Title:
Quantifying Systemic Dependencies Through Attack Surface Analysis

Authors:
Eric Osterweil Verisign Labs eosterweil@verisign.com Danny McPherson Verisign Labs
dmcpherson@verisign.com Lixia Zhang UCLA lixia@cs.ucla.edu

Abstract:
To systematically address the increasing security threats of today's networked systems, one important step is to quantify the potential vulnerabilities a system may face. The concept of "attack surface" has emerged in recent years as a measure of such vulnerabilities. However given the high degrees of interdependencies among networked systems, it remains an open challenge of how to systematically identify and quantify the attack surface of a given system.

In this work we use two real Internet systems, the X.509 CA verification system and DANE, a newly standardized alternative solution, as case studies to showcase a novel methodology that offers a repeatable way to systematically quantify their attack surfaces. We believe this work represents the first step towards systemically modeling dependencies of actual Internet-scale systems in order to formally quantify the often elusive notion of a system's attack surface.