Security Information Management for Enclave Networks (SIMEN)

Authors
Rosalie M. McQuaid, Principal Investigator
William Heinbockel
Joseph Judge
Peter Kertzner
Brian Soby
The MITRE Corporation, United States

Security Topics:
Enterprise Security
Intrusion detection and event correlation
Security management

Abstract

Ideal Information Assurance (IA) requires enterprise-wide collection and feeds of security data, often to a centralized, SIM-enabled monitoring location. Timely focused event collection and the processing of security data is a challenge where bandwidth is constrained, connectivity is limited or intermittent, and where high volumes of data occur in rapidly changing environments.

The Security Information Management for Enclave Networks (SIMEN) research project is focused on the challenges associated with the ineffective collection of security event messages and the inefficient transport of such events to a centralized monitoring location. The ultimate product of SIMEN is the transportation of relevant event messages in a network-sensitive manner than currently exist in COTS applications.

Introduction

The SIMEN project was funded as part of a US Air Force research program. A key component of Computer Network Defense in DoD enterprises, such as the Air Force, is Security Information Management (SIM) technology. Commercial SIM solutions provide some of the most powerful IA monitoring available to Network Operations and Security Center (NOSC) personnel. However, the Air Force contains intermittently-connected, low-bandwidth, and high-latency WAN-connected networks that are not often seen in commercial enterprises. Such networks may include airborne and forward-deployed enclaves; commercial SIM systems were not specifically designed for these challenging environments.

SIMEN has succeeded in building a prototype to demonstrate that IA equipment can be effectively monitored by a central location. This success was achieved through an improved, network-aware, messaging transport and event management capabilities.

SIMEN Accomplishments

In FY06, SIMEN research confirmed the feasibility of extending IA monitoring to airborne enclaves through a prototype which applies simple algorithms to collect, prioritize, and reduce raw security data transmission to a monitoring facility. In addition, FY06 research prototyped a data architecture

methodology that categorizes IA events, allows for security data manipulation, and provides the means for threat-focused event collection.

Currently, the SIMEN project is participating in an experiment with NATO C3A (NC3A) which aims at integrating the SIMEN prototype with an NC3A research project, Low Maintenance Intrusion Detection Systems (LMIDS), as well as other security products. The experiment is to test the interoperability in a deployed semi-operational environment in coordination with the NATO Computer Incident Response Center (NCIRC). The result of this integration experiment will provide important feedback to SIMEN for improvement in intrusion event and event correlation.

In addition, SIMEN has collaborated closely with IA research projects at the Air Force Research Laboratory (AFRL) and is planning participation in Joint Expeditionary Force Experiment (JEFX) 2008 and NATO Coalition Warrior Interoperability Demonstration (CWID) 2007.

SIMEN Research Directions

Although SIMEN research has taken the first step in ensuring that the "right" data reaches the SIM in an effective and timely manner, our research indicates that a complete solution must also address the dynamic nature of IA event data. Static configurations and rules cannot adapt to the need for changing threat focus, event prioritization, and selection of data transmission – issues that are especially pertinent to enclave networks.

A reactive and intelligent security appliance is needed which adapts its behavior based on network and link performance, local event content/volume, and security analyst. The research goal is to produce and adaptive security appliance to be located on a network enclave to collect, to prioritize, and to reduce the volume of security data while reacting to net-centric behaviors and SIM-correlated threats.

The SIMEN appliance will build upon the previously-developed upstream communication by focusing on bi-directional communication with SIMEN and other security products. The additional downstream communication is essential for leveraging central threat correlation at the remote network enclave.

The data architecture methodology and categorization research will continue with the goal to develop a standard security event grammar. This grammar will enable a standard event representation to be shared between products. The data analysis that leads to a common event grammar will also allow for predictive analysis and modeling for the identification of event patterns that can allow for the transmission of related events that may otherwise have not been sent.

SIMEN research provides a venue for in-depth collaboration and experimentation with IA vendors and researchers through participation various deployment exercises and standards working groups. SIMEN's technical transition will influence commercial SIM vendors, and enterprise security information management strategy for enclave networks.