Distributed Intrusion Detection System based on Anticipation and Prediction Approach

Hajar Benmoussa, Anas Abou El Kalam and Abdallah Ait Ouahman
Oscars Laboratory, Cadi Ayyad University, ENSA Marrakesh, Marrakesh, Morocco

Keywords: Intrusion Detection System, Anticipation and Prediction Strategy, Agent, Distributed Architecture.

Abstract: Despite the importance and reputation of the current intrusion detection systems, their efficiency and effectiveness remain limited as they rely on passive defensive approaches. In fact, when an intrusion is detected by the IDS, it is already happened on the network and the time required to update security rules is usually short, which provide opportunity to the attacker to inflict damages that may paralyze the network. For this purpose we suggest a new approach of distributed intrusion detection system to wisely anticipate and predict intrusions before their first occurrence in the network to secure. Our approach is based on intelligent agents and using honeypot technology to gather a vast scope of information about attacks. Moreover it combines the two detection strategies "anomaly approach and misuse approach".

1 INTRODUCTION

The rate of cyber attacks has increased in the last few years. Attackers become experienced and more agile. They rely on mainly sophisticated and diversified techniques and strategies. Therefore, various attacks occur every day and threaten the security of networks and systems. According to IBM X-Force 2013 Mid-Year Trend and Risk Report, 4,100 vulnerabilities were detected by vendors, researchers and independents in the first half of 2013. Under these circumstances, there is a great need for several lines of defense mechanisms such as security policies, firewalls and Intrusion Detection Systems (IDSs). However, current IDS(s) rely on passive defensive approach and simply alert the administrator of attempted attacks against his network or system. Subsequently, the huge number of alerts to analyze and the amount of time required to update security rules after analyzing alerts provides time and opportunity for the attacker to compromise the network. We thus believe that in the air of cyberterrorism, cybercrime and cyber Wars, classical IDS(s) are not really efficient as they should have the ability to wisely anticipate intrusions before their first occurrence in our network.

In this paper, we propose a new approach of distributed intrusion detection system (IDS) to protect our network against potential targeted attacks. We base our approach on intelligent agent technology to achieve intrusion detections and on honeypot technology to gather a vast scope of information about attacks. This paper is organized as follows. We present in the first section the comparison between the centralized, hierarchical and distributed architecture of intrusion detection system. In the second section, we describe our proposed system and we outline the different components. Finally, we discuss in details our work.

2 ARCHITECTURE OF INTRUSION DETECTION SYSTEM BASED ON AGENT TECHNOLOGY

Intrusion detection system (IDS) plays an important role in monitoring and analyzing events occurring in a computer system or network. In some works, authors describe intrusion detection system as a detector that processes information coming from the system that is to be protected (Debar et al., 1998). Basically, intrusion detections systems can basically be described in terms of three functional components:

- Data capture module: is responsible for the collection of data and for sending it to the

Benmoussa H., Abou El Kalam A. and Ait Ouahman A..
Distributed Intrusion Detection System based on Anticipation and Prediction Approach.
DOI: 10.5220/0005556803430348
In *Proceedings of the 12th International Conference on Security and Cryptography* (SECRYPT-2015), pages 343-348
ISBN: 978-989-758-117-5

analysis module.

- Analysis module: is the core of the intrusion detection system. It analyses events and data gathered by the data capture module.
- Response module: applies countermeasures to the system according to the generated alarms.

In this context, many schemes have been proposed to perform collection and processing of information in intrusion detection systems. Basically, these schemes can be classified into three categories: centralized approach, hierarchical approach and fully distributed approach.

2.1 Centralized Architecture

Centralized systems have only two components in their architecture: data collection components and a single central analyzer that performs analysis of the information received from each data collection component. Collection data can be distributed but correlation is centralized. There are many works that focus on distributed collection and centralized correlation, like DIDS (Distributed Intrusion Detection System) (Snapp et al., 1991) and IDA (Intrusion Detection Agent) (Asaka et al., 1999).The main shortcoming of centralized architecture is the central analyzer which presents a single point of failure and a single target for an attack. In fact, if the central analyzer fails or is attacked, the whole system is compromised. Moreover, communication with the central component can overload parts of the network (Kannadiga and Zulkernine, 2005; Zhou et al., 2010).

2.2 Hierarchical Architecture

This architecture has been proposed to deal with disadvantages of centralized systems. It is composed of multiple layers organized in a hierarchical structure. Each layer performs a set of intrusion detection task. Data collected locally is passed to higher level in the hierarchy for further analysis. AAFID (Autonomous Agent for Intrusion Detection) and RL-IDS (Reinforcement Learning IDS) are examples of hierarchical IDS (Servin and Kudenko, 2007; Zamboni et al., 1998). The hierarchical architectures scale better than the centralized approaches (Zhou et al., 2010). However, it's still vulnerable because of reliance on its hierarchical structure. Attackers can cut off a control branch of the IDS by attacking an internal node or even decapitate the entire IDS (Li et al., 2004).

2.3 Fully Distributed Architecture

Fully distributed systems are used to address some limitations of the two first generations described above. In this architecture, each component of the IDS has two function units: a detection unit responsible for collecting data locally and a correlation unit that is a part of the distributed correlation scheme (Zhou et al., 2010). When a node needs specific information it directly sends this request to another node and the processing is done locally. Most of recent fully distributed systems are based on the technology of mobile agent (MA) for example DIDMA (A Distributed Intrusion Detection System Using Mobile Agents) (Kannadiga and Zulkernine, 2005) and MADIDF (Mobile Agents based Distributed Intrusion Detection Framework) (Ye et al., 2008). This architecture has some advantages compared to centralized and hierarchical approaches. Mainly, distributed architectures do not have single point of failure. Also, instead of having a central monitoring station to which all data has to be forwarded, there are independent entities performing collection and analysis of data. This provides better scalability of the system (Zhou et al., 2010).

3 OUR PROPOSED SYSTEM

Whatever the used architecture, centralized, hierarchical or distributed, the efficiency and effectiveness of classical IDS remain limited. In fact, when an intrusion is detected by the IDS, it is already happened on the network and the time left to administrator to update security rules to fix the problem is usually short, which leads directly to undertake damages of the attack which may paralyze the network. If this same attack takes place it may be blocked; but, what about the first occurrence?

The main idea of our solution is inspired by what happens in real war. Instead of remaining on defensive and waiting for the enemies, it is sometimes more interesting to go on the offensive, especially in the age of cyberterorism; as the saying goes: *who stays in the defensive does not make war, he endures it.* In this way, we move from the passive defense position to an active and intelligent. The aim is thus to wisely anticipate intrusions and legally act before they occur on our network.

Based on this new research direction, our first approach expected using mobile agents able to act upstream and infiltrate into suspicious networks in order to collect a maximum of information which will be transferred to the manager within our network. However, this behavior may be considered as illegal. We subsequently explored another idea based on collaborative and distributed honeynet deployed in many universities in morocco. Those universities play the role of our collaborator networks. Each honeynet is targeted by many attacks that are stored in the log file. The latter will thus very helpful in our context to gather and analyze a vast scope of information about attacks.

Note that a honeynet is a special kind of high-interaction honeypot. It extends the concept of a single honeypot to a highly controlled network of honeypot. A honeynet is a specialized network architecture configured in a way to achieve data control, data capture and data collection (Mairh et al., 2011).

Furthermore, we use agents that are inherent to the characteristics of multi-agents system. They in fact have the following features:

- Cooperation: it means that agents work together to solve intrusion detection task.
- Coordination: The coordination of the actions of agents ensures coherence of the system.
- Delegation: it is the ability of an agent to execute tasks for a third party.
- Communication: agents must be able to communicate with each other to cooperate and coordinate their actions.
- Effectiveness: collected data must be accurate and represent often a malicious traffic. The agent must be able to distinguish a malicious traffic (representing threats) from normal traffic (minimum of false positives).
- Security: the agent must be able to communicate with other agents and the manager. This communication must absolutely be encrypted and digitally signed to ensure that data will not be listened to, on one hand, and that the manager can ensure their authenticity and their origin on the other hand.

To satisfy these properties, we believe that the agent technology constitutes an interesting mechanism for developing our distributed intrusion detection system and offers a lot of flexibility.

3.1 Overall System Architecture

At first, given the advantages of distributed system compared with centralized and hierarchical architectures, we design our intrusion detection system based on distributed detection approach. Our system consists of two separate parts. The first one is the network to secure which contains the manager agent and the second one is composed of a set of collaborator networks which deploys honeynet platform. Basically, each collaborator network is made up of four major components as shown in Figure 1: sensor and three static agents cooperative and communicating: parser agent, misuse detection agent and anomaly detection agent. Moreover the two networks have a local signature database.

In the following, we describe each component of the proposed architecture:

- Sensor: installed on each collaborator network, it is able to intercept and log traffic passing over the network. Afterwards, it saves the captured packets in a sniffing file.
- Parser agent: it is a static agent which parses data and distinguishes the various fields of the collected packets such as source /destination addresses, protocol and other specific information related to the captured packet. The parser agent parses data from two files; (1) the sniffing file which contains the packets already captured by the sensor and (2) the log file containing various actions performed by attackers on the honeynet platform. The output data is saved into the parsing database.
- Misuse detection agent (MDA): This kind of agent is responsible for detecting well-known attacks. In fact, it analyses the parsed data by matching their characteristics with those contained in the rules stored in the signature database. If there is a match - which means it confirms that the attack is known, it reports it as alerts to manager agent. The later updates its signature database. Although the known attacks are detected, it remains the problem of the new attacks detection. In this context, if misuse detection agent does not confirm that the attack is known, which means the packets do not contain intrusion's signature, it sends it to the anomaly detection agent. To detect known attacks, misuse detection agent uses snort signature database. Snort is a free lightweight network intrusion detection system, configured with an intrusion signature rule set to detect known attack pattern.
- *Anomaly Detection Agent (ADA)*: It is responsible for detecting unknown attacks. When it detects unknown attacks, it reports it as alert to manager agent and it updates signature database.
- *Manager Agent (MA)*: Installed on the network to secure, when it receives alerts from Misuse detection agent and anomaly detection agent, it updates its signature database.

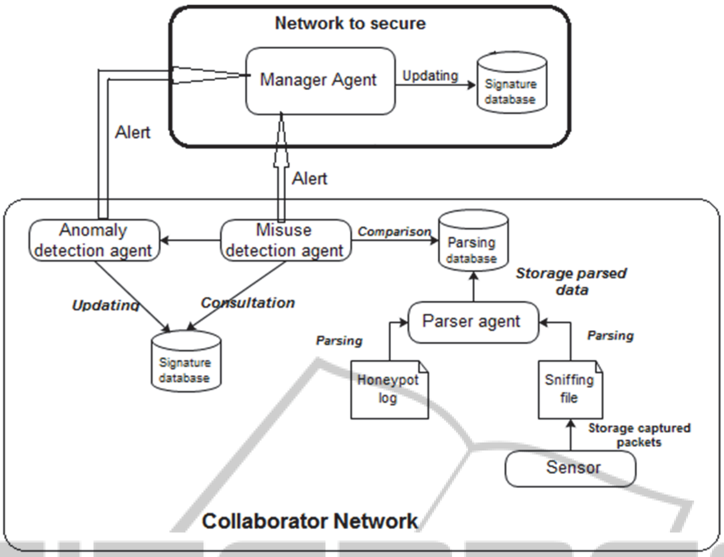

Figure 1: The global architecture of our proposed IDS.

Moreover, Manager agent plays the role of an agent interface to provide the final information to the security administrator. The latter can then take appropriate measures to protect his network before the attack takes place.

3.2 Challenges of Our Proposed IDS

3.2.1 Our Proposed IDS versus IPS

Intrusion Prevention Systems (IPSs) seem to be a solution that can compensate the IDS(s) passivity as they intervene immediately and actively to foil the attack attempt. IPS(s) can respond to a detected threat by attempting to prevent it from being successful. However, they are not strongly recommended because of false positives which may identify a legitimate and normal activity as malicious. Indeed, attackers often make IPS to block a legitimate traffic when they detect its presence in the attacked network. There is even a largely used attack where the attacker spoofs a production server address (or important node in the network), then execute an attack in his name. This will push IPS to banish and isolate this legitimate server (victim) from the rest of the network. For these reasons, IDS(s) are generally preferred to IPS(s). In this context, many works concerning comparative studies of IDS are being pursued (Ahmed et al., 2009).Our proposed system can prove to be an invaluable tool, where its goal is to anticipate and predict intrusions before their first occurrence in the protected network. The prediction is done through knowledge of different attacks and intrusions detected on the collaborator and then take appropriate measures to protect the network to secure (our network) before the attack takes place.

3.2.2 Our Proposed System versus Current IDS(s)

The major difference between our proposed system and current IDS(s) is the active defense strategy. Instead of waiting for the attacks to detect it (strategy of the current IDSs), it is more interesting to anticipate intrusions before they are addressed to our network by detecting and analyzing them on the collaborator network, and then take appropriate measures to protect our network(the network to secure) before the attack takes place.

Moreover, our IDS is hybrid, it combines the two detection strategies; misuse approach and anomaly approach to exploit their advantages and overcome the drawbacks corresponding to each of them while the most existing distributed IDS(s) based on agent, use a single detection strategy. Furthermore, other works (Kannadiga and Zulkernine, 2005; Ye et al., 2008) which are based on mobile agents don't give any information about the approaches and techniques used to detect suspicious activities.

On the other hand, in contrast to the existing works which use only log files as sources of data to detect any signs of intrusions, this work uses both the log file which contains the packets already captured by the sensor and the honeypot log file which contains various actions performed by attackers on the honeynet platform**.**

3.2.3 Interaction and Communication between Agents

To communicate, the different agents described above use the ACL (Agent Communication Language) language which is defined by FIPA (FIPA: Foundation for Intelligent, Physical Agents). The message communication in JADE is asynchrone and implemented as an object of the jade.lang.acl.ACLMessage class that provides get and set methods for accessing all fields specified by the ACL format.

Sending and receiving messages to/from another agent is as simple as filling out the fields of an ACLMessageObject and then call the send () method (to send message) and the receive () (to receive message) or blockingReceive () method.

The code below creates a message sent by Misuse detection agent (MDA) to Manager Agent in order to inform it about the signature of detected attack.

```
   ACLMessage message = new ACLMessage
(ACLMessage.INFORM);
   message.addReceiver (new AID ("ADA",
AID.ISLOCALNAME));
message.setContent ("alert tcp
$EXTERNAL NET any →$HOMENET 21(msg:"FTP
passwd attempt" flags:A+;
content:"passwd";)”);
Send (message);
```

3.2.4 Discussion and Implementation Direction

The architecture of our system contains various intelligent and cooperative agents for the collection and the analysis. It relies on distributed collection and distributed analysis. In fact, there is no central station, therefore no central point of failure. Moreover, thanks to decentralized data analysis, the scalability problem is addressed. Furthermore, the proposal design of intrusion detection system can be easily extended even the number of our collaborator networks increases.

We are working on implementing the system with JADE 4.3.3 (Java Agent Development Framework). This choice is made according to a comparison study of five agent platforms (Singh et al., 2011). JADE is software framework fully implemented in Java language, to make easy the development of multi-agent applications in compliance with the FIPA (Foundation for Intelligent, Physical Agents) specifications. JADE offers flexible and efficient communications between agents and allows good runtime efficiency, agent mobility and the realization of different agent architectures (Bellifemine et al., 2007)

The development of this architecture needs using Sun Java Develop Kit 8, the Eclipse and the open source library JPCAP 0.7 (Java library for capturing and sending network Packets).

As regards Honeypot log file, we are working on Moroccan honeynet project which is based on a distributed system honeynet installed on several universities in Morocco. These later present our collaborator network. We will use the log file containing various actions performed by attackers on the each honeynet.

4 CONCLUSIONS

Current intrusion detection systems are not really efficient because they alert the administrator of attempted attacks already happened on his network or system. Thus, the need of active defense strategy to anticipate and predict attacks before their first occurrence. In this paper we proposed a new approach of distributed intrusion detection system to protect our network against potential targeted attacks. First, we have recalled the three main IDS schemes. Then we have presented the proposed distributed intrusion detection system based on intelligent and active defense strategy. Our architecture benefits from agent technology and distributed intrusion detection capabilities. In a future work, we will finish the implementation of our proposed architecture which will be better in detecting attacks. Moreover we will use correlation techniques to correlate information from a large number of networks to achieve better detection result.

REFERENCES

Ahmed, M., Pal, R., Hossain, Md. M., Bikas, Md. A. N., Hasan, Md. K.: A comparative study on the corrently existing intrusion detection systems. Dept. of Computer Science & Engineering Shahjalal University of Science & Technology Sylhet, Bangladesh 2009.

Asaka, M., Okazawa, S., Taguchi, A. , Goto, S.: A method of tracing intruders by use of mobile agents. *INET '99*, San Jose, USA, June 1999

Bellifemine, F., Caire, G., Greenwood, D., “Developing multi-agent systems with JADE” (Vol. 7). John Wiley. 170, 2007.

C, Li., Q, Song., C, Zhang: MA-IDS Architecture for Distributed Intrusion Detection using Mobile Agents.

In *Proceedings of the 2nd International Conference on Information Technology for Application (ICITA 2004)*.

Debar, H., Dacier, M., Wespi, A.: Towards a taxonomy of intrusion Detection systems. *Computer Networks*, 31(9) pp: 805-822, 1999.

Kannadiga, P., Zulkernine, M.: DIDMA a distributed intrusion detection system using mobile agent. *Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, and First ACIS International Workshop on Self-Assembling Wireless Networks*, pages 238–245, 2005.

Mairh, A., Barik, D., Verma, K., Jena, D., "Honeypot in network security: A Survey," In proceedings of the 2011 *International Conference on Communication, Computing & Security, ICCCS 2011*, Odisha, India, February 12-14, 2011.

Patil, N., Patankar, S., Das, C., Pol, K.: Analysis of distributed intrusion detection systems using mobile agents. In *First International Conference on Emerging Trends in Engineering and Technology*, 2008.

Servin, A. L., D. Kudenko, D.:Multi-agent reinforcement learning forintrusion detection. In *Adaptive Learning Agents and Multi Agent Systems 2007*, pages 158–170, 2007.

Snapp, S. R., Brentano, J., Dias, G. V., Goan, T. L., Heberlein, L. T., Ho, C., Levitt, .K .N., Mukherjee, B., Smaha, S. E., Grance, T., Teal, D. M., Mansur, D.:DIDS (distributed intrusion detection system) - motivation, architecture and an early prototype. In *Proceedings 14th National Security Conference*, pages 167–176, October, 1991.

Singh, A., Juneja, D., Sharma, A. K.: Agent Development Toolkits. International Journal of Advancements in Technology, ISSN 0976-4860, Vol. 2, No. 1, pp. 158-164, 2011.

Ye, D., Bai, Q., Zhang, M., Ye, Z.: P2P distributed intrusion detections by using mobile agents. In Proceedings of the Seventh IEEE/ACIS International Conference on Computer and Information science (ICIS 2008), pages 259–265, Washington, DC, USA, 2008. IEEE Computer Society. ISBN 978- 0-7695-3131-1.

Zhou, C. V., Leckie, C., Karunasekera, S.: A survey of coordinated attacks and collaborative intrusion detection. *Computers & security 2010*, vol. 29, no 1, p. 124-140.

Zamboni, D., Balasubramaniyan, J., Garcia Fernandes, J. O., Spafford, E. H.: An architecture for intrusion detection using autonomous agents. Department of Computer Sciences, Purdue University; 1998.