Journal of Theoretical and Applied Information Technology
29th February 2012. Vol. 36 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NEW APPROACH TO INTRUSION DETECTION SYSTEM

[1]A. KARTIT, [2]A. SAIDI, [3]F. BEZZAZI, [4]M. EL MARRAKI, [5]A. RADI

[1,2,3,4,5] Laboratoire de Recherche en Informatique et Télécommunications, Faculty of Sciences,

University of Mohammed V, Rabat, Morocco

E-mail: [1]alikartit@gmail.com

ABSTRACT

The design and implementation of intrusion detection systems (IDS) remain an important area of research in the field of security of information systems. Despite the undeniable progress, much remains to be done to improve the security of computer networks today. For this, many mechanisms have been developed {[1], [2]}. In general, these systems are vulnerable to attack from unauthorized users (external attacks) as well as attacks by authorized users (internal attacks) who abuse the privileges granted to them. In this paper, our contribution consists of the design of an intrusion detection system based on security policy at three levels. This approach, very interesting even for complex information systems, allows administrators of information systems and responsibles of network security, the protection from external attacks and internal attacks.

Keywords: *Security Policy (SP), Intrusion Detection System (IDS), Alerts Correlation (AC), Data Fusion (DF), Network Security (NS)*

1. INTRODUCTION

In recent years, significant progress has been made towards improving the security of computer systems. Unfortunately, the undeniable reality remains that all computer systems are still vulnerable. These systems are vulnerable to attack from both unauthorized users and attacks by authorized users who abuse their privileges.

In this paper, we propose an approach based on security policy at three levels for complex computer systems. These three levels working together to protect the computer system from inside and outside attacks. This global security policy will allow the administrator security systems not only to detect attacks but also to warn about this intrusion and deny access to all networks.

2. INTRUSION DETECTION SYSTEMS

2.1 DEFINITION

An intrusion detection system (IDS) is a mechanism to detect abnormal or suspicious activity on a given target to address the problems as quickly as possible. Given their practical value, the IDS have been studied heavily over the past 20 years in order to improve their effectiveness. The fruits of these studies are of different classes of IDSs that rely on different detection techniques, each of which is more appropriate for a particular context. Among others, we find the intrusion detection systems that base their decisions on information found in machines called HIDS and intrusion detection systems that base their decisions solely on information flowing in a network called NIDS. More details on the various classes of IDS and their evolution can be found in [3].

2.2 VULNERABILITY OF SYSTEMS

An attack is an exploitation of vulnerability in a system. Thus, reducing attacks can only be done with a good understanding of the system and possible sources of vulnerability in order to find suitable remedies. The word vulnerability expresses all the weaknesses of computer resources that can be exploited by malicious people. In [4], D. Denning explains the presence of vulnerabilities in information systems by, among others, the following reasons:

- ✓ Good security costs usually very expensive and most organizations do not have sufficient budget to afford this need.
- ✓ Security tools used cannot be 100% sure, see that they are often ineffective.
- ✓ Security policies are commonly complex, incomplete and sometimes inconsistent.
- ✓ The bugs in programs that are common and are still exploited by attackers.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- ✓ The weaknesses due to the management and system configuration.

2.3 CATEGORIES OF SECURITY ATTACKS

We know that the main function of computer systems is to provide information and resources to users. Therefore, there is a flow of data exchanged between a source and a destination on a channel.

The task of the security system is to limit access to data and resources only to authorized parties (people or processes) are allowed to use them, according to established security policies. The normal flow of data or information is targeted by several classes of security attacks [5] which are illustrated in figure 1.

- ✓ Interruption: the system is destroyed or becomes unavailable. This is an attack on availability.
- ✓ Interception: an unauthorized party has access to data by listening to the channel. This is an attack on confidentiality.
- ✓ Modification: the data is not only intercepted, but also modified by an unauthorized third party. This is an attack on integrity.
- ✓ Masquerade: the attacker pretends to be a legitimate source, and inserts the data you want. This is an attack on authentication.

2.4 CLASSIFICATION OF INTRUSION DETECTION SYSTEMS

2.4.1 SCENARIO APPROACH

This approach consists to look into the activities of the supervised entity fingerprints or signatures of known attacks. Each of these signatures described an attack very specific and each attack can be detected by one or a sequence of events obtained from one or more sensors (collecting information). These are used to classify the events of attacks that can come from either a host (eg, audit files, track order fulfillment, etc...) or a network. Figure 2 shows a generic model of intrusion detection system suitable for the scenario approach. This is very similar to antivirus tools and has the same drawbacks as these.

It is easy to see that this type of IDSs can only detect attacks that they have the signatures. They also require regular updates to their signature database and their effectiveness depends on the contents of this database. If the signatures are false or improperly designed, the entire system is therefore ineffective. This model is very simple to implement and optimize.

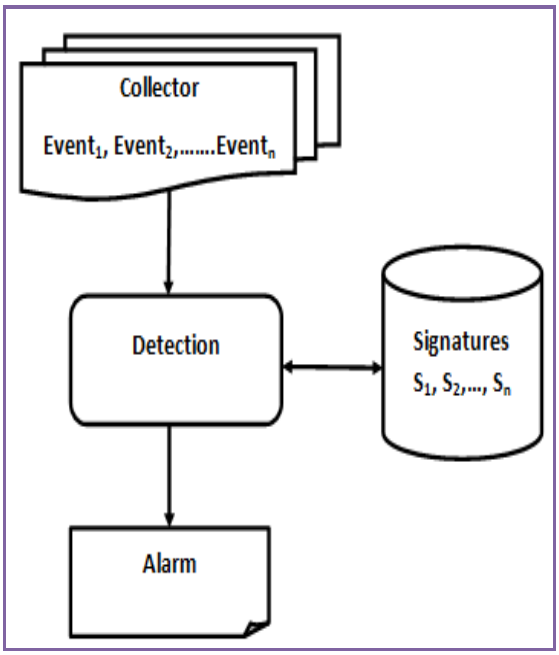

Fig. 2: Detection model for the scenario approach

2.4.2 BEHAVIORAL APPROACH

This approach was proposed by J. Anderson [6] in 1980, then revised and extended in [7] by D. Denning in 1987. It consists to detect if a user has an anomalous behavior with respect to its habits. It uses a statistical model developed by Denning in [7] and it's based on a profile of normal behavior of the user, in light of several random variables. During the analysis, we calculate a rate of deviation between current behavior and past behavior.

If this rate exceeds a certain threshold, the system said it was attacked. For example, an employee working in a company which connects the night at certain times, in addition to the day might bring IDS to report unusual behavior.

The main advantage of behavioral IDS is to detect new types of attacks. Indeed, the IDS is not programmed to recognize specific attacks but to report any abnormal activity. Figure 3 shows an example of a detection model using the approach profile. The latter uses the profile constructed from past events to compare to current events of the collector [8]. However, this approach can lead to many false alarms as it cannot detect certain attacks.

Journal of Theoretical and Applied Information Technology
29th February 2012. Vol. 36 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

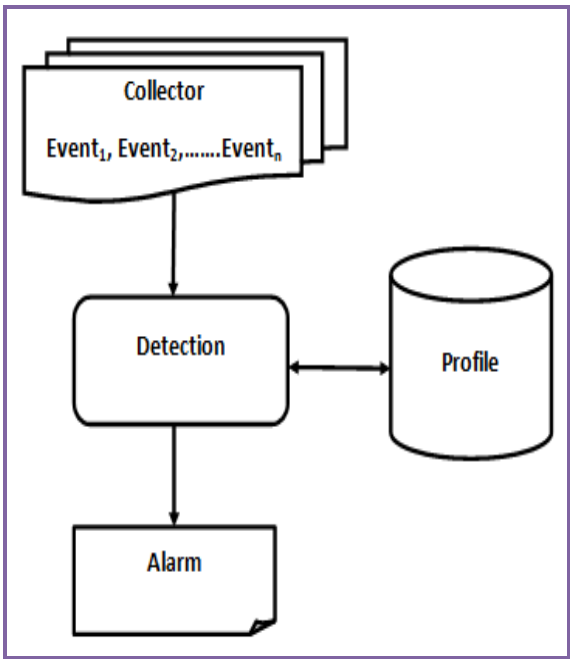

Fig. 3: Detection model for the behavioral approach

3. SECURITY POLICY AT THREE LEVELS

Traditional approaches presented earlier have shown their limitations when they protect computer systems, in particular, from the inside. They secure the network only on the point of entry against attacks from the external network based on a model of normal behavior or database attacks. Where did the idea to seek solutions for the protection of computer systems from unauthorized users and authorized users those permitted to abuse their privileges. The solution proposed in this paper is to develop a global security policy at three levels.

This is an exciting new method that offers new techniques suitable for those responsible for security and enhances network security.

3.1 LEVEL 1: STRATEGIES FOR EXTERNAL PROTECTION

The first level of intrusion detection is to use an intrusion detection system using a well-known classical approach with the advantages of the above approaches. So it will be placed in firewall to prevent network attacks from outside by refusing malicious connection attempts by unauthorized third parties outside.

In our case, we propose an intrusion detection system network based (NIDS) using a database of attacks [9]. The main advantage of a detection system based on knowledge is that it usually produces very few false positives, its limitation is that it cannot detect any new intrusions that do not exist in the database of attacks, and this drawback will be improved in levels 2 and 3, which will help us to detect new attacks. The analysis of these attacks will help us to update our database attacks.

3.2 LEVEL 2: FUNCTIONAL SECURITY POLICIES

The second level of detection is to define functional security policies, which means that policies are based on the tasks assigned to users in the company by the segmentation of the network to VLAN "Virtual Local Area Network" and the use of ACL "Access Control List". We will therefore:

- ✓ Users may communicate and share some resources computer system will be in the same VLAN.
- ✓ The gateway machines from different VLAN will be configured with an ACL defining the list of allowed actions for users who belonged to the same VLAN (all other actions are prohibited) or conversely, other users will not have access to this VLAN. In addition, the VLAN can restrict the scope of contamination of the network. Indeed, if an intruder has successfully taken control of a host, the attack will be limited to a small subnet and cannot infect the whole network.

The main objective of this level is to protect the internal network by malicious internal users may abuse their privileges (insider attacks) and forwards that reach from the outside and infiltrate computer systems by identity usurpation (external attacks).

3.3 LEVEL 3: OPERATIONAL SECURITY POLICIES

The third level of intrusion detection is to define a security policy operating through a mechanism that correlates the information in the list of physical access control to the company and the information from the list of logical access control guests to the user. This means, deny network access to users who are not actually operational (ie those who are absent or permanently resigned) of the company at this time. This control will prevent identity usurpation from inside or from outside to the internal computer network.

These levels of our intrusion detection system can automatically detect violations of security policies.

Journal of Theoretical and Applied Information Technology
29th February 2012. Vol. 36 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The analysis of the behavior of the network in this process will reveal abnormal traffic from a host such as:

- ✓ Attempts to connect to network servers by the user that is not present in the company;
- ✓ Attempts to connect to a machine or resource by unauthorized internal or external users;
- ✓ The detection of attempts to access a computer network or to certain resources by unauthorized users.

3.4 GENERAL ARCHITECTURE AND DIAGRAM OF THE PROPOSED SYSTEM

Figure 4 summarizes the major steps in our system based on security policy at three levels.

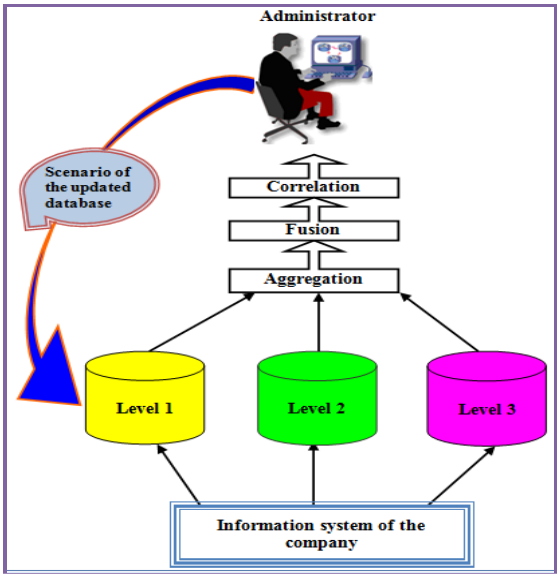

Fig. 4: Architecture of security policy at three levels

We need to collect event logs from three different levels, then we can group, filter alerts chronic and, finally, we can correlate our data to reduce their volumes for ease of analysis and optimization of processing time in search of some intrusions.

In the case of an intrusion of level 2 or level 3, the administrator can group data together to know exactly how events unfolded.

This method is called "event reconstruction" and it is really useful for administrators, because they can:

- ✓ Have a better understanding of the needs of their networks;
- ✓ Identify weaknesses in the system and improve safety policies;
- ✓ Preventing abuse of these weaknesses by malicious internal and external;
- ✓ Update the knowledge base of level 1;
- ✓ We help solve the problem of false positive and negative, to reduce their numbers, thus reducing the number of alerts and speed up the processing thereafter;
- ✓ Improve, continuously, the performance of our system.

As shown in the diagram in figure 5, where the traffic packet arrives, it passes through the first level where the IDS is installed. If a packet is intrusive and his script is included in the IDS database, the packet will be rejected, if it is not the case, it passes through the second level where we check the type of service performed or requested by the user behind the machine, if it is allowed to use the requested service or not. If it is not allowed to access the services requested and / or resources, the application will be rejected and the network administrator will be notified by an alert to start the diagnostics, if so, the packet passes through the third level. In this level, we check if the user is present in the company or not. If he is present, so the user will have full access to services and / or resources required. If he is absent, it will not be allowed to access it remotely, the packet will be rejected and the network administrator will be notified by an alert to run diagnostics. The analysis of the intrusive packet provided to the network administrator to determine the origin of the attack with the reconstruction of events to highlight what exactly happened, and implement measures to against this new type of attack and subsequently update the IDS's database of level 1.

4. CONCLUSION

In this paper, we made a description of the different levels of system security policies at three levels:

Level1: consists of applying an external protection.
Level2: consists to implement security policies functional.
Level3: consists to implement security policies operational.

These three levels can help the administrator to prevent intrusion and implement proactive measures to detect a possible attack.

In the future, we will work even on the intrusion detection system at three levels of security that we proposed to improve it and we will try to implement it in a real network of large size.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFRENCES:

[1] Jean-Philippe Pouzol and Mireille Ducassé, Formal specification of intrusion signatures and detection rules, 15th IEEE Computer Security Foudations Workshop (S. Schneider, ed.), IEEE Press, 2002, pp. 64–76.

[2] R. Sekar, M. Bendre, D. Dhurjati, and P. Bollineni, A fast automaton-based method for detecting anomalous program behaviors, SP '01: Proceedings of the 2001 IEEE Symposium on Security and Privacy (Washington, DC, USA), IEEE Computer Society, 2001, p. 144--155.

[3] Mé L. et V. Alanou. Intrusion detection: A bibliography. Technical Report SSIR-2001-01, Supélec, Rennes, France, September 2001.

[4] D. Denning. Protection and defense of intrusion, presented Presented at Conf on National Security in the Information Age, US Air Force Academy, Feb. 1996.

[5] E C. Kruegel, F. Valeur and G. Vigna, "Intrusion Detection and Correlation Challenges and Solutions", Université de Californie, Père Noël Barbara, USA, edition La ©2005 Science Springer.

[6] J. Anderson. Computer security threat monitoring and surveillance. Technical Report 56, Box 40 Fort Washington, pa. 19034, February 26, 1980.

[7] D.E. Denning. An intrusion-detection model. IEEE Trans. Softw. Eng, Piscataway, NJ, USA, 13(2):222-232, 1987.

[8] P. Lespérance. Détection des variations d'attaques à l'aide d'une logique temporelle. Master's thesis, Université Laval, 2006.

[9] Radi, B. Regragui and A. Ramrami, "Establishment of an Intrusion Prevention", University Mohammed V, Rabat, Morocco-VSST'2007 – Marrakech, Morocco.

AUTHOR PROFILES:

Dr. Ali KARTIT received the PhD degree in

network security from the University of Mohammed V, Faculty of sciences of Rabat, in 2011. His research interests include network security and distributed Systems.

Journal of Theoretical and Applied Information Technology
29th February 2012. Vol. 36 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

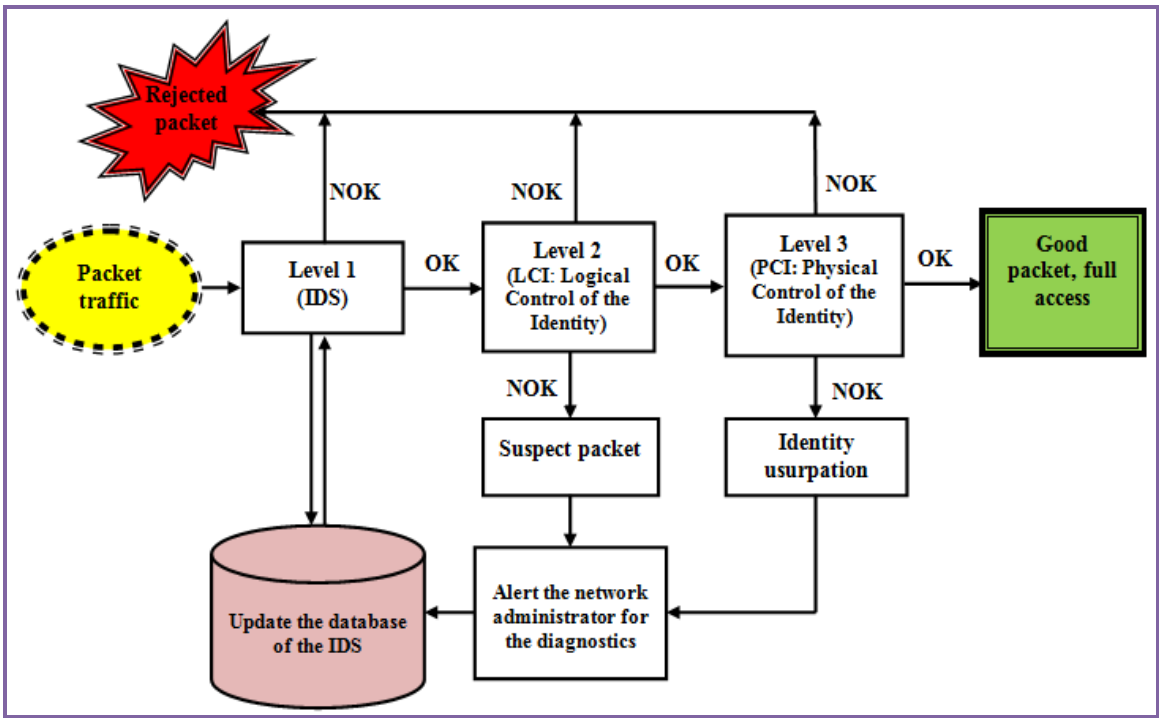

Fig. 5: Diagram of algorithm of security policy at three levels

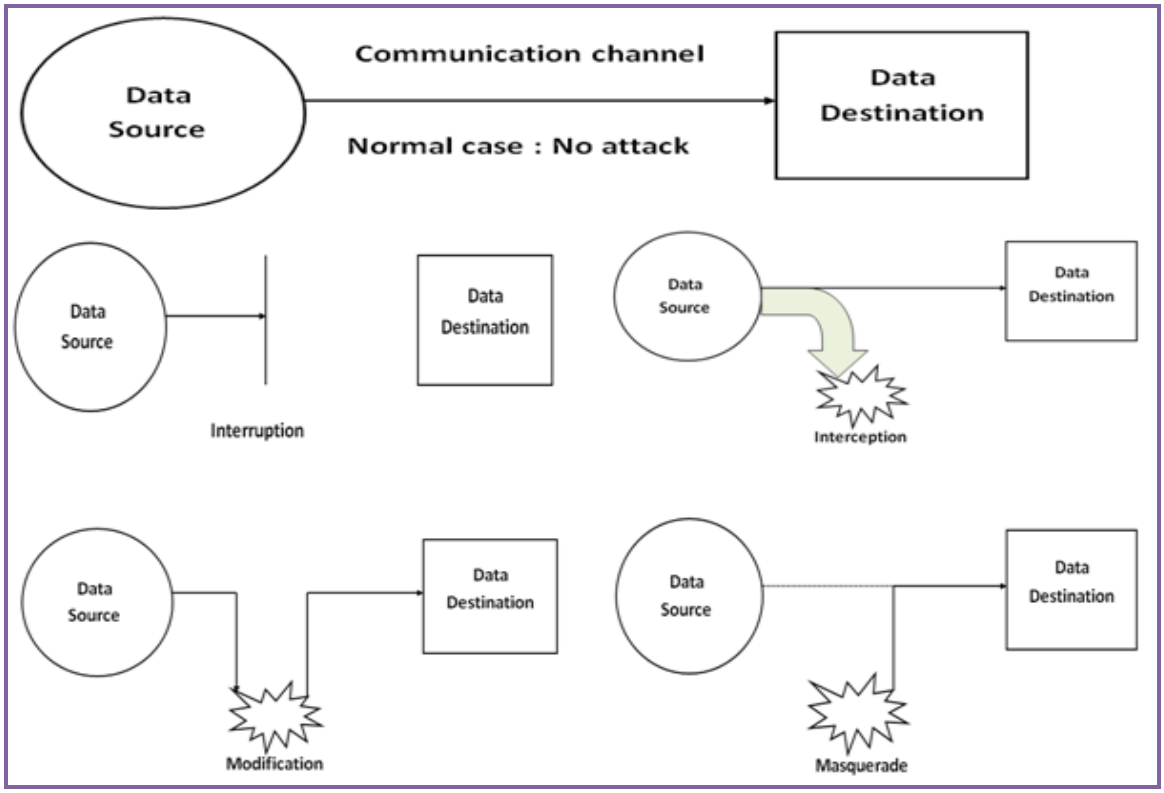

Fig. 1: Types of security attack