Keynote Talk

Software Security: Is OK Good Enough?

John B. Dickson, CISSP
Denim Group, Ltd.
San Antonio, Texas USA
john@denimgroup.com

Abstract

Widely publicized breaches regularly occur involving insecure software. This is due to the fact that the vast majority of software in use today was not designed to withstand attacks encountered when deployed on hostile networks such as the Internet. What limited vulnerability statistics that exist confirm that most modern software includes coding flaws and design errors that put sensitive customer data at risk. Unfortunately, security officers and software project owners still struggle to justify investment to build secure software. Initial efforts to build justification models have not been embraced beyond the most security conscious organizations. Concepts like the "Rugged Software" are gaining traction, but have yet to make a deep impact. How does an organization – short of a breach – justify expending critical resources to build more secure software? Is it realistic to believe that an industry-driven solution such as the Payment Card Industry's Data Security Standard (PCI-DSS) can drive secure software investment before headlines prompt government to demand top-down regulation to "fix" the security of software?

This presentation will attempt to characterize the current landscape of software security from the perspective of a practitioner who regularly works with Fortune 500 chief security officers to build business cases for software security initiatives. Given the current status of software security efforts, and the struggles for business justification, industry would be well-served to look further afield to other competing models to identify future justification efforts. There is still much that can be learned from models outside the security and information technology fields. For example, the history of food safety provides lessons that the software security industry can draw from when developing justification models. We can also learn from building code adoption by earthquake-prone communities and draw comparisons to communities that have less rigorous building codes. Finally, we can learn much from certain financial regulations that have or have not improved confidence in our financial system.

Categories & Subject Descriptors: Economics, Human Factors, Management, Measurement, Security, Standardization.

General Terms: Management, Measurement, Documentation, Design, Economics, Reliability, Security, Human Factors, Standardization, Theory, Legal Aspects, Verification.

Bio

John Dickson, CISSP, has over 15 years in the information security field including hands-on experience with intrusion detection systems, telephony security, and application security in the commercial and government sectors. In his current position as a Principal at Denim Group, he helps Chief Security Officers of Fortune 500 clients and Federal organizations launch successful software initiatives. John is a member of the US Space Command Commander's Group, the Founders Council, Institute for Cyber Security Studies, University of Texas at San Antonio, and is President Elect of the Texas Lyceum, a statewide leadership group in the State of Texas.

CODASPY'11, February 21–23, 2011, San Antonio, Texas, USA.
ACM 978-1-4503-0465-8/11/02.