work and to help address gaps where new practices might be needed

Fundamental Practices for Secure Software Development

What is the Paper?

- It's short!
 - Only 22 pages
- A list of fundamental practices in use by SAFECode members
- A highly practical and actionable document
- Not an academic research document
- Software development process agnostic

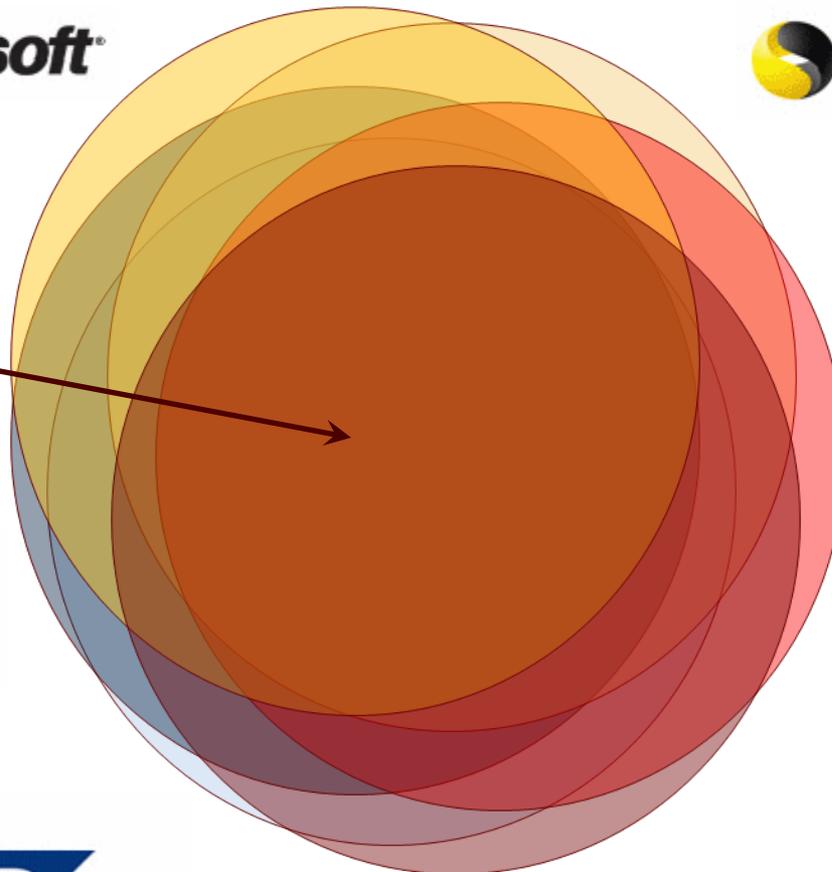
10001
01111
10001
11111
10001

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

An Industry Consensus Document

Microsoft

 **symantec.**



NOKIA

EMC²
where information lives[®]

SAP

 **Juniper**
NETWORKS



**Fundamental Practices for
Secure Software Development**
A Guide to the Most Effective Secure
Development Practices in Use Today
OCTOBER 8, 2008

Lead Writer: Michael Howard, Microsoft Corp.
Contributors:
Aron Bruch, SAP
Andrew Chiles, Microsoft Corp.
Mark Clary, SAP Corporation
Henry DeMa, SAP Corporation
Chris Egner, Microsoft Corp.
Gordon Gammeter, Symantec Corp.
Wally Hight, Symantec Corp.
Steve Jones, Microsoft Corp.
John Kester, Symantec Corp.
Mark Kettle, SAP Corporation
Dan Kish, SAP Corporation
Michael Longenecker
Steve Madsen, SAP Corporation
Steve Ouellette, SAP
Andreas Lipp, SAP

- Implemented SAFECode member practices that fit into the “rhythm of the business”
- Each section includes explanation and references for secure development during:
 - Design
 - Programming
 - Testing
 - Code Integrity and Handling
 - Documentation
- Education and Response/Updates intentionally left out

- “Threat analysis,” “risk analysis,” “threat modeling”
- Some members use “misuse cases”
- Basic knowledge of Saltzer and Schroeder

- Minimize unsafe function use
- Use the latest compiler toolset
- Use static and dynamic analysis tools
- Manual code review
- Validate input and output
- Use anti-cross site scripting libraries
- Use canonical data formats
- Avoid string concatenation for dynamic SQL
- Eliminate weak cryptography.
- Use logging and tracing

- Fuzz Testing
- Penetration Testing
- Third-party Assessment
- Automated Test Tools

- Protect source code with strong authentication and access control
 - Protect source at rest and while in transit
- Least privilege access
- Establish code chain of custody throughout lifecycle
- Audit, monitor, analyze
- Verify and sign final code
- Resolve security vulnerabilities promptly

- Describe deployment security practices
- Secure configuration
 - Ports
 - Firewall settings
 - OS changes
- Minimally a set of security “Do’s and Don’ts”

- It's a short, readable document
- A pragmatic list of “practiced practices” in use by SAFECode members

Questions ???

SAFECode Contact:

Paul Kurtz, Executive Director

Paul@safecode.org

+ 1 703-812-9199

www.safecode.org

SAFECode.org is a comprehensive online resource for news and information about software assurance.

SAFECode members include EMC Corporation, Juniper Networks, Inc., Microsoft Corp., Nokia, SAP AG, and Symantec Corp.

10001
01111
10001
11110
10001

SAFECode

Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SAFECode members:

