Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, December 2009, vol. 14, no.3
(*http://www.arraydev.com/commerce/jibc/*)

New Distributed Methodology for Security Base on Multiagent System

Siham BENHADOU
Equipe Architecures Système, ENSEM, Université Hassan 2 Ain Chock.
BP. 8118, Oasis Casablanca, Morocco
Email: ***benhadou.siham@gmail.com***

Driss RAOUI
Equipe Architecures Système, ENSEM, Université Hassan 2 Ain Chock.
BP. 8118, Oasis Casablanca, Morocco
Email: ***raoui.driss@gmail.com***

Hicham MEDROMI
Equipe Architecures Système, ENSEM, Université Hassan 2 Ain Chock.
8118, Oasis Casablanca, Morocco
Email: ***hmedromi@yahoo.fr***

Abstract

The development of networks and computer systems has enabled both to facilitate communication and exchange of information and secondly, it has created significant risks in the field of security of information systems. Therefore, it is important to take adequate measures to be protected from these threats. Similarly, intrusions detection systems are known to adapt to changing user behavior and evolution of complex networks. In this paper, we propose a platform of intrusion detection based on a distributed approach that uses multi-agent aspect to eliminate heavy attacks and make further discussion on the intrusions may represent low threats.

Keywords: **security; intrusion detection; platform; analyzer; multi-agent system**

INTRODUCTION

The network security is a level of assurance that all machines on the network are working optimally (Solange, 2004). To eliminate the vulnerabilities, attacks and ensure a high level of network and systems, we must proceed with the implementation of preventive security policy complemented by tools and techniques for intrusion detection to monitor the activities 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.
Systems current intrusion detection are becoming an increasingly important mechanism for ensuring the security of information systems. However, they can not adapt to dynamic environments related to changes in user behavior and changing attacks. It is therefore important to design a new model that will overcome its disadvantages and improve the analyzer of the intrusions detection system. We propose a platform for distributed intrusion detection combining two analyzers (analyzer level 1 and analyzer level 2) based on multi-agent aspect.

OVERVIEW

A system for intrusion detection (IDS Intrusion Detection System) is a mechanism to identify abnormal or suspicious activities on the target analysis (network or host) (Dagorn, 2006). It can have a preventive action on the risk of intrusion and knowledge on successful attempts failed as intrusions. This analysis can be performed on various types of data (network traffic, files, statistics, etc..).

Depending on where they monitor and what they control, two main families are usually distinguished [3,4]:

- ✓ The N-IDS (Network Based Intrusion Detection System), allows the analysis and interpretation of packets on a network.
- ✓ H-IDS (Host Based Intrusion Detection System), provides security at the host.

Many tools use techniques of intrusion detection following:

- ✓ The approach "behavior" is to define a monitored system behavior will be considered as normal and any deviation from the observed behavior of reference is reported as suspect.

- ✓ The approach "scenario" to search for types of events characterizing a known attack. It involves using a database containing specifications of attack (attack signatures).

Most intrusion detection systems are based heavily on analysis based on rules that characterize the known types of intrusion to launch an alarm if the activity observed corresponds to one of its rules encoded. This type of analysis is intended to detect attempts to exploit known vulnerabilities of security systems monitored.

ISSUE

Existing intrusion detection systems have been designed for environments and well-defined and do not offer a solution to some features of networks such as the changing behavior of users and services, the complexity and the increasing trend types of attacks to which they may be subject, the speed of attacks that can occur simultaneously on several machines (Boudaoud, 2000). They are therefore not suitable for dynamic environments.

Many network attacks are characterized by abnormal behavior in various network elements (servers, routers,..). It is therefore very important to distribute the functions of detecting several entities that oversee different parts of the network.

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.

SYSTEM ARCHITECTURE OF INTRUSION DETECTION PROPOSED

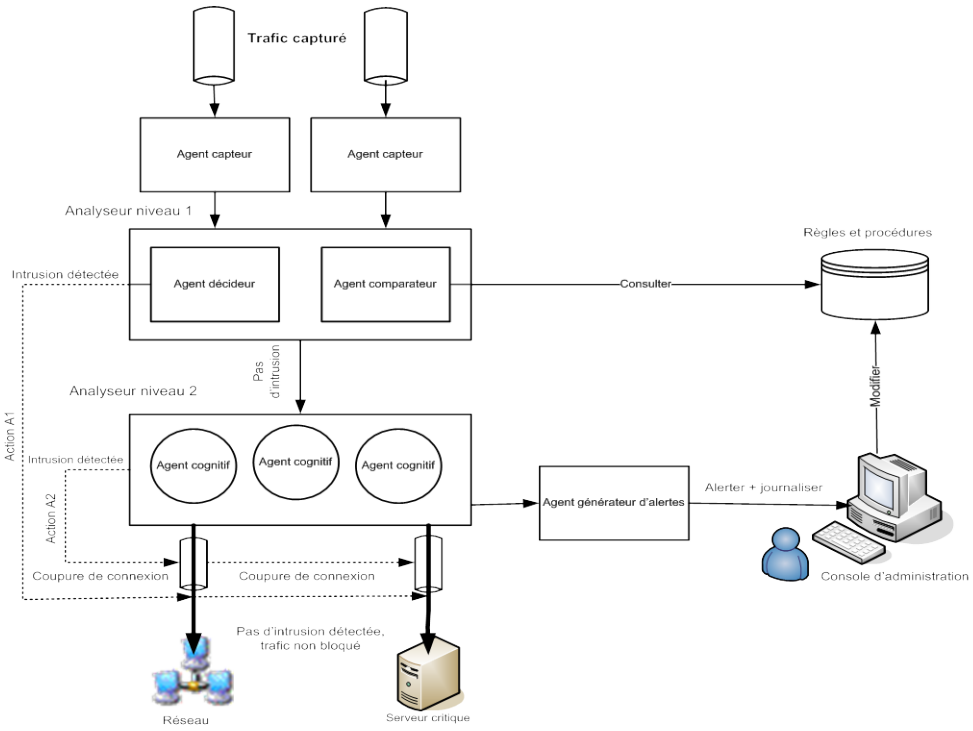

Figure 1: Schematic of the intrusion detection platform proposed

PRINCIPLE OF OPERATION

We propose a new model of security and intrusion detection based on a distributed approach using multi-agent system for receiving intelligence of these agents. It is formed by agents with the capacity to react quickly reactive against known and agents with the cognitive abilities to detect also unknown attacks and has two analyzers:

- ✓ Analyzer Level 1: based on an architecture of multi-agent system formed by reagents (comparator agent and officer decision-maker), his role is to analyze the flow of information collected by the sensor agent. Agent "comparator" responsible to confront traffic captured with signature-based and the degree of threat that may represent the intrusion and the rules and procedures that were applied to the analyzer agent "decision maker" will block or allow traffic continued its path to the parser level 2.
- ✓ Analyzer Level 2: composed of cognitive agents is responsible for studying the behavior of the target monitored and who will conduct further analysis of data and subsequently decide to block or no traffic and generate an appropriate warning.

PERFORMING A SIMULATION PLATFORM

✓ Design of 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 notions agent. Agent UML inherits representations proposed by UML (Huget, 2002). The design of the proposed architecture is described through the two class agents and sequence diagrams to illustrate respectively the static and dynamic aspect of the developed platform.

- Static aspect

We are interested in 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 of Figure 2 represents the conceptual level platform to develop.

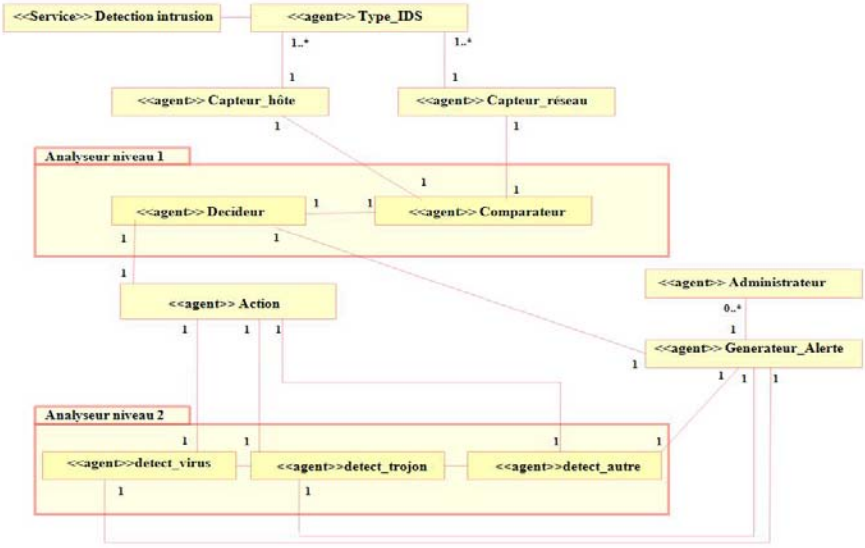

Figure 2: Conceptual level class agent diagram

The *implementation level* gives details of the contents of agents.

Figure 3 shows a portion of the class agent diagram for the agents “capteur”.

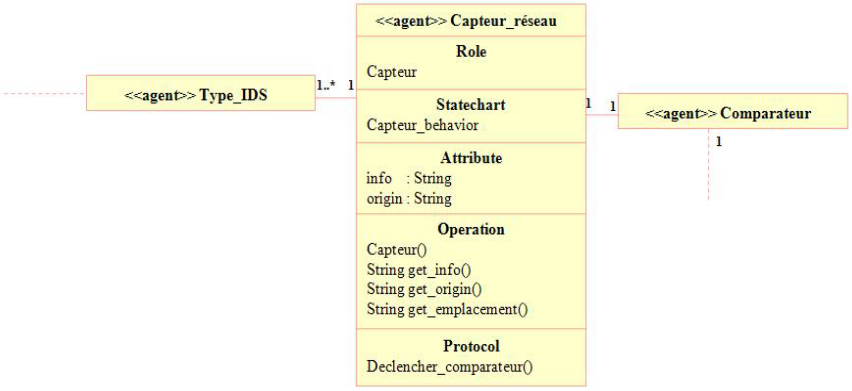

Figure 3: Implementation level of the agent “capteur”

- Dynamic aspect

The sequence diagrams in AUML represent message exchanges between agents.

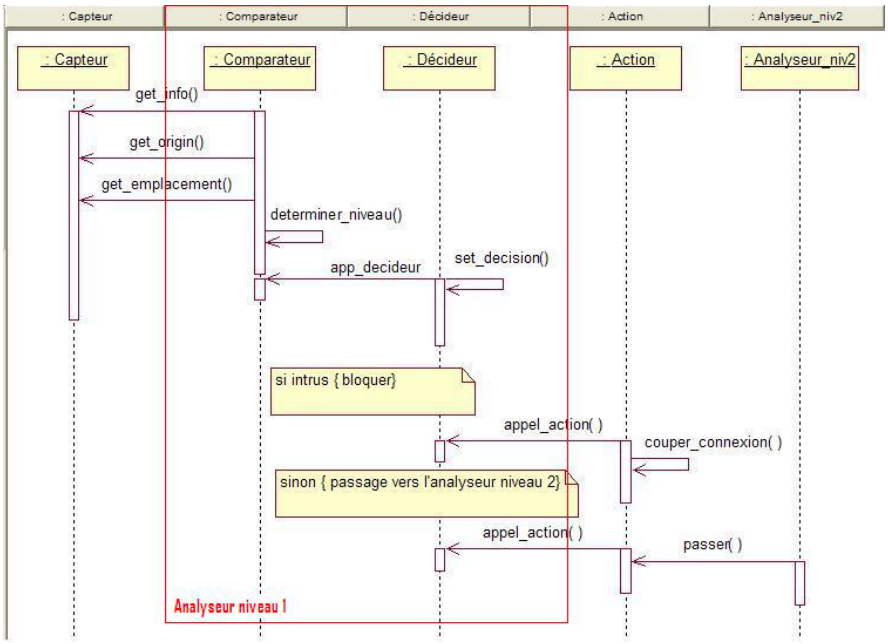

Figure 4: Sequence diagram

The sequence diagram given in Figure 4 shows the interaction between different agents in time.

✓ Achievement

After the design phase of the proposed model, we used an open source distribution(Java and Linux) to develop the new system intrusion detection and we conducted a simulation platform that reflects the goals already set.

CONCLUSION

In this article we have presented a model of intrusion detection brought by a distributed architecture based on the intelligence of the multi-agent system allowing both to react rapidly against complex attacks and evaluate the state of flows relative to predefined rules and procedures and other hand, further research on intrusion which may represent low threat and therefore enhances the level of security provided to the target monitored using cognitive agents of the second analyzer.

REFERENCES

Solange, G. (Octobre 2004). Sécurité informatique et réseaux. Edition DUNOD

Dagorn, N. (2006). Détection et prévention d'intrusion : présentation et limites. LORIA.

Müller, K. (Mai 2003). IDS – Systèmes de Détection d'Intrusions, Partie I. http://www.linuxfocus.org/Français/May2003/article292.shtml.

Müller, K. (Juillet 2003). IDS – Systèmes de Détection d'Intrusions, Partie II. http://www.linuxfocus.org/Français/July2003/article294.shtml.

Boudaoud, K. (2000). Un système multi-agents pour la détection d'intrusions. LIP6-OASIS.

Huget, M. (2002). Une application d'AgentUML au Supply Chain Management. JFIADSMA.