SAFECODE UNVEILS SOFTWARE BEST PRACTICES FOR THREAT MODELING AND THIRD PARTY COMPONENTS WHITE PAPERS

Developers and threat modelers can more effectively assess and defend against risk by leveraging the papers' guidance on vulnerability types and best practice mitigation methods

Wakefield, Mass. – May 10, 2017 – The Software Assurance Forum for Excellence in Code (SAFECode) today announced the release of two papers that provide software developers and security professionals with clear and actionable recommendations for threat modeling as a fundamental part of the software development process and for using third party components safely. The newly published papers Managing Security Risks Inherent in the Use of Third-party Components and SAFECode Tactical Threat Modeling provide guidance and real-world examples from which any size organization can implement a comprehensive software security strategy.

- Read Managing Security Risks Inherent in the Use of Third-party Components White Paper
- Download SAFECode Tactical Threat Modeling White Paper
- Learn more about SAFECode with this :90 second video

"It is almost impossible for software developers and security professionals – on their own - to keep up with the rapid changes in the threat environment and the security protocols required for effective defense," said Eric Baize, chairman, SAFECode. "SAFECode has gathered the best recommendations from the collective experience and expertise of its members and the larger community. These papers embody some of these efforts, providing the industry improved

methods to enhance trust in software. This work represents the experience and expertise of the SAFECode practitioner members."

Jointly developed by SAFECode members, the papers are grounded in an extensive analysis of the proven best practices that SAFECode member and large customer organizations actually follow in their day-to-day software assurance efforts.

"The main focus of the papers is helping organizations build, deliver, and sustain secure software" said Steve Lipner, executive director, SAFECode. "The threat modeling paper will help organizations achieve security at the design level, and the third party component paper helps combine security with the efficiency gained by using externally developed components."

For third party components, Managing Security Risks Inherent in the Use of Third-party Components paper breaks down the process and procedures developers need to test, improve and quantify the security of third party components:

"Third party components can be a very cost-effective approach to building capability fast, but they are also a source of risk to developers who don't consider the security implications of shipping and supporting such components. The new SAFECode paper provides guidance on what developers should be thinking about as they adopt third-party components," said Lipner.

Threat modeling, a key technique for architecting and designing systems securely, is a method that many SAFECode members employ. Leveraging SAFECode members' insights, the SAFECode Tactical Threat Modeling paper offers effective ways to better integrate threat modeling and provides a great resource for organizations that are looking to integrate threat modeling into their own development processes and teams.

In addition to the new papers, SAFECode offers developers free online training material based on the experience and in-house training developed by SAFECode members.

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, CA Technologies, Dell EMC Corporation, Intel Corporation, Microsoft Corp., Siemens AG and Symantec Corp. For more information, please visit www.safecode.org.

###