

Media Contact:

Stacy Simpson
Policy and Communications Director
SAFECode
703-812-9199
stacy@safecode.org

FOR IMMEDIATE RELEASE**SAFECode Releases First Industry-Developed Guidance on Software Integrity Controls**

New Report Outlines Assurance-Based Approach to Securing the Software Supply Chain

Arlington, Va. – June 14, 2010 – The Software Assurance Forum for Excellence in Code (SAFECode), 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, today released “*Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain.*” The new report provides actionable recommendations for minimizing the risk of vulnerabilities being inserted into a software product during its sourcing, development and distribution. The paper was jointly developed by SAFECode’s members, which include Adobe Systems Incorporated, EMC Corporation, Juniper Networks, Inc., Microsoft Corp., Nokia, SAP AG and Symantec Corp., and is based upon an analysis of the real-world actions these companies take to secure their supply chain processes.

“Software assurance is most commonly discussed in terms of security engineering, or in other words, building security into the software as it is being developed. However, another important aspect of assurance is securing the supply chain processes for software sourcing, development and distribution to protect the integrity of delivered software,” said Paul Kurtz, executive director of SAFECode. “SAFECode’s latest paper addresses this emerging area of assurance and represents the first industry-led effort to identify and analyze the software integrity controls used by software vendors to protect software from the insertion of vulnerabilities as it moves along the global supply chain.”

The software integrity controls identified in the paper are used by major software vendors to address the risk that insecure processes, or a motivated attacker, could undermine the security of a software product as it moves through the links in the global supply chain. The controls aim to preserve the quality of securely developed code by securing the processes used to source, develop, deliver and sustain software. The controls identified in the report cover issues ranging from contractual relationships with suppliers, to securing source code repositories, to helping customers confirm the software they receive is not counterfeit. The work builds upon SAFECode’s previously released “[Software Supply Chain Integrity Framework](#),” which defines a taxonomy for describing supply chain security in the context of software assurance.

“By basing our analysis on the actual practices and controls being used by SAFECode members today, we were able to identify software integrity controls that are not only effective, but also practical, repeatable and verifiable,” said Gunter Bitz, Head of Product Security Governance at SAP and a key contributor to the report. “We believe that broad industry adoption of software integrity controls can greatly improve customer confidence in IT systems. To help achieve this goal, SAFECode encourages other producers and distributors of software to tailor and adopt these controls into their own supply chain processes, as well as continue future study and analysis on additional methods to improve software integrity.”

The paper also identifies areas that SAFECode believes deserve future industry-led collaboration and study. The ideas proposed include improved supplier management and communications along the supply chain, additional research on software testing, and the development of effective strategies for software assurance measurement. To continue the discussion, SAFECode encourages public comment on this paper and will consider feedback collected for future projects. To comment, please visit www.safecode.org.

“Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain” is available for free download at www.safecode.org.

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 Corp., Nokia, SAP 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.

###