Empirical Software Security Assurance

Dave Harper

Fortify Software, USA
dharper@fortify.com

By now everyone knows that security must be built in to software; it cannot be bolted on. For more than a decade, scientists, visionaries, and pundits have put forth a multitude of techniques and methodologies for building secure software, but there has been little to recommend one approach over another or to define the boundary between ideas that merely look good on paper and ideas that actually get results. The alchemists and wizards have put on a good show, but it's time to look at the real empirical evidence.

This talk examines software security assurance as it is practiced today. We will discuss popular methodologies and then, based on in-depth interviews with leading enterprises such as Adobe, EMC, Google, Microsoft, QUALCOMM, Wells Fargo, and Depository Trust Clearing Corporation (DTCC), we present a set of benchmarks for developing and growing an enterprise-wide software security initiative, including but not limited to integration into the software development lifecycle (SDLC). While all initiatives are unique, we find that the leaders share a tremendous amount of common ground and wrestle with many of the same problems. Their lessons can be applied in order to build a new effort from scratch or to expand the reach of existing security capabilities.

C. Serrão, V. Aguilera, and F. Cerullo (Eds.): IBWAS 2009, CCIS 72, p. 11, 2010.