International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:6, 2007

Intelligent Agents for Distributed Intrusion Detection System

M. Benattou, and K. Tamine

Abstract**—**This paper presents a distributed intrusion detection system IDS, based on the concept of specialized distributed agents community representing agents with the same purpose for detecting distributed attacks. The semantic of intrusion events occurring in a predetermined network has been defined. The correlation rules referring the process which our proposed IDS combines the captured events that is distributed both spatially and temporally. And then the proposed IDS tries to extract significant and broad patterns for set of well-known attacks. The primary goal of our work is to provide intrusion detection and real-time prevention capability against insider attacks in distributed and fully automated environments.

Keywords**—**Mobile agent, specialized agent, interpreter agent, event rules, correlation.

I. Introduction

THE growing importance of network security is shifting security concerns towards the network itself rather than being host based. Security services must be evolving into network-based and distributed approaches to deal with heterogeneous open platform and support scalable solution [1].

The intrusion detection technology is the process of identifying network activity that can lead to a compromise of security policy. IDS must analyse and correlate a large volume of data collected from different critical network access points. This task requires an IDS to be able to characterise distributed patterns and to detect situations where a sequence of intrusion events occurs in multiple hosts.

A cooperative intrusion is one of the difficult problematic where the intruder(s) can use network access points as an attempt to disguise their activities, since all of the activities on one node may be characterized as intrusive, but a few activities from the cooperative intrusion on single node would most likely not be characterised an intrusive.

Manuscript received May 20, 2005.

M. Benattou is with the Institut d'Ingénierie Informatique de Limoges, Laboratoire de Recherche Informatique , 43, Rue Sainte Annes, 87000 Limoges, France (phone: 33-0 6-13-99-80-46; fax: 33-05-55-06-30-16; e-mail: benattou@3il.fr).

K. Tamine, was with University of Limoges, LMSI Laboratoire de Méthodes et Structure Informatique, 8 Rue d'Isle, 87000 Limoges, France (phone: 33-05-.55-43-69-75; e-mail: tamine@msi.unilim.fr).

Thus, the IDS must be able to correlate events and related users from all of the system nodes that are potentially participating to a cooperative intrusion. For example, a *Smurf attack* sends PING requests to a network broadcast addresses.

The return address of the PING request is spoofed to be the address of the attack target. All *Sniffers* located in different nodes detecting the PING requests must not reply to the pinging source.

Detecting intrusion in distributed network from outside network segment as well as from inside is a difficult problem [2]. Intrusion detection system must analyze a large volume of data while not placing a significant added load on the monitoring systems and networks. There are several limitations of existing IDS product: current systems report alerts to a centralized database and hope that a network administrator is immediately on-hand to take an action. The administrator analyzes alert reports and takes some actions. Other proposed system analyze database using knowledge discovery techniques for deciding which actions must be taken. It's often too late in critical systems to decide where actions must be taken by one centralized device or user when the given system may have been compromised and vital information may have been stolen.

In [3] we have proposed a distributed intrusion detection system based on a mobile agents community to assess malicious activity against computer networks. Our approach is based on two concepts. Firstly, the system uses a specialized agent approach to separate monitoring tasks. Individual specialized agents perform their own execution of input data sources. Secondly, we introduce the agents community concept: agents with the same speciality and the same purpose for detecting one attack type. All specialized agents from the same community communicate using mobile platform environment for collecting and analysing all the data fetched from all the predetermined network nodes in order to evaluate and confirm some attack types and the actions that must be performed in different network nodes.

This paper extends our proposed IDS by defining the semantic of intrusion events occurring in a predetermined network. And then a set of attack rules has been defined for well-known attacks. The correlation rules referring the process which our proposed IDS combines the captured events that is distributed both spatially and temporally. And

then tries to extract significant and broad patterns for set of well-known attacks. Agent based, our system shares a common goal of exploiting the mobility paradigm of the agents to perform distributed correlation.

This paper is organized as follows: section 2 presents the Intrusion Detection System in distributed context and the related previous work; section 3 describes our model approach and reports in details how the proposed components works; Finally, we outline our prototype realisation and we provide directions for future work.

II. Mobile Agents Based IDS

Based on the distributed architecture, the proposed approaches, implementing different IDS, integrate the concepts of distributed agent and mobile computing. Agents are defined as entities that detect and take predefined actions against malicious activity. Installed on critical network infrastructure, including network segments, servers and selected hosts, distributed agents apply the required attack recognition algorithms to detect typical malicious activity on private networks. Agents share critical alerts knowledge to better understand the impact of an attack across the predetermined network. It could be implemented as software running on servers and host or as independent hardware devices segments.

In order to include overcoming network latency, reducing network load, performing autonomous and asynchronous execution, and adapting to dynamic environments, current Distributed IDS uses mobile agents technology [4]-[5]. The Mobile agent paradigm extends the agent by including the concept of mobile computing. In this context, the agent can be executed autonomously over a set of network hosts, on behalf of an individual organisation. Mobile Agent Environment creates an appropriate execution environment for Mobile Agent that gives the basic services including creation, transportation and execution. It also performs constraint mechanism, fault-tolerant strategy, security control and communication mechanism [6]. It implements agent transfer protocol, communication protocol and supports events transmission [7].

We can identify three technologies In proposed distributed IDS research architectures based on agent paradigm: Based on fully distributed architecture like [8] where data collection and analysis are performed locally; Based on distributed architecture where data collection and analysis are performed with a central management unit [1]; Based on multiple independent entities called Autonomous Agent for intrusion detection framework, where data is collected from different sources. These systems are imitating the behavior of natural distributed systems in order to achieve the efficiency found in natural systems [9] .

The difficulties found in the proposed IDS, result in the great variety of vulnerable attacks that the generalized agent consider to be uncertain. Processing uncertain attacks causes unnecessary time resources to be diverted from achieving the network system mission and system administrators to dismiss reports of intrusions. Therefore, the cooperation of distributed Intrusion Detection System nodes, based on the values of the thresholds, must be set to detect as many intrusions as possible, without an intolerable amount of false alarms. For the certain (intrusion) attacks, the proposed IDS executes local actions and the administrator system is responsible of informing all of the other predetermined network nodes.

III. Multi-Agent IDS Framework

A. Multi-Agents Architecture

The Specialized Local Agent is the engine component of our system. It must combine several kinds of attack analysis such as signature detection, anomaly detection and performed global analysis, for detecting distributed attacks. Due to the complex analysing tasks made by the SLA for detecting intrusions, the SLA delegates performed tasks to well defined agents and uses different data sources. As shown in figure 1, SLA delegates predetermined performed tasks to four agents (Filter, Analyser, Correlate, Interpreter and Mobile), and use two knowledge database (Event Rules, Events DB).

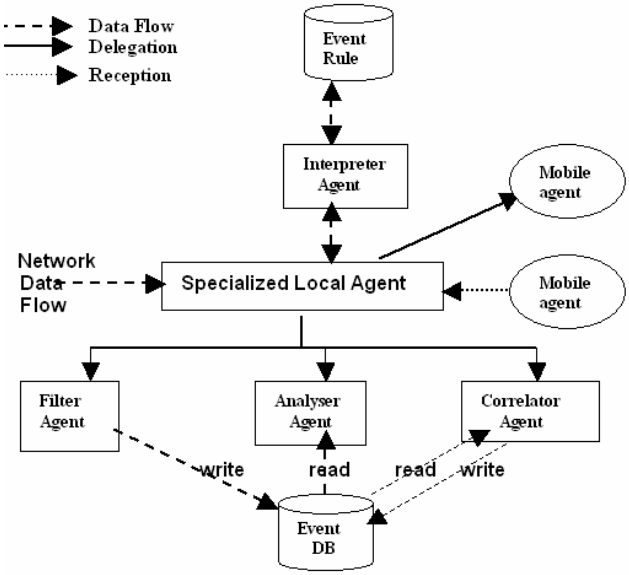

Fig. 1 Multi-Agents Architecture

B. Flow Data Source

In the high design level, suspicious network traffic [10] is captured by Snort sensor and log files are generated. According to event keywords specified in detection *Event rules, Filter Agent* is agent responsible for filtering specialized security events from the log files. It examines the packets for well-known attack events and stores all its characteristics into *Event DB*. According to events rules, we have identified two event types: local events occur in a local network node and extern events occur in other network nodes. Specialized Local Agent delegates the filtering tasks to different *Filter Agents.*

C. Intrusion Event Rules

An event is an indication of intrusion. A security event is characterized by its signature, its type, location, and a temporal attribute representing the event occurring moment. According to the event type and its observation point, [11] identifies various events classes. In our model, each event is characterised also by its keyword signature attacks, for example ping, nmap, etc. Based on the combination of keyword signature events, a set of a set of attack rules has been defined for well-known attacks. A rule is a set of requirements that will trigger an alert. Each rule is characterised by its sequence of events and the alerts block describing the predetermined actions executed by the system where events has been occurred.

We have identified two classes of signature rules:

- Local event rules, where all events occur in the same network node:

(1) Alert <actions> when $even\_local_1, ..., even\_local_n$

- Extern event rules, where at least one event of the given sequence events rule occurs in other local network nodes. This class of event rules is introduced to detect distributed attacks:

(2) Alert <actions> when $even\_local_1, ..., even\_local_n$
and then $even\_ext_1, ...even\_ext_m$.

D. Intrusion Detection Mechanism

The heart of our detection mechanism is the *Interpreter Agent.* It collaborates with the *Analyser Agent* for detecting complex local attacks, and uses the *Correlate agent* with the *Mobile Agent* for determining whether some suspicious activities in different node can be combined to be a distributed intrusion.
According to local event rules, the analyser agent is responsible for detecting local intrusions.

The *Analyser Agent analyses* the events database. It looks for the local events selected by the *Interpreter Agent*. These patterns are retrieved from *Events DB*. Then, it reports a search results to the *Interpreter Agent* using its Specialized Local Agent.

It's clear that correlation of the relevant events significantly reduces the number of false positive and gives a better view of an attack scenario in case of coordinated distributed attacks [12]. According to extern event rules given by the *Interpreter Agent,* the correlate agent is responsible for determining whether some suspicious activities in different network nodes can be combined to be a distributed intrusion. It queries the events database to search the occurrence of some event, and accesses to database events to store the occurrence of the external event received from other network nodes using *Mobile Agent*.

A mobile agent based IDS uses agents with analysis capabilities to perform remote query and search actions. In our IDS model, mobile agent is used to perform well defined tasks: search the events occurrence in a given network or confirm occurrence of some event in a local network node. In the case of correlating events for detecting distributed attacks, the mobile agent is used to confirm the occurrence of some event in network nodes. For example, if the SLA is informed by the correlate agent that some correlating events are detected in the local network area, it would dispatch a mobile agent to search the occurrence of the same event type in the network nodes, and report the responses in its results area. The other case is made where SLA receive a mobile agent to confirm some extern event. Figure 2 shows the itinerary example taken by the mobile agent from node source to nodes 1 and 2. Mobile agent created by specialized agent of node source looks for confirming the *Event1* by nodes 1 and 2, and also informs them that the Event2 occurred.

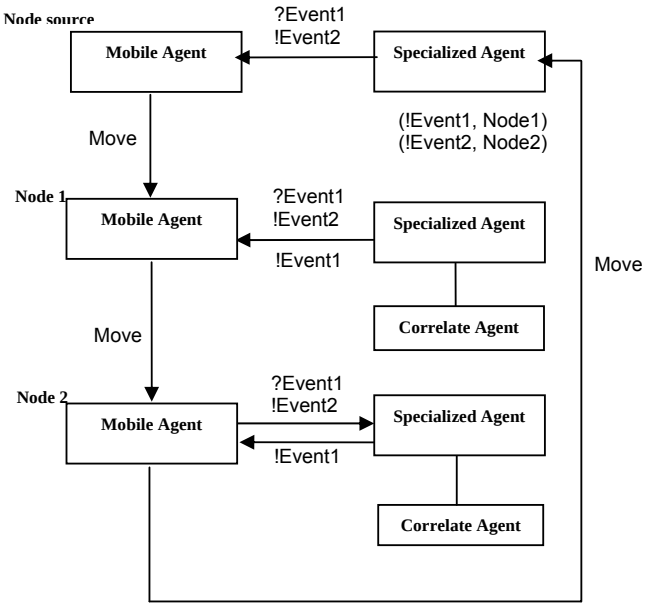

Fig. 2 Itinerary Example of a Mobile Agent

The Interpreter Agent behavior can be seen as an inference engine system. It processes the events Knowledge encoded in the Knowledge base (Event Rules) for detecting the attacks. It consults the Event Rules and repeats the following scenario:

- Choose the first rule with no active state
- Make this rule in active state
- Submit the local events belonging to the premise part of the given rule (1), to the Analyser Agent that have the pattern matching task to confirm the occurrence of the given events in Event DB . When all the local events of the given rule have been occurred, the *Interpreter Agent* makes the rule in not active state.

And then transmits the alert actions to the *Specialized Local Agent*. In the case of the extern rule (2), the *Interpreter Agent* completes the pattern matching task by submitting the externs events to the *Mobile Agent*. The extern event is characterized by its node location. The extern event locations give the itinerary taken by the mobile agent, and then it looks for confirming the given events. When all the local and extern events of the given rule have been occurred, the Interpreter Agent deactivates the rule. And then transmits the alert actions to the specialized local agent.

In the all case the active state of a given rule has been performed in well defined processing time.

IV. Conclusion and Future Works

In this paper, we have proposed an approach for distributed intrusion detection system based on the specialized local agent and the agents community concepts. A specialized local agent is used to separate monitoring tasks. The agents community is a group of specialized agents, created for collecting and analysing all the data transit from all predetermined network nodes. The specialized local agent executes predetermined actions and uses the Mobile Agent Environment to investigate all the other network nodes of the same community. The agents community collaborate and cooperate for confirming intrusion in predetermined network. The semantic of intrusion events occurring in a predetermined network has been defined. The correlation rules referring the process which our proposed IDS combines the captured events that is distributed both spatially and temporally, and tries to extract significant and broad patterns for set of well-known attacks.

Our prototype of this model has been experimented in a local network context. In our case Snort has been chosen [13] as the first level network data event flow capturing. Snort is chosen for its availability, ease of configuration and customisation. We have chosen Voyager [14] as Mobile Agent Environment to implement our prototype testing. Voyager, from recursion software, can be seen as strengthened object request broker. Compared with other mobile agents development platforms, Voyager integrates with Java more intensely, which can be used easily to develop mobile agent platforms, and also to build up traditional distributed systems. Prototype testing has been experimented in local network. Our work is now oriented to defining the hierarchy of specialized local agents and formalize the communication inter-communities.

References

[1] M. Eid, "A New Mobile Agent-Based Intrusion detection System Using distributed Sensors", *In proceeding of FEASC*, 2004.
[2] G. Hulmer, J. S.K. Wong, V. Honavar, L. Miller, Y. Wang, "Lightweight Agents for Intrusion Detection", *Journal of Systems and Software* 67 (03), pages 109-122, 2003.
[3] M. Benattou and K. Tamine, "Mobile Agents Community For Distributed Intrusion Detection System", *accepted for publication in proceeding of International conference on Computing, Communication and Control Technologies*, Austin, USA, July 2005.
[4] W. A. Jansen, "Intrusion detection with mobile agents", Computer *communication* (15): page: 1392-1401, 2002.
[5] C. Kruegel and T. Toth "Applying Mobile Agent Technology to Intrusion Detection", *technical report*, University of Vienna, TUV-1841-2002-31, 2002.
[6] M. Benattou and Jean-Michel Bruel, "Active Objects for Coordination in Distributed Testing", *Proceedings of the 8th Int. Conf. on Object-Oriented Information Systems OOIS'02,* Lecture Notes in Computer Science, Vol 2425, pp 348-357, 2002.
[7] W. A. Jansen, "Determining Privileges of Mobile Agents", *17th Annual Computer Security Applications Conference*, pages 149-160, 2001.
[8] J. Barrus and N. Rowe, "Distributed Autonomous-Agent Network-Intrusion detection and response System. *In proceeding of Command and Control research and Technologies Symposium*, 1998.
[9] S. Fenet and S. Hassas, "A Distributed Intrusion Response System Based on Mobile Autonomous Agents Using Social Insects Communication Paradigm". *Published by Elsevier Science B. V.*, pages 21-29, 2001.
[10] S. Anasari, Rajeev S.G., and H.S. Chandrashekar, "Packet Sniffing: A brief Introduction", *IEEE*, January 2003.
[11] K. Boudaoud, N. Foukia, Z. Guessoum "An Intelligent Agent Approach for Security Management ", *Proceeding of the 7th HP OpenView University Association Plenary Workshop, HPOVUA'2000*, Santorini, Greece 12-14 June 2000.
[12] K. Singh, Son Vuong "Blaze: A Mobile Agent Paradigm for VOIP Intrusion Detection System", *Proceeding of ICETE 2004, First International Conference on Business and Telecommunication Networks*, Setubal, Portugal, August 2004.
[13] M. Roesch, "Snort: Lightweight Intrusion detection for networks", *A white paper* on the design features of snort 2.0, 2004. www.sourcefire.com/technology/whitepapers.html
[14] T. Wheeler, "Reducing Development Effort Using the Voyager ORB", *Recursion Software*, Inc, 2002.