Intrusion Detection for Grid and Cloud Computing (Slides)

Article · January 2010

4 authors, including:

Carlos Becker Westphall

Federal University of Santa Catarina

256 PUBLICATIONS **883** CITATIONS

SEE PROFILE

Carla Merkle Westphall

Federal University of Santa Catarina

77 PUBLICATIONS **250** CITATIONS

SEE PROFILE

Intrusion Detection for Grid and Cloud Computing

Author Kleber Vieira, Alexandre Schulter, Carlos Becker Westphall, and Carla Merkle Westphall

Federal University of Santa Catarina, Brazil

Content Type Journals

Appears IT Professional

Date July/August 2010

Speaker Jyue-Li Lu

Introduction

- Providing security in a distributed system requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. The Grid and Cloud Computing Intrusion Detection System integrates knowledge and behavior analysis to detect intrusions.

- Because of their distributed nature, grid and cloud computing environments are easy targets for intruders looking for possible vulnerabilities to exploit.

- To combat attackers, intrusion-detection systems can offer additional security measures.

Introduction

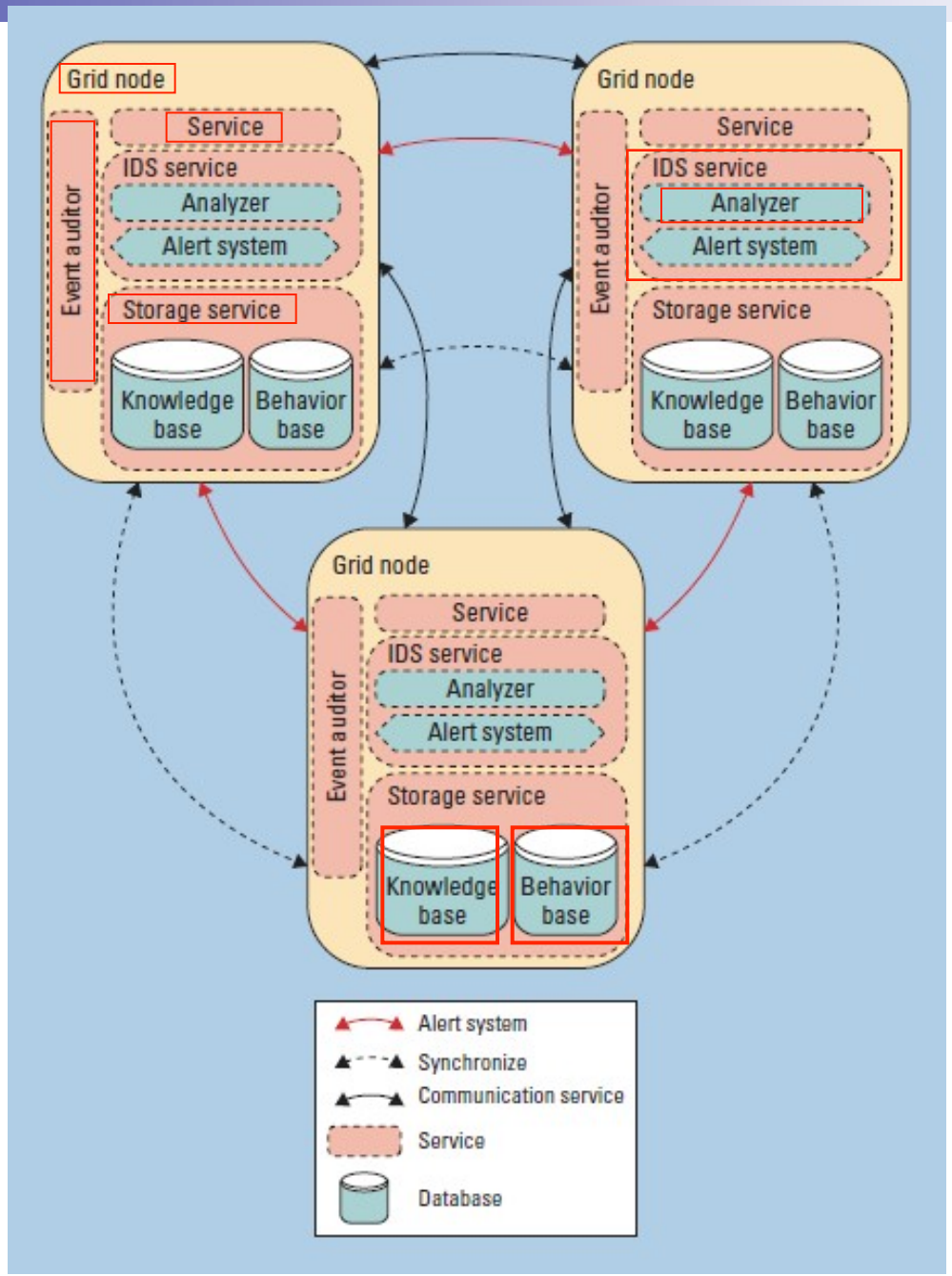
- IDS (intrusion-detection systems) must monitor each node and, when an attack occurs, alert other nodes in the environment.
- This kind of communication requires compatibility between heterogeneous hosts, various communication mechanisms, and permission control over system maintenance and updates—typical features in grid and cloud environments.
- Cloud middleware usually provides these features, so we propose an IDS service offered at the middleware layer.

Introduction

- An attack against a cloud computing system can be silent, because cloud-specific attacks don’ t necessarily leave traces in a node’ s operating system.
- In this way, traditional IDSs can’ t appropriately identify suspicious activities in a grid and cloud environment.
- We propose the Grid and Cloud Computing Intrusion Detection System (GCCIDS), which has an audit system designed to cover attacks.

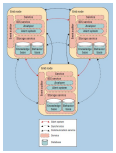
Figure 1

- The architecture of grid and cloud computing intrusion detection. Each node identifies local events that could represent security violations and sends an alert to the other nodes.



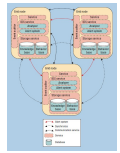
Out Proposed Service

- Figure 1 depicts the sharing of information between the IDS service and the other elements participating in the architecture: the node, service, event auditor, and storage service.
  - Node : resources, which are accessed homogeneously through the middleware.
  - Service : provides its functionality in the environment through the middleware, which facilitates communication.
  - Event Auditor : is the key piece in the system. It captures data from various sources, such as the log system, service, and node messages.
  - Storage Service : holds the data that the IDS service must analyze. It’ s important for all nodes to have access to the same data.



IDS Service

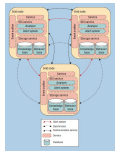
- The IDS service increases a cloud’ s security level by applying two methods of intrusion detection.
- The behavior-based method dictates how to compare recent user actions to the usual behavior.
- The knowledge-based method detects known trails left by attacks or certain sequences of actions from a user who might represent an attack.



IDS Service - Analyzer

- The analyzer uses a profile history database to determine the distance between a typical user behavior and the suspect behavior and communicates this to the IDS service.

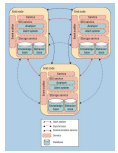
- With these responses, the IDS calculates the probability that the action represents an attack and alerts the other nodes if the probability is sufficiently high.



Behavior Analysis

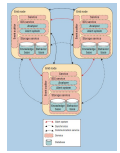
- Numerous methods exist for behavior-based intrusion detection, such as data mining, artificial neural networks, and artificial immunological systems.

- We use a feed-forward artificial neural network, because this type of network can quickly process information, has self-learning capabilities, and can tolerate small behavior deviations. These features help overcome some IDS limitations.



Behavior Analysis

- Using this method, we need to recognize expected behavior (legitimate use) or a severe behavior deviation.
- For a given intrusion sample set, the network learns to identify the intrusions using its **retropropagation algorithm**.
- However, we focus on identifying user behavioral patterns and deviations from such patterns.
- With this strategy, we can cover a wider range of **unknown attacks**.

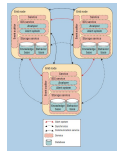


Knowledge Analysis

- Knowledge-based intrusion detection is the most often applied technique in the field because it results in a low false-alarm rate and high positive rates, although it **can’ t detect unknown attack** patterns.

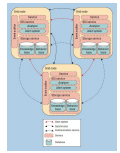
- Using an **expert system**, we can describe a malicious behavior with a rule. One advantage of using this kind of intrusion detection is that we can add new rules without modifying existing ones.

- In contrast, behavior-based analysis is performed on learned behavior that can’ t be modified without losing the previous learning.



Increasing Attack Coverage

- The two intrusion detection techniques are distinct.
- The knowledge-based intrusion detection is characterized by a high hit rate of known attacks, but it’ s deficient in detecting new attacks. We therefore complemented it with the behavior based technique.
- The volume of data in a cloud computing environment can be high, so administrators don’ t observe each user’ s actions—they observe only alerts from the IDS.



Results

- We developed a prototype to evaluate the proposed architecture using **Grid-M**, a middleware of our research group developed at the Federal University of Santa Catarina.

- We prepared three types of simulation data to test.
  - First, we created data representing **legitimate action** by executing a set of known services simulating a regular behavior.
  - Then, we created data representing **behavior anomalies**.
  - Finally, we created data representing **policy violation**.

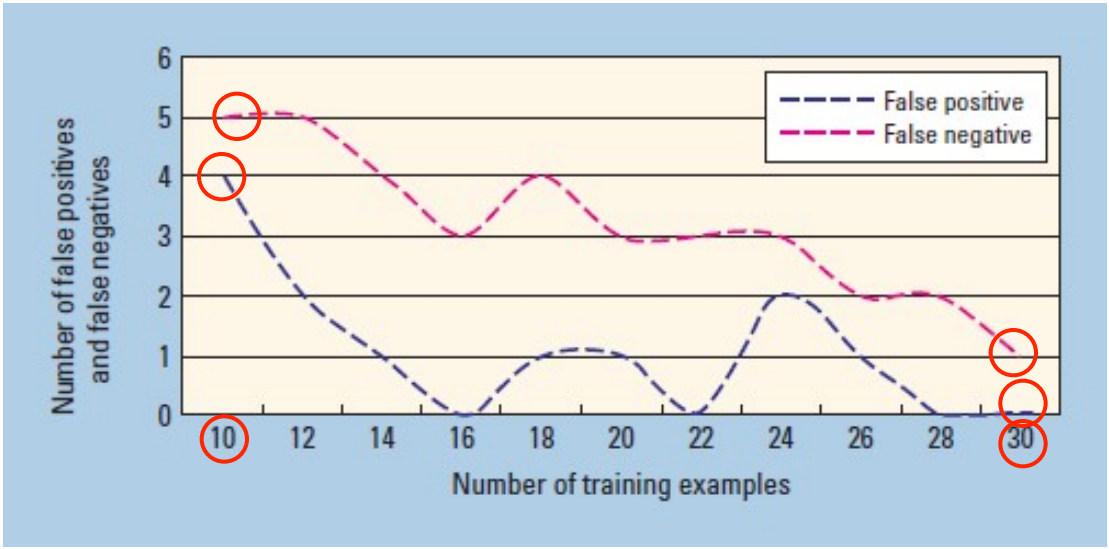
Evaluating the Event Auditor

- The event auditor captures all requests received by a node and the corresponding responses, which is fundamental for behavior analysis.
- In the experiments with the behavior-based IDS, we considered using audit data from both a log and a communication system.
- Unfortunately, data from a log system has a limited set of values with little variation.

Evaluating the Event Auditor

- This made it difficult to find attack patterns, so we opted to explore communication elements to evaluate this technique.
- We evaluated the behavior-based technique using artificial intelligence enabled by a feedforward neural network.
- In the simulation environment, we monitored five intruders and five legitimate users.

Evaluating the Event Auditor



- We initiated the neural-network training with a data set representing 10 days of usage simulation.
- Using this data resulted in a high number of false negatives and a high level of uncertainty.
- Increasing the sample period for the learning phase improved the results.