Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Distributed security policy conformance

Mirko Montanari[*], *Ellick Chan, Kevin Larson, Wucherl Yoo, Roy H. Campbell*

Department of Computer Science, University of Illinois at Urbana-Champaign, USA

ARTICLE INFO

Article history:
Received 6 March 2012
Received in revised form
27 October 2012
Accepted 12 November 2012

Keywords:
Security
Monitoring
Policy compliance
Policy analysis
Vulnerability analysis
Monitoring integrity

ABSTRACT

Security policy conformance is a crucial issue in large-scale critical cyber-infrastructure. The complexity of these systems, insider attacks, and the possible speed of an attack on a system necessitate an automated approach to assure a basic level of protection.

This paper presents Odessa, a resilient system for monitoring and validating compliance of networked systems to complex policies. To manage the scale of infrastructure systems and to avoid single points of failure or attack, Odessa distributes policy validation across many network nodes. Partial delegation enables the validation of component policies and of liveness at the edge nodes of the network using redundancy to increase security. Redundant distributed servers aggregate data to validate more complex policies. Our practical implementation of Odessa resists Byzantine failure of monitoring using an architecture that significantly increases scalability and attack resistance.

1. Introduction

Security management and policy compliance are critical issues in modern infrastructure systems. Regulatory and security organizations introduce policies and best practices to raise the minimal level of security required for power grid systems, government systems, and airport systems. We have studied industrial security policies (NIST, 2009; NERC, 2007) that have complex challenging compliance and auditing concerns at the network level at the scale of the system concerned. Manual attempts to audit these systems are tedious, error prone, and potentially vulnerable to insider attacks or credential theft. Therefore a more principled solution to this problem is required.

The formalization of security policies and the use of hardened automated systems that validate compliance can improve the quality and efficiency of this auditing process. Although previous approaches analyzed the representation of these policies (Anwar and Campbell, 2009) and described centralized systems for collecting network information and analyzing it (Jajodia and Noel, 2010; Narain et al., 2008), neither has adequately addressed the issue of scaling to networks of thousands of nodes or of resilience to attacks.

To address these issues, we have implemented and evaluated our policy compliance monitoring system Odessa. Our approach addresses the scaling problem by decomposing policies and distributing the validation process. Each of the complex rules that define the compliant and non-compliant states of the system is decomposed into local components and an aggregate component. We securely delegate the validation of local components to secure agents installed on hosts. These agents are able to reliably monitor the state of the system using virtual machine introspection. Using this information, we partition the validation of aggregate components across several distributed servers. Resilience toward attacks aimed at compromising the validation process uses Byzantine

[*] *Corresponding author.*
E-mail addresses: mmontan2@illinois.edu (M. Montanari), emchan@illinois.edu (E. Chan), klarson5@illinois.edu (K. Larson), wyoo5@illinois.edu (W. Yoo), rhc@illinois.edu (R.H. Campbell).

0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.11.007

failure resistant, redundant information acquisition employing multiple agents and independent critical policy validation in multiple server style monitors.

The contributions of this paper include:

1.An algorithm for determining which portion of each policy can be validated on devices.
2.A resilient tree-based architecture that distributes to multiple servers the validation of the aggregate components of the policies and that delegates to several hosts the load of monitoring for the liveness of each device.
3.An evaluation of the scalability of our solution.

The rest of the paper is structured as follows. Section 2 describes related work in the area. Section 3 defines policy compliance and presents several examples of policies. Section 4 describes the Odessa architecture. Section 5 presents our algorithm for distributing policy evaluation. Section 6 describes our experimental evaluation. Finally, Section 7 summarizes our contributions and results.

2. Related work

Research in access control and in network management addresses problems related to policy compliance monitoring. However, the techniques we present in this paper are unique and suited for monitoring compliance to industrial security policies.

In the area of access control, research in policy compliance monitoring has been focusing on formalizing access control policies defined by regulations such as HIPAA (Lam et al., 2009), or on providing mechanisms for verifying the compliance of a set of access control actions to such policies (e.g., (Garg et al., 2011)). Our work focuses on a complementary set of policies related to network management that are present in most recent regulations such as NERC CIP (NERC, 2007), FISMA (United State Government, 2002), and PCI-DSS (Payment Card Industry Security Standards Council, 2010). Monitoring for compliance to such policies presents a different set of challenges. While access control events can be found generally in a few centralized logs, in our setting the information used in the compliance validation process is distributed across a large number of systems. Our approach provides specific techniques such as the distribution of the validation of compliance and the distributed check for liveness that are suited for such a scenario. Additionally, previous work did not address the problem of the security of the monitoring process.

In the area of network management, several agent-based systems have been introduced for monitoring the security configurations of systems. NetQuery (Shieh et al., 2011) and the DMTF Web Based Enterprise Management (WBEM) framework (Distributed Management Task Force, 2012) provide a unified view of the configuration of a system and create notifications in case of changes in the state. Additionally, in the context of MANETs, previous work introduced an abstract framework for guiding the interactions between agents for managing security policies (Workman et al., 2008). However, none of these approaches provide automatic methods for distributing the evaluation of policies or decentralized mechanisms for detecting the failure of hosts.

Other non-agent based systems have been proposed for performing specific security assessments. Network scanners and security assessment tools such as TVA (Jajodia and Noel, 2010), or MulVAL (Ou et al., 2006) acquire information about the configuration of the system by using port scans or direct access to hosts. These systems have several limitations. First, changes to host configurations are detected with considerable delay because of the polling approach. Second, their architecture is centralized: the evaluation of policy compliance is performed in a central host. For very large networks, this can become both a bottleneck and a vulnerability as a single supervisory node audits, monitors, and checks remote operations that may impact integrity. ConfigAssure (Narain et al., 2008) takes a top–down approach and synthesizes network configurations from high-level specifications. However, the top–down approach is not always applicable, as the organizational network is often managed by different divisions and it is not always possible to centralize the control into a single entity. Other work addressed the problem of providing suitable ontologies for the representation of security information and network management data (dos Santos Moreira et al., 2008). The problem we address in this work is complementary to such issues: we focus on the process of monitoring the data required for validating such policies at runtime.

Ontology-based systems for network management and security have been the subject of previous work. In particular, KAoS (Uszok et al., 2004) introduced an ontology-based mechanism for enforcing access-control policies in a distributed setting. The goal of such policies is to restrict access to a set of distributed resources, and the check of the policies is performed upon an access request. The policies we consider are more general and their goal is to ensure that the state of a system is compliant to policies at any point in time. Additionally, our approach focuses on distributing the processing of information about policies to a large number of devices, and on a distributed architecture for maintaining the ability of monitoring the system in the case of failures and attacks.

Distributed analysis of Datalog rules has been studied in the area of Deductive Databases (see Ramakrishnan and Ullman (1995) for a survey). However, previous work analyzed the general case of active databases where statements and rules can be processed on any machine on the network. In contrast, our approach uses specific knowledge about the physical location of statements and rules to distribute the computation. Additionally, we address the problem of the security of the monitoring process and we provide monitoring for liveness.

3. Policy compliance

Policy compliance is a basic security and regulatory requirement for infrastructure systems. Although policy compliance cannot guarantee security, it still offers a minimal level of assurance against attacks that would be avoidable had proper security measures been taken. These policies can be specified as constraints created from regulatory requirements, or from the formalization of organization-specific security requirements. Policies are often posed as high-level specifications,