MISSISSIPPI STATE UNIVERSITY

HIGH PERFORMANCE DATA ANALYTICS

DASI

Autonomic Security Management Framework for High Performance Computing Systems

CHALLENGE

Securing data and applications in high-performance computing (HPC) systems is challenging, particularly due to the complex and large-scale nature of such systems, the open operational environment needed to support external access, and the variety of network protocols and network interfaces that characterize HPC infrastructure. All of these factors can introduce the potential for illicit cyber penetration. The issue at the heart of HPC security concerns, however, is the potential for malicious users in multi-tenancy environments and in the sharing of resource pools on the same physical platforms. Intruders can exploit massive resources in order to mount sophisticated and damaging attacks, gaining access to critical data and applications.

In order to address these concerns and to meet the challenge of ensuring continuously available and trustworthy HPC resources we are developing of a model-based autonomic security management framework for HPC systems that integrates system control, security analysis, and auto-response mechanisms into a model-based management framework to automatically identify and mitigate potential security intrusions and maintain a functional system.

CURRENT PRACTICE

Traditional detection techniques have addressed a portion of system attacks, but have not provided effective techniques to protect against application attacks. Current detection methods adopt predominantly reactive approaches, using signature-based and/or anomaly-based detection. They are typically designed in an ad hoc manner and only for specific system or operating conditions. These approaches

Utilizing model-based techniques and tools to develop effective and proactive security management structure for high-performance computing systems.

are also labor-intensive and challenging to manage. In addition, with the exponential growth in the volume and sophistication of cyberattacks, it is no longer possible to track the signature of new intrusions. Thus a new innovative solution is required to solve this dilemma. In this project we are developing autonomic computing based approach to make HPC systems self-protected with minimum or no involvement from system engineers or administrators.

TECHNICAL APPROACH

This research develops an autonomic security management system for HPC systems by extending our current technologies including the predictive performance management system and our earlier work on security management that have been developed as part of our PNNL funded project to:

- Develop efficient algorithms and mechanisms for accurately identifying anomalous events triggered by attacks and malicious access,
- Develop stochastic models for system security levels based on monitored system/network performance parameters/events and provide the ability to accurately characterize current state and perform risk and impact analysis of potential attacks in real-time, and
- Develop proactive mechanisms to detect and

characterize cyber-attacks and deploy autonomic responses to disrupt and mitigate the impacts of such attacks on the system, and recover the system back to normal operation.
- Utilize the existing MSU and the Idaho Bailiff HPC testbeds to conduct the proposed research and demonstrate pre-deployment capabilities.

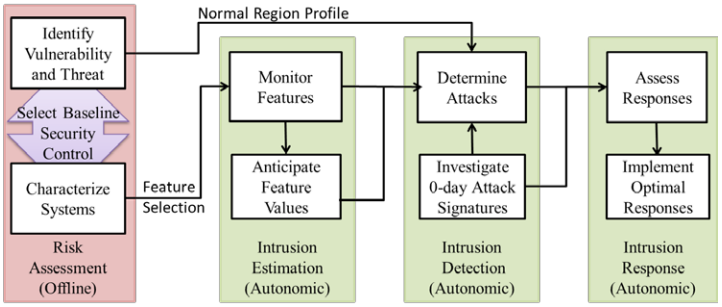
We are producing monitoring and behavior analysis tools to collect information about the current operational states of HPC systems and their applications, a risk assessment model to evaluate the overall vulnerability of the HPC system, attack prediction and early warning systems, and ultimately, autonomic control and security management structure for HPC systems. This security management structure provides an optimal plan of action that includes a sequence of control responses to mitigate and protect against cyber-attacks while maintaining the resilience of the underlying cloud infrastructure.

IMPACT

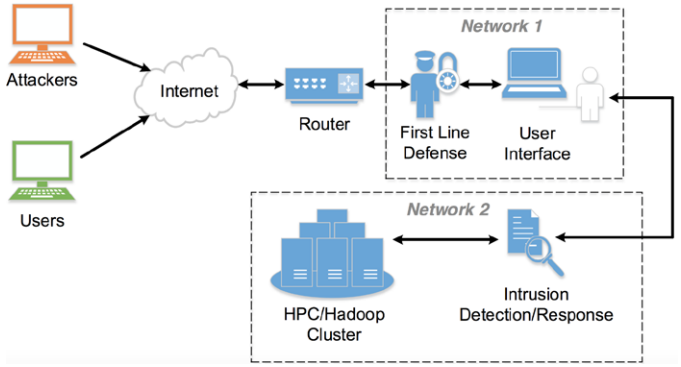
The set of technologies — theory, models, and algorithms — produced as part of this work will convert a significant number of intrusion detection and incident response tasks into systematic and semi-automated processes using concrete mathematical models and proven reasoning and optimization techniques. The project is anticipated to produce:

- Monitoring and behavior analysis tools to collect information about the current operational states of HPC systems and their applications,
- Risk assessment model to evaluate the overall vulnerability of the HPC system.
- Attack prediction and early warning system.
- Autonomic control and security management structure for HPC systems.

By proactively detecting attacks and responding to them at an early stage we will be able to significantly mitigate their impacts and provide effective mechanisms for system recovery. As such, the proposed research has the potential to make a major improvement in the effective protection of critical data and applications hosted in HPC systems.



A model for self-protection system a coordinated processes of real-time monitoring, data processing and analysis, intrusion detection and classification, and automated system protection.



Enhanced security for an experimental HPC cluster testbed with two demilitarized zones (DMZs), Network 1 and Network 2. The first-line of defense (e.g. firewall) are installed in Network 1 to protect from known attacks. External requests pass the first-line of defense are sent to Network 2.

Contacts

Sherif Abdelwahed
Task Lead
662.325.6903
sherif@ece.msstate.edu

David Haglin
Chief Scientist
509.372.4707
david.haglin@pnnl.gov

Funding provided by a grant from Pacific Northwest National Laboratory.