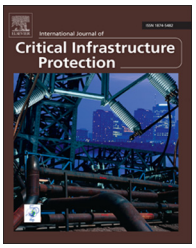
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



# A novel security information and event management system for enhancing cyber security in a hydroelectric dam

Cesario Di Sarno[a,*], Alessia Garofalo[b], Ilaria Matteucci[c], Marco Vallini[d]

[a]Department of Engineering, University of Naples "Parthenope," Centro Direzionale Isola C4, 80143 Naples, Italy
[b]Computer Science Research Group (COSIRE), 81031 Aversa, Italy
[c]Institute for Informatics and Telematics, National Research Council (CNR), via Giuseppe Moruzzi 1, 56124 Pisa, Italy
[d]Department of Control and Computer Engineering, Polytechnic University of Turin, Corso Duca degli Abruzzi 24, 10129 Turin, Italy

ARTICLE INFO

*Article history:*
Received 15 April 2015
Received in revised form
11 February 2016
Accepted 29 February 2016
Available online 18 March 2016

*Keywords:*
Security information and event management (SIEM) Systems
Decision support systems
Resilient event storage
Hydroelectric dam

ABSTRACT

Security information and event management (SIEM) systems are increasingly used to cope with the security challenges involved in critical infrastructure protection. However, these systems have several limitations. This paper describes an enhanced security information and event management system that (i) resolves conflicts between security policies; (ii) discovers unauthorized network data paths and appropriately reconfigures network devices; and (iii) provides an intrusion- and fault-tolerant storage system that ensures the integrity and non-forgeability of stored events. The performance of the enhanced system is demonstrated using a case study involving a hydroelectric dam. The case study considers an attack model that affects portions of the information technology infrastructure of the hydroelectric dam and demonstrates that the security information and event management system is successfully able to detect and respond to attacks.



## 1. Introduction

The U.S. Department of Homeland Security [20] defines the critical infrastructure as "assets, systems and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." The protection of critical infrastructures is a priority to avoid disasters that could affect government, industry and society. President Obama's Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21) of 2013 [15] identifies 16 critical infrastructures that must be monitored and protected. The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has noted that the energy sector, which includes hydroelectric dams, is one of the most attractive targets for cyber attacks. In 2013, the media reported that U.S. intelligence agencies traced a compromise of the U.S. Army Corps of Engineers National Inventory of Dams (NID) to Chinese government or military entities [8]. The compromised database stored vulnerabilities of major dams that could be exploited in future cyber attacks against the U.S. electric power grid.

*Corresponding author.
E-mail address: cesario.disarno@uniparthenope.it (C. Di Sarno).

http://dx.doi.org/10.1016/j.ijcip.2016.03.002
1874-5482/

Security information and event management (SIEM) systems are an emerging technology that can significantly enhance critical infrastructure protection. These systems are designed to analyze security information from the monitored infrastructures to discover security breaches. Existing SIEM systems lack several important features such as the abilities to detect and resolve conflicts between security policies, to identify and control network data paths existing in the monitored infrastructures and to securely store data while ensuring its integrity and non-forgeability.

This paper describes an enhanced SIEM system that overcomes these limitations by integrating a decision support system and a resilient event storage system. The enhanced system is customized for a specific critical infrastructure, namely a hydroelectric dam. An attack model that affects various portions of the information technology infrastructure of the hydroelectric dam is employed to demonstrate that the SIEM system can significantly enhance the cyber security of the monitored dam infrastructure.

## 2. SIEM systems

SIEM systems are widely used to perform real-time monitoring and control of critical infrastructure assets. A SIEM system integrates two formerly heterogeneous systems – a security information management (SIM) system and a security event management (SEM) system [3]. A security information management system focuses on the analysis of historical data to improve the long-term effectiveness and efficiency of cyber security mechanisms [21]. A security event management system, on the other hand, aggregates data into a manageable amount of information to enable the rapid handling of security incidents [21].

SIEM technology aggregates event data produced by security devices, network infrastructures and information technology systems and applications. The data fed to a SIEM system comprise log entries generated by devices and components installed within the monitored infrastructure (e.g., routers, servers and applications). Several protocols (e.g., Syslog, SNMP and OPSEC) are available for transferring log entries from data sources to a SIEM system. If a device or component does not support such a protocol, then an "agent" is required to translate (or normalize) the log data to a format that is recognized by a SIEM system. Also, an agent may provide filtering functionality to prevent irrelevant data from being sent to a SIEM system, helping reduce network bandwidth, storage space and SIEM processing resources. The task of distinguishing useful data from irrelevant data in a SIEM application is an important, albeit challenging, task.

Each agent outputs events that contain relevant data. The events are sent to a correlator that performs complex security analysis using attack signatures. If an attack is detected, the correlator generates an alarm containing information about the security breach. The events and alarms are saved in a storage system. A Gartner report [14] provides an overview of SIEM technologies; two of the most widely used SIEM systems are OSSIM and Prelude.

SIEM systems have three principal weaknesses when used in critical infrastructure protection applications:

- Critical infrastructure protection invariably involves the implementation of multiple – and conflicting – security policies. However, while SIEM systems permit the definition of security policies, they often do not provide mechanisms for resolving policy conflicts.
  A search of the literature reveals that several researchers have proposed conflict resolution strategies and mechanisms. Matteucci et al. [12] have developed a conflict resolution strategy based on the prioritization of the most specific privacy policies customized for the e-health domain. Cuppens et al. [5] employ an OrBAC methodology to manage conflicts involving permissions and prohibitions. Lupu and Sloman [10] define and review policy conflicts, discuss precedence relationships that enable inconsistent policies to coexist and present a conflict analysis tool that is part of a role-based management framework. Syukur et al. [19] have investigated policy conflict resolution in pervasive environments using standard strategies such as role hierarchy overrides and obligation precedence. Masoumzadeh et al. [11] consider attributes related to subjects, objects and environments, grouping them under a unique context; a conflict resolution strategy is then used to prioritize authorization rules according to the specificity of the context as a whole. Dunlop et al. [7] present four strategies for solving conflicts based on the evaluation of the role of the requester. Unfortunately, while all these conflict resolution approaches show promise, none of them has been integrated in a SIEM architecture.
- Critical infrastructure monitoring is performed by deploying communication networks that enable the exchange of information between the monitored facilities and the control system. In order to control connections between external networks and internal networks, security policies that place strong limitations on data flows are established. For example, sensor firmware updates can only be performed by specific hosts located in an authorized local-area network that has privileged accounts and limits access to trusted employees. Current SIEM systems are unable to identify and control all possible data paths existing in a monitored infrastructure. The OSSIM SIEM system, for example, allows certain actions for controlling a monitored scenario, such as sending an email containing an alarm to the system administrator or executing a specific command.
  Network reachability analysis is required to identifying allowed and disallowed traffic between network entities. Over the years, several dynamic approaches (e.g., using network tools such as `ping`) and static approaches (e.g., using router and firewall configurations) have been proposed. Some approaches rely on graph-based representations to model the routing and filtering features of computer networks. Xie et al. [22] have proposed a unified model for analyzing static reachability based on two views: (i) a graph that describes the physical network topology, where the nodes are routers and the edges are network links and (ii) a graph that models the routing process, where the nodes are routing processes and the edges are adjacencies that implement a routing policy. The composition of these views makes it possible to evaluate reachability by combining routing policies that govern the