Distributed And Intelligent Platform Of Intrusion Detection At Two Levels

***Driss Raoui, Siham Benhadou, Hicham Medromi**
Systems Architecture Team (EAS), Laboratory of Computer Science , Systems and Renewable Energy (LISER), National School of Electricity and Mechanics (ENSEM), Hassan II University Aïn Chock, BP 8118, Oasis Casablanca, Morocco
*Correspondence to: Driss Raoui, raoui.driss@gmail.com
Published online: June 12, 2010

Abstract

The development of the networks and the distributed systems permitted to ease the communication and the information exchange on one hand, and on the other hand, it generated important risks in the field of information systems security. So, it is important to take the right necessary measures to be protected from these threats. Similarly, the intrusion detection systems have to be adapted to the change of the users' behaviour and to the complex evolution of the networks. In this paper, we propose a platform for the intrusion detection based upon a distributed approach using the multi-agents aspect so as to eliminate the strong attacks and to do a more deepened analysis of the intrusions representing eventually weak threats.

Keywords: Security; Intrusion Detection; Platform; Analyzer; Multi-Agents Systems.

1. INTRODUCTION

The security in a network is to guarantee that all the machines in the network work in the optimal way. With the development of Internet, computer systems are becoming more open and collaborative enabling, facilitating communication and exchange of information by improving the transmission speed and technology of interconnection. Consequently, computer networks have become increasingly complex and therefore the number of vulnerabilities found on computer systems may be important. Thus, attacks against these vulnerabilities can be both varied and complex [1]. To ensure optimum operation of the network and computer systems, it is necessary to identify potential threats. In many ways, technology can be implemented to ensure system security information. Among these methods, we found the intrusion detection system is to monitor the activity of a network or system to detect real time abnormal use of computing resources, to log these events, to analyze this information in search of violation or abuse, warning generating alerts and sometimes reacting against intrusion [2]. Currently, intrusion detection systems lack of methods and mechanisms to detect complex attack scenarios. They are exposed to many challenges as the network evolves and as new attacks emerge. Existing intrusion detection systems are not adapted to the increasing complexity of attacks and changing network dynamics and user behaviour.

In this paper, we present in the following section the state of the art on current intrusion detection systems and the multi-agent systems. In Section 3, we detail our approach by proposing a distributed intrusion detection platform with two levels of analysis based on multi-agent system and methodology of intrusion detection applied. Section 4 is devoted to the realization of a simulation platform where you will find different AUML diagrams illustrating the static and dynamic platform developed. Finally, we present a summary of work done and the prospects envisaged in Section 5.

2. STATE OF THE ART

A- Intrusion detection system

An intrusion detection system (IDS: Intrusion Detection System) is designed to automate the detection of a violation or attempted violation of security policy implementation within an information system. It is composed of separate elements providing the real time or delayed analysis of security events, aggregation and correlation of these events and the implementation of processes and alerts the appropriate response [3]. The integration of an intrusion

detection system in a security platform therefore allows the collection of accurate and practical information on the status of threats to information systems.

There are two distinct major families of IDSs:

- ✓ The N-IDS (Network Based Intrusion Detection System): it provides security at the network level.
- ✓ The H-IDS (Host Based Intrusion Detection System): it ensures the security level for hosts.

The network-based intrusion detection system (NIDS) requires dedicated hardware and is a system capable of controlling packets on one or more network links in order to discover if a malicious on abnormal act occurs. This type of IDS has the advantage that a single sensor, properly placed, can detect attacks that target multiple hosts. However, it has its own limitations. For example, it cannot detect attacks carried out locally that have no manifestations on the network card (e.g., attacks executed by a local user from the console).

The host-based intrusion detection system (H-IDS) monitors the host on which the sensor is installed. The event stream can be system call sequences, log records from one or more services, operating system logs, or any other log for activities within the monitored machine. Normal activities as well as intrusions may consist of a single event or of a series of events. For example, an ftp session might generate log records on the host that runs the FTP server indicating the start of the session, successful authentication, transferred files, examined directories and termination of the session. These records may be mixed with the records of other simultaneous ftp sessions as well as records from other services. The main advantage of HIDS is that it can theoretically detect intrusions where a local legitimate user tries to perform some illegal actions and can help detecting attacks such as Trojan or other attacks that may involve software integrity breaches without leaving traces on network traffic. Although the HIDS has the advantage of not requiring additional hardware, it can cause a significant degradation in the performance of its host due to the overhead of the HIDS operations. Another limitation is the difficulty to port it from one platform to another [4].

B- Analysis methods

The primary classification of IDS remains the method of analysis. Two methods exist today: the scenario approach and behavioural approach [5, 6]. The scenario approach: is to look in the activity of the monitored element fingerprints (or signatures) of known attacks. This type of IDS is purely reactive and it can only detect attacks that he has signed. The behavioural approach: is to detect abnormalities. The implementation always includes a learning phase during which the IDS will see the normal operation of the elements monitored. It is thus able to report deviations from the reference function. The mechanism of intrusion detection is centralized, which means that data collection is local but the analysis is centralized. The complexity of coordinated attacks does not facilitate their detection by a single entity. Indeed, each entity having a limited local view of the network, it is very difficult to detect such attacks. Detecting such attacks requires a correlation of different tests performed at different points in the network. The various entities must then communicate their analysis and cooperate to effectively detect attacks.

C- Multi-agent System

A multi-agent system (MAS) consists of a set of IT processes taking place simultaneously, so several officers living at the same time, sharing common resources and communicating between them [7]. These agents are characterized particularly by their ability autonomy, adaptation, communication or coordination to react against complex attacks in a dynamic environment. Architecture of multi-agent hybrid system allows the officer to have a reactive behaviour when situations require, and deliberative behaviour in other circumstances. A reactive agent is only reacting to changes in the environment. A deliberative agent performs some deliberation in choosing his action. It must use planning techniques to predict the actions to bring him to his goal. The agent may combine information about his goals with information on the results of its actions to choose actions that will enable it to achieve its goals is what allows him to improve and adapt to their environment. The intelligent agents, divide on two analysers, collaborate

and communicate to discern attacks efficiently according to schemata of attacks defined in their knowledge base. Therefore, the capacity to intervene in real-time to block, destroy, leak out and exploit information.

3. A PLATFORM FOR INTRUSION DETECTION

A- Motivation of the proposed approach

Many network attacks are characterized by abnormal behaviour in various network elements. It is therefore very important to distribute the functions of detecting several entities that oversee different parts of the network. Excessive exchange of information between the distributed entities can congest the network. It is important to let the entity overseeing a network element, performing a local analysis and detecting intrusions at this level. Thus, the distributed entities must be independent. The functions of intrusion detection must be modified to adapt to changing user behaviour and evolution of complex networks by sending the tasks delegated to autonomous entities. The objective is to design a solution for intrusion detection soft and flexible to adapt to this dynamic environment and the increasing complexity of attacks.

B- Proposal

We offer a platform and distributed intelligent intrusion detection based on multi-agent system consists of two levels of analysis allows on one hand to distribute the monitoring / detection of several entities and enforce rules and safety procedures to eliminate the strong and known attacks and on other hand, benefit cognitive abilities of its staff to conduct a more thorough assessment of intrusions that can represent low threats. This solution is autonomous and distributed intelligent for experiment system. Making decision is distributed to ensure a high level of intrusion detection.

C- Architecture of proposed platform of intrusion detection

The proposed architecture consists of several agents with different roles and distributed at different network points. These agents combine the capabilities responsive to cognitive abilities. It consists of two levels; the first level is based on rules and safety procedures. This approach allows to shape the rules that describe the unintended uses, is relying on past intrusions or known weaknesses. The effectiveness of this approach is based on rapid response officers to eliminate the known attacks. To block intrusions complex unknown by the system or represent low threat level 2 of this device identifies these events and automatically determines whether action is needed due to cognitive abilities of its staff. Figure 1 shows the block diagram of the distributed platform based on multi-agent system.

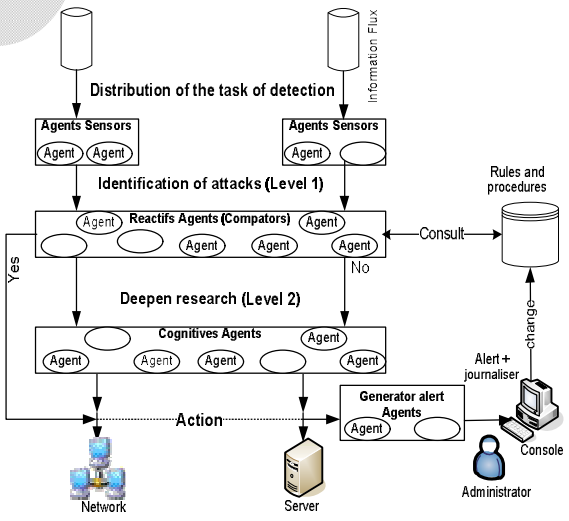

Figure 1. Proposed platform of intrusion détection.

D- Principle of operation

The proposed intrusion detection system consists of several intelligent agents, monitoring the network or sensitive positions, with the following characteristics:

The analyzer based on a distributed approach, using multi-agent system, includes:

- ✓ Agents responsible for collecting sensor data exchanged on the network or those who arrive at a sensitive position and will be transmitted to comparators.
- ✓ Comparators agents, with the reactive capacity, responsible to compare the flow of events with the rules and procedures describing the unintended uses.

If a rule is violated when there is interference and the degree of threat that may represent the intrusion, the officer will compare the direct traffic or to the cognitive agent to search further, or it acts to block traffic and cut the connection.

- ✓ Cognitive agents with adaptive and learning function, their role is to check whether the event may represent a low threat and react quickly when an intrusion to block traffic and prevent the agent generator warning.
- ✓ Agents generating alerts their role is to generate an alert message to the appropriate administrator and store information about the event in a log file.

E- Description of the method of detection

Used analysis method is:

- ✓ Gather the event flow passing through the agent sensor
- ✓ Analyze the agent compare the data collected and compare them to a database of rules and procedures to determine the degree of threat represented by the intrusion
- ✓ Check the level of intrusion is acceptable or not and determine the direction of traffic, it will continue its path towards cognitive agent or close the connection
- ✓ Make the cognitive agent further investigation of the flow of event and determine its condition and decide to let the traffic continued its path toward the target or block
- ✓ Storing information on the event at risk in a file log and generate a notification message intrusion by generating agent alert
- ✓ Fuelling basic rules and procedures by the security administrator.

4. IMPLEMENTING A SIMULATION PLATFORM

We begin the realization with the modelisation and the conception system.

A- Design Model

In this section, we propose a design based on the AUML language.

Agent UML is an extension of UML to take into account the agent notions. Agent UML inherits representations proposed by UML [8]. It contains ten type's diagrams and symbolizing many different views to represent particular concepts of information system. They fall into two main groups:

- ✓ Behavioural diagrams or dynamic diagrams: Sequence diagrams, Collaboration diagrams, Activity diagrams, State chart, Use Case diagrams
- ✓ Structural diagrams or static diagrams: Class diagrams, Object diagrams, Packages, Component diagrams, Deployment diagrams

These diagrams are not necessarily all products at modelling.

The design of the proposed architecture is described through the two class diagrams and sequence agents to illustrate respectively the static and dynamic platform.

B- Static aspect

Agent UML allows to represent several levels of abstraction in the design class diagrams. We consider the following two levels: the conceptual level and implementation level.

The *conceptual level* is high enough for the multi-agent system eliminating all surface information for understanding the structure of the system. The agent class diagram in Figure 2 shows the conceptual level of the platform.

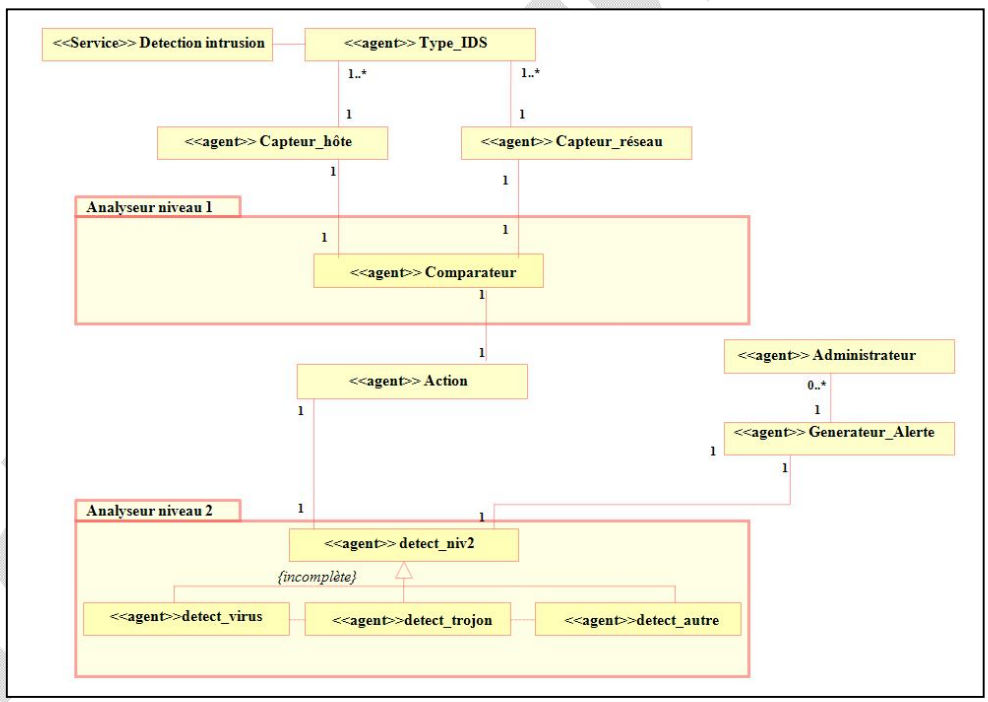

Figure 2. Agent class diagram conceptually.

The *level implementation* gives in detail the contents of agents. Figure 3 shows a portion of the class diagram for the agents level implementation.

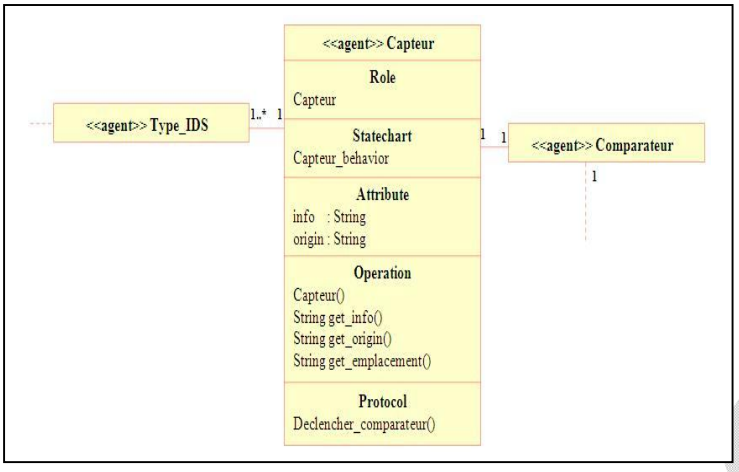

Figure 3. Class diagram level implementation agents.

C- Dynamic Aspects

The sequence diagrams in AUML represent message exchanges between agents.

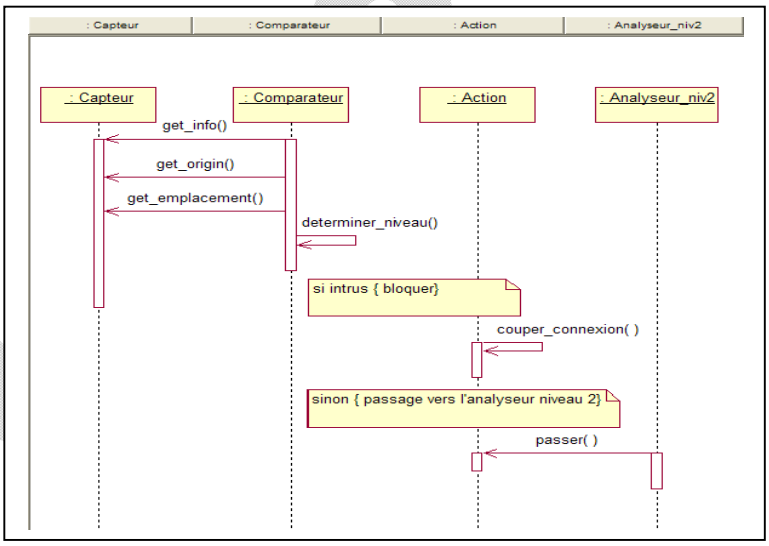

Figure 4. Sequence Diagram.

The sequence diagram given in Figure 4 shows the interaction between different agents over time in the case of recovery of information flows at the analyzer level 1.

The sequence diagram shown in Figure 5 shows the interaction between different agents over time in the case of recovery of information flows at the analyzer level 2.

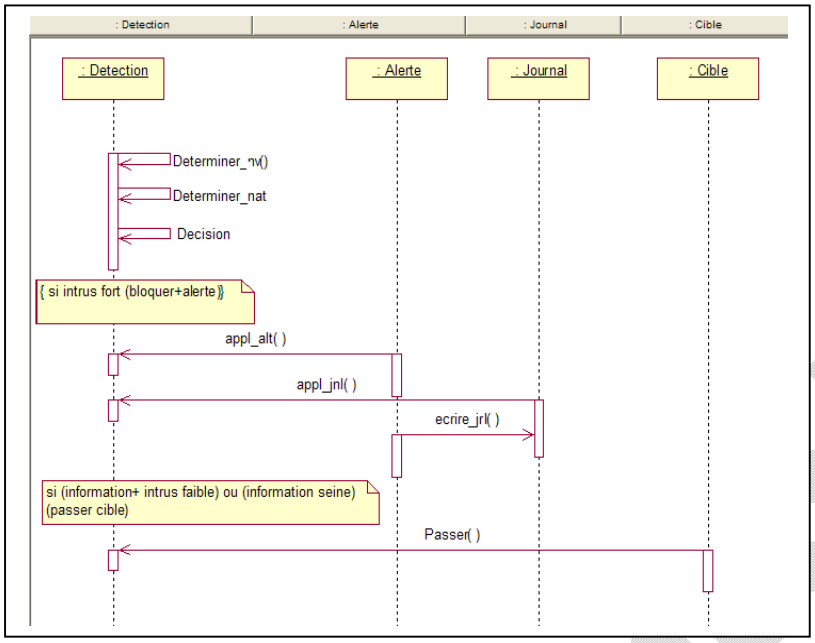

Figure 5. Sequence Diagram.

D- Implementing the simulation platform

After the design phase of the proposed model, we developed a simulation application using an open source distribution (Java and Linux). The simulation platform developed using a new methodology in the assessment mechanism system intrusion detection reflects the goals already set. The results achieved from the application of simulation is that it has allowed us to test the efficiency of the analyser level 1.In fact, we have sent some attacks in which the rules are applied on the analyser level 1 that react and block those attacks thanks to the capacity of the reactive agents. In the same time, for testing the intelligence of the agent's analyser level 2, we have sent some attacks which are unknown by the database of the rules that are not used with the analyser level 1. In contrast, with the use of knowledge used by the analyser level 2, they were able to block those attacks. Further, more, we have already tested the pertinence brought by the analyser level 2 to our security platform and it was a real success.

5. CONCLUSION

In this paper, we presented a new mechanism for detecting intrusions formed by an intelligent, distributed architecture based on multi-agent aspect based on two levels of analysis allows one hand to respond quickly against the attack complex assess the state of the flow captured by reference to rules and procedures and other predefined hand, to detect unknown attacks by the system and reinforces the level of security provided to the target monitored using the cognitive agents of the second analyzer. Looking ahead, we are currently working on adapting the behaviour of agents to automate the generation mechanism of a rule, which corresponds to an attack not known. This process allows the automatic feeding of the basic rules and security procedures new rules dedicated to the recognition of an intrusion or attack unknown. In addition, most of the systems of intrusion detection are based on operating systems; they can sometimes themselves be targets of attack. We plan to replace the parser level 1 by hardware (PLC) to protect intrusion detection systems from attacks to which they may be subject.

6. AUTHORS' CONTRIBUTIONS

DR carried out comparative study of both commercial and open source intrusion detection system. DR proposed new developed, distributed and intelligent architecture of intrusion detection system based on multi-agent system. DR drafted part of the manuscript.

SB initially developed the simulation application using open source development tools to validate the proposed architecture. SB performed the design using the modeling language AUML to take into account the aspect Agent. SB made the application using the Java programming language and participated in drafting of manuscript.

7. ACKNOWLEDGEMENT

HM is our Supervisor. HM has coached through this project to fix the line of research on the safety aspect, especially, intrusion detection.

REFERENCES

[1] Solange G, 2004. Sécurité informatique et réseaux. Edited by DUNOD.

[2] Zalewski M, 2008. Menaces sur le réseau - Sécurité informatique : guide pratique des attaques passives et indirectes.

[3] Northcutt S, Novak J, McLachlan D. Détection des intrusions réseaux. Edited by CampusPress.

[4] EL-Sayed Gadelrab M, 2008. Évaluation des Systèmes de Détection d'Intrusion. PhD thesis. Toulouse University.

[5] IDS-Systèmes de Détection d'Intrusions, Partie I [http://www.linuxfocus.org/Français/May2003/article292.shtml]

[6] IDS-Systèmes de Détection d'Intrusions, PartieII [http://www.linuxfocus.org/Français/May2003/article294.shtml]

[7] Boudaoud K, 2000. Un système multi-agents pour la détection d'intrusions. In Proceedings of the Journées Doctorales Informatique et Réseaux (JDIR): 6-8 November, 2000; Paris.

[8] Huget M, 2002. Une application d'Agent UML au Supply Chain Management. In Proceedings of the Journées Francophones d'Intelligence Artificielle et Systèmes Multi-Agents: 28-30 October 2002; Lille.