Scargos: Towards automatic distribution of zero-day vulnerabilities

Florian Rhinow (Author) — Michael Clear (Supervisor)

M.Sc. in Computer Science (Networks and Distributed Systems)
Trinity College, University of Dublin

Abstract

Information about vulnerabilities spread too slow and allow for a significant attack window during which applications are virtually unprotected. Zero-day attacks jeopardise the security of any IT-system due to the lack of an effective remedy. Recent work has suggested automated approaches to vulnerability distribution, but are limited to memory-corruption detection techniques and disallow custom vulnerability response processes. We present Scargos, a novel approach to automate the distribution and verification of vulnerabilities, while allowing for automatic, custom countermeasures without the need to trust a central authority. By leveraging collaborative detection, vulnerabilities can be contributed by anybody and are announced to an open network by using packet-based self-certifying alerts (SCA), which are a proof of existence of a vulnerability by capturing the original, unmodified attack.

We compare two ways to generate and verify an attack: brute-force replay and exact stream replay. After successful verification, SCAs allow for a custom vulnerability response process such as generating automatic malware analysis reports or IDS signatures.

We evaluate Scargos with 24 real-world attacks, and show that for all detected attacks, we can generate and verify packet-based SCAs inexpensively and accurately. Scargos performs better for bigger SCA file sizes than previously proposed mechanisms. We show that our approach allows for detection of previously unknown attacks, whereas an entire life cycle including distribution and verification is achieved on average in under 2 seconds. While vulnerability distribution is at present mainly done manually, often reaching end-users after several hours, Scargos reduces the available attack window of adversaries to a minimum.

August 29, 2013