Master thesis : Distributed Logging Transport for Unreliable and Lossy Networks

Auteur : Scheer, Egon
Promoteur(s) : Leduc, Guy; 12788
Faculté : Faculté des Sciences appliquées
Diplôme : Master en sciences informatiques, à finalité spécialisée en "computer systems security"
Année académique : 2021-2022
URI/URL : http://hdl.handle.net/2268.2/16294

Distributed Logging Transport for Unreliable and Lossy Networks

Egon Scheer

School of Engineering and Computer Science
University of Liège

A thesis submitted for the degree of
Master of Science in Computer Science with a professional focus on
"Computer systems security"

Supervised by Prof. G. Leduc & E. Tychon

Academic year 2021-2022

Abstract

Message logging is the tool of choice to stay informed about the health of a machine or application. These messages, called logs, are used for various purposes, including system management, performance optimization, investigation of suspicious activities, and more generally analysis and debugging. Operations that demand a level of reliability at least equivalent to the emphasis placed on them during their use. However, the syslog protocol was originally designed to work exclusively over UDP. Traditional applications, which have not benefited from the a postorio additions such as TCP, are forced to communicate over a network that is not suitable for them (corrupted or lost messages, reordering, or unreachable server) and over which they have no control. The objective of this work is to develop a resilient syslog relay that will operate downstream of applications, collect their syslog messages and send them to a central syslog server. Several mechanisms such as the use of the TCP protocol and the retention of messages in case of connection loss guarantee reliability. Topics related to message ordering and strategies in case of an overload are also discussed and several approaches are presented to either mitigate or regulate their impact. The implementation, in the form of a prototype, is deployed inside a router running the Cisco IOx environment and features the modern syslog message engine, *rsyslog.* The model is evaluated on the basis of its functionality and performance in a test environment with network quality such as 3G cellular and EDGE. Several configurations are proposed depending on the type of usage involved. Although the solution does not cover all possible and imaginable problems, such as router outages, the evaluations demonstrate the efficiency and scalability of the proposed solution, which can for example easily handle several tens of thousands of messages per second with a very low resource footprint.