Configuring Software and Systems for Defense-in-Depth

Trent Jaeger
The Pennsylvania State University

Abstract

The computer security community has long advocated *defense in depth*, building multiple layers of defense to protect a system. Realizing this vision is not yet practical, as software often ships with inadequate defenses, typically developed in an ad hoc fashion. Currently, programmers reason about security manually and lack tools to validate assurance that security controls provide satisfactory defenses. In this keynote talk, I will discuss how achieving defense in depth has a significant component in configuration. In particular, we advocate configuring security requirements for various layers of software defenses (e.g., privilege separation, authorization, and auditing) and generating software and systems defenses that implement such configurations (mostly) automatically. I will focus mainly on the challenge of retrofitting software with authorization code automatically to demonstrate the configuration problems faced by the community, and discuss how we may leverage these lessons to configuring software and systems for defense in depth.

CCS Concepts

• Security and Privacy → Software and Application Security - *Software Security Engineering*

Keywords

Defense in depth; Security configuration; Software security; Systems security

Short Bio

Trent Jaeger is a Professor of Computer Science and Engineering at The Pennsylvania State University and Co-Director of the Systems and Internet Infrastructure Security (SIIS) Lab. He specializes in systems and software security research.

SafeConfig'16, October 24, 2016, Vienna, Austria.
ACM ISBN 978-1-4503-4566-8/16/10.
DOI: http://dx.doi.org/10.1145/2994475.2994483