Online and Offline Security Policy Assessment

Title	Online and Offline Security Policy Assessment
Publication Type	Conference Paper
Year of Publication	2016
Authors	Valenza, Fulvio, Vallini, Marco, Lioy, Antonio
Conference Name	Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats
Publisher	ACM
Conference Location	New York, NY, USA
ISBN Number	978-1-4503-4571-2
Keywords	configuration analysis, Human Behavior, policy assessment, policy verification, pubcrawl, Resiliency, Scalability, Security Policies Analysis

Abstract

Network architectures and applications are becoming increasingly complex. Several approaches to automatically enforce configurations on devices, applications and services have been proposed, such as Policy-Based Network Management (PBNM). However, the management of enforced configurations in production environments (e.g. data center) is a crucial and complex task. For example, updates on firewall configuration to change a set of rules. Although this task is fundamental for complex systems, few effective solutions have been proposed for monitoring and managing enforced configurations. This work proposes a novel approach to monitor and manage enforced configurations in production environments. The main contributions of this paper are a formal model to identify/ generate traffic flows and to verify the enforced configurations; and a slim and transparent framework to perform the policy assessment. We have implemented and validated our approach in a virtual environment in order to evaluate different scenarios. The results demonstrate that the prototype is effective and has good performance, therefore our model can be effectively used to analyse several types of IT infrastructures. A further interesting result is that our approach is complementary to PBNM.

URL	http://doi.acm.org/10.1145/2995959.2995970
DOI	10.1145/2995959.2995970

Citation Key valenza_online_2016

configuration analysis Human behavior policy verification policy assessment pubcrawl Resiliency Scalability Security Policies Analysis