

Media Contact:
Stacy Simpson
+ 1 703 926 1963
stacy@safecode.org

FOR IMMEDIATE RELEASE

SAFECode Outlines Current Industry Best Practices for Software Assurance

New report aims to increase understanding and adoption of the most effective secure development methods and integrity controls used by technology vendors

Arlington, Va. – Feb. 13, 2008 – The Software Assurance Forum for Excellence in Code (SAFECode), a non-profit organization exclusively dedicated to increasing trust in information technology (IT) products and services through the advancement of effective software assurance methods, today released its first member report, *Software Assurance: An Overview of Current Industry Best Practices*. The report outlines the secure development methods and integrity controls currently used by SAFECode members to deliver high-assurance systems to government and commercial customers. SAFECode members include EMC Corporation, Juniper Networks, Inc., Microsoft Corp., SAP AG and Symantec Corp.

“Software assurance is a vital component to ensuring the security of critical information technology resources, and information and communications technology vendors thus have an obligation to address assurance through every stage of application development,” said Paul Kurtz, executive director of SAFECode. “As the initial step in our efforts to help the industry meet this important responsibility, SAFECode has identified the assurance best practices that have proven to be effective across its member companies. By sharing this information, we hope to encourage the adoption of these types of practices by other software developers and respond to the growing customer desire for greater visibility into the steps technology vendors are taking to continually improve the security of their products.”

Software development processes vary by vendor according to their unique organizational structures and customer requirements. Yet regardless of the methods used, there is a core set of best practices for software assurance and security that apply to diverse development environments. The paper identifies and explains the following security best practices and controls that are currently in use by SAFECode members:

- **Security Training:** A prerequisite to coding secure software is for engineers to be knowledgeable about information security issues that may affect people who use the product.
- **Defining Security Requirements:** Security requirements must be defined during the early stages of product development.
- **Secure Design:** The early design phase must identify and address potential threats to the application and ways to reduce those risks to a negligible level.
- **Secure Coding:** The product development team must implement secure programming practices.
- **Secure Source Code Handling:** The integrity and confidentiality of source code must be protected.
- **Security Testing:** Specialized validation should be implemented to ensure that security requirements and secure design and coding guidelines were followed.
- **Security Documentation:** Documentation for users should include explicit treatment of security issues to help customers understand how to optimally configure security controls, and how configuration options may or may not develop potential security vulnerabilities.

- **Security Readiness:** Prior to releasing a product, the application developer must evaluate, document and assess risks posed by potential security gaps in the product.
- **Security Response:** Any security vulnerabilities (exploited or not) reported against the deployed product should be handled through incident response mechanisms and relayed to the product development or sustaining teams to mitigate the vulnerability.
- **Integrity Verification:** Products must offer customers methods to verify that the software they have acquired is indeed from their trusted vendor.
- **Security Research:** Ongoing research should be conducted into new threat vectors and mechanisms to mitigate them.
- **Security Evangelism:** Leaders in the area of software assurance should promote the use of best practices by discussing their practices and findings in open forums, articles, papers and books.

“Vendors who have implemented these best practices have seen dramatic improvements in software product assurance and security,” said Kurtz. “We encourage all software developers and vendors to consider, tailor and adopt these practices into their own development environments. The result of efforts like these will be a higher level of end-user confidence in the quality and safety of software that underpins critical operations in governments, critical infrastructure and businesses worldwide.”

In the coming months, SAFECode will issue a number of reports building on these high-level best practices to offer specific and actionable information on the key concepts, principles, and research and development activities the organization is pursuing to improve software assurance and security.

A full copy of *Software Assurance: An Overview of Current Industry Best Practices* is available for download at http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf. The paper also includes eight important questions that organizations should ask vendors during the procurement process to help evaluate the software assurance of products or vendor engagements.

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. Founded by EMC Corporation, Juniper Networks, Inc., Microsoft Corp., SAP AG and Symantec Corp., SAFECode works to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Membership in SAFECode is open to information and communications technology vendors with significant global business activity in technology products such as hardware, software and services who have demonstrated a commitment and dedicated resources to software assurance. For more information, please visit www.safecode.org.

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

###