AN ENHANCED THREE LEVELS SECURITY POLICY

[1]A. RADI, [2]A. KARTIT, [3]B. REGRAGUI, [4]M. EL MARRAKI, [5]A. RAMRAMI, [6] D. ABOUTAJDINE

[1, 3, 5, 6]Department of Physic, Faculty of Sciences, University Mohammed V, Rabat Morocco
[2,4]Department of Computer Sciences, Faculty of Sciences, University Mohammed V, Rabat Morocco

ABSTRACT

Design and implementation of intrusion detection systems remain an important research issue in order to maintain proper network security. Despite the undeniable progress in the area of computer security there is still much to be done to improve security of today's computer systems and so many mechanisms have been developed to assure its security.
These systems are vulnerable to attacks from both non-authorized users (outsider's attacks) as well as attacks from authorized users (insiders' attacks) who abuse their privileges. Many researches have proved that more than 60% of the attacks come from the inside of the computer systems.
In the previous article [1], we have proposed an exact algorithm for the deployment of security policies for single computer systems but in this paper, we will propose an approach for complex computer systems, base on a three levels security policy. Each level will protect the computer system from both outsiders' attacks and insiders' attacks. This global security policy will allow the administrator of the security systems not only to detect attacks, but also to warn him about this intrusion and forbid access to the whole networks.

Keywords: *Security policy, Intrusions detection, scenario, alerts correlation, data fusion, attack prevention*.

1. INTRODUCTION

The computer systems security aims to protect the access and the manipulation of data and resources by mechanisms of authentication, access control, etc. Nevertheless, with opening and the interconnection of computer systems, bypassing of these security mechanisms is always possible. It is not therefore so sufficient to act preventively, by setting up security policies, in terms of confidentiality, integrity and availability "C.I.A." of data and resources [2] to protect, it is also necessary to be able to detect all violation attempts at this policy, So, we can apply a permanent surveillance of actions undertaken on computer systems in order to assure their legitimacy

During the past few years, significant progress has been made toward the improvement of computer systems security. Unfortunately, the undeniable reality remains that all computer systems are still vulnerable to compromise. These systems are vulnerable to attacks from both non-authorized users (outsiders attacks) as well as attacks from authorized users (insiders attacks) who abuse their privileges. As a result of the global economic crisis, some unsatisfied or dismissed employees who abuse their privileges they had during their period of activity, try sometimes to steal information deserve to be sold or to create problems in the network security.
Thus, different intrusion detection systems or strategies are implemented both as a deterrent and for terminating abusive computer usage once it is discovered.

2. INTRUSION DETECTION SYSTEMS AND METHODS

2.1 Introduction

The intrusion detection has been introduced in 1980 by J.P Anderson; he was the first who shows the importance of the security audit [3] in the goal to detect possible violations of the computer systems security policies. Are added in continuation the works of Denning [4], together put the foundations of the intrusion detection.

2.2 Security Attacks and Properties

If we know that the principle function of computer systems is to provide information and resources to users. Therefore, there is a flux of data exchanged between a source and a destination on a channel.

The task of the security system is to restrict access to data and resources only to authorised parts (people or process) that are allowed to use it, according to established security policies.
The normal flux of data or information is aimed by several categories of security attacks that are illustrated in the figure -1, according to [5]:
- Interruption: system gets destroyed or becomes unavailable.
- Interception: Unauthorized party gets access to data by eavesdropping into the channel.
- Modification: data is not only intercepted, but also modified by an unauthorized party.
- Masquerade: Attacker pretends to be a legitimate source and inserts his desired data.

The four classes of attacks shown in figure-1 violate different security properties of the computer systems (confidentiality, integrity and availability).

2.3 Intrusion Detection Systems

It is not foreseeable to detect intrusions manually because of the huge volume of data events flows that must be analyzed. Intrusion detection systems (IDS) are tools (software and/or material) [2] that analyze traffic flows of the computer network in order to detect automatically non authorized actions done by intruders in the supervised computer systems.
An intrusion detection system must accomplish the following requirements [5]:
- Accuracy: not to detect a legitimate action as malicious actions (called: positive false).
- Completeness: not to miss a true intrusion (called: negative false).
- Performance: to do real time intrusion detection, before some considerable damages are produced on the computer system.
- Resistance: intrusion detection systems would have to be resistant to attacks.
- Scalability: to be able to work in worse case, with a huge number of events without dropping or missing data traffic flow.

2.4 Intrusion Detection Systems Classification

Many intrusion detection systems have been developed up to day. In [6] and [7] we count about hundred of commercial tools in public domain or research prototypes. Criteria used to classify intrusion detection systems, illustrated in figure-2 [8], are:
- Detection methods,
- Behaviour after detection,
- Audit source location,
- Usage frequency.

The two criteria which are the most important: Audit source location (traffic network, audit system and audit applicative) and detection method used [9], which we will detail thereafter.

2.5 Detection Methods

Two kinds of methods are used to detect intrusions:
- Misuse-based Systems: the most used, required a database of attack models called knowledge base which is compared with the audit data collected by the intrusion detection systems and if a match is found an alert is generated, 3. Its main advantage is that it usually produces very few positive false, but can't detect previously unknown attacks which may be harmful and it is difficult to keep the knowledge base up-to-date.

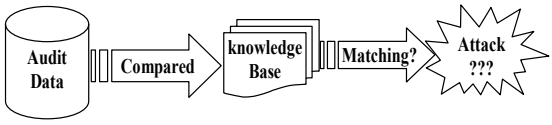

FIGURE -3: DIAGRAM OF TYPICAL KNOWLEDGE-BASED IDS

An example of scenario attack is shown figure-4

```
Alert tcp $EXTERNAL_NET any ->
$IXTERNAL_NET 80
(msg : « WEB-PHP edit_image.php
access » ;
flow:established,to_server;
uricontent:"/edit_image.php";
reference :nessus,11104 ;
reference :cve,CVE-2001-1020 ;
classtype:web-application-activity;
sid:1999;
rev:1;)
```

FIGURE -4: EXAMPLE ATTACK SCENARIO

- Anomaly-based Systems: we first build a model of a normal behaviour of the computer systems and flags as attacks deviations from normality qualified as malicious, as shown figure-5. Its main advantage is that, in theory, it is able to detect unknown attacks but is prone to generate many positive false.

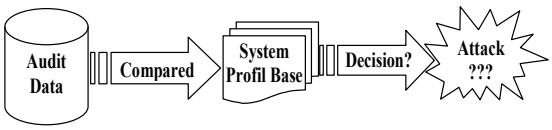

FIGURE -5: DIAGRAM OF ANOMALY-BASED IDS

3. A THREE LEVELS SECURITY POLICY SYSTEM

3.1 Introduction

Traditional approaches presented above have shown their insufficiencies when protecting computer systems, in particular, from the inside. They permit to secure the network only on its entry point against the attacks coming from external network based on a model of a normal behaviour or database of attacks. However, according to several achieved studies [10]:

- 60 to 70% of attacks come from the inside of the computer systems.
- 70% of attacks that cause damages come from the inside of the network (Garthner Inc).
- Enterprises recorded a rise of 44% for the attacks coming from the inside between 2004 and 2005 (IDC and Pricewaterhouse Coopers).

As a result of the global economic crisis, the number of unsatisfied or dismissed employees increases each year. Some time, they can abuse their privileges they had during their period of activity, try sometimes to steal information deserve to be sold to competitor. In 1993, a British Airways company employee was smuggled over the Internet in Virgin Atlantic Airways computer system reservation to obtain the list of passengers who bought first class tickets. These passengers were then contacted by British Airways to cancel their reservations and travel on their own lines with lower price [12].

From where comes the idea to look for solutions providing protection of the computer systems from both non-authorized users (outsiders' attacks) as well as attacks from authorized users who abuse their privileges (insiders' attacks). The solution proposed, in this paper consists in setting up a three levels global security policies. It is a new interesting method that will offer adequate new techniques to the security managers and enhance security network.

3.2 Level 1: External Protection Policies

The first level of intrusion detection consists to use a well known intrusion detection systems using a mono or hybrid classic approach taking advantages of the aforementioned approaches. It will be placed therefore in the firewall to prevent attacks from the outside network by denying malicious connection attempts from unauthorized parties located outside. For our case we propose a network-based intrusion detection system (NIDS) using a database of attacks [11]. The main advantage of a misuse-based detection system is that it usually produces very few positive false, its limitation is that it can not detect possible new intrusions not exist in the database of attacks; this disadvantage will be improved by level 2 and level 3, which help us to detect new attacks. Analysis of these attacks will help to update our data base system.

3.3 Level 2: Functional Security Policies

The second level of detection consists to define functional security policies, which means policies according to tasks assigned to users within the enterprise by the segmentation of the network into VLAN "Virtual Local Area Network" and the use of ACL "Access Control Lists". So:

- Users who are susceptible to communicate and share some computer system resources will be put in the same VLAN.
- Gateway machines of the different VLAN will be configured with ACL defining lists of the actions allowed to users who belonged to the same VLAN (all other actions are forbidden) or inversely, other users won't have access to this VLAN. Also, VLAN will allows - in worse case - if an intruder has succeeded taking control on a host (few number of machines), the attack will be restricted to a small subnet and can't contaminate the hole computer network.

The main objective of this level is to protect inside network from the internal malicious users who can abuse their privileges (insiders attacks) and from outside attackers who manage to infiltrate in the computer systems by usurpation.

3.3.1 Security with Virtual LAN

A VLAN is a broadcast domain created by one or more switches. The network design in Figure-6 shows three VLAN (named: VLAN1, VLAN2 and VLAN3) created by separate switches. The router routes traffic between VLANs using Layer 3 routing. Switches forwards frames to the router interfaces if it is a broadcast frame or if the destination is the router's MAC addresses.

The headline of frame is encapsulated or modified to include an identifier (ID) of VLAN before forwarding the frame on the link between switches (VLAN1-ID=100, VLAN2-ID=200 and VLAN3-ID=300), and the original frame is re-established before forwarding it to the destination host.

3.3.2 Example: Configuration of VLAN

Creates 3 virtual local area networks named: VLAN1, VLAN2 and VLAN3, and identified respectively by numbers 100, 200 and 300. These

VLAN are respectively configured with ip address 131.107.1.1, 131.107.2.1. and 131.107.3.1. This configuration is placed in a router named "rt-test" and a switch named "sw-test".

i) Creation

```
sw-test#vlan database
sw-test(vlan)#vlan 100 name VLAN1
VLAN 100 added:
Name: VLAN1
sw-test (vlan)#vlan 200 name VLAN2
VLAN 200 added:
Name: VLAN2
sw-test (vlan)#vlan 300 name VLAN3
VLAN 300 added:
Name: VLAN3
sw-test(vlan)#exit
Exiting....
```

ii) Show the configuration to verify it

```
sw-test#show vlan

VLAN Name      Status    Ports
---- --------------------------------- --------- ---------------
1 . default    active    Fa0/0, Fa0/1, Fa0/2, Fa0/3,Fa0/4,
                         Fa0/5, Fa0/6
                         Fa0/7, Fa0/8, Fa0/9, Fa0/10
                         Fa0/11, Fa0/12, Fa0/13, Fa0/14
                         Fa0/15, Fa0/16, Fa0/17, Fa0/18
                         Fa0/19, Fa0/20, Fa0/21, Fa0/22
                          Fa0/23
100 VLAN1  active
200 VLAN2  active
300 VLAN3  active
```

iii) Encapsulation

```
rt-test#configure terminal
rt-test(config)#interface fastethernet 0/1.100
rt-test(config-subif)#encapsulation dot1Q 100
rt-test(config-subif)#ip      address      131.107.1.1
        255.255.0.0
rt-test(config-subif)#exit
rt-test(config)# interface fastethernet 0/2.200
rt-test(config-subif)#encapsulation dot1Q 200
rt-test(config-subif)#ip      address      131.107.2.1
        255.255.0.0
rt-test(config)# interface fastethernet 0/3.300
rt-test(config-subif)#encapsulation dot1Q 300
rt-test(config-subif)#ip      address      131.107.3.1
        255.255.0.0
rt-test(config-subif)#exit
rt-test(config-subif)#end
```

3.3.3 Security with Access Control List

Access Control Lists "ACLs" are lists of instructions that you apply to router's interfaces which indicate what kinds of packets to accept or to deny (figure-7). The acceptance or dropping based on specified conditions in the ACL which could be source address, destination address, port number, protocol, or other information

There are many reasons to create ACLs. For example :

- Limit network traffic and increase network performance.
- Provide traffic flow control.
- Provide a basic level of security for network access.

The figure-6 shows mecanisme of access control list. Extended ACLs are more often used than standard ACLs because they provide a greater range of control. We can control, not only, the ip addresses of origin and destination of the packet, but also, We can verify the protocols and port numbers. This gives greater flexibility to describe what parameter checks the ACL.

3.3.4 Example: Configuration of VLAN

The following commands below show as the full syntax's commands of a standard ACL and of an extended ACL whitch are applied to interface ethernet0/5:

- The standard ACL named "Internetfilter" permitted internet access only for user whose machine ip address is 10.1.1.1.
- The extended ACL named "group_1" witch permit packets access using tcp protocol with telnet application and deny packets access using udp protocol with application through port number less than 1024 and notify non authorised services in the log file.

i) Configuration

```
interface ethernet0/5
ip address 192.168.5.1   255.255.255.0
ip access-group Internetfilter out
ip access-group group_1 in
end
conf t
ip access-list standard Internetfilter
permit 10.1.1.1
deny any
ip access-list extended  group_1
permit tcp any 172.30.0.0 0.255.255.255 eq telnet
deny  udp  any  any
deny  udp  any  171.30.0.0  0.255.255.255  lt  1024
deny  ip  any  log
```

ACL emplacement is very important. If the ACL are correctly placed, not only the traffic can be filtered, but the whole network becomes more

effective. Accordding to [1], we can change ACL rules in a correct and safe way.

3.4 Level 3: Operational Security Policies

The third level of intrusion detection consists on the definition of an operational security policies by a mechanism that correlate information from the list of the physical control access to the company and information from the list of the logical access control to the users' hosts. That means to deny access network to users who aren't really operational (i.e. who are absent or definatly dismissed) in the company at that time. This control will stop identity usurpation from the inside or from outside to the internal computer network.

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

The analysis of the behavior of the computer network in this approach will permit to know the abnormal traffic from a host as:

- Connection attempts to the server network by user who isn't present in the enterprise.
- Connection attempts on a machine or non authorized resource by internal or external users.
- Detect attempting access to computer network or to some resources by non-authorized users.

3.5 Implementing Proactive Actions

Most intrusion detection tools are passive, when attacks are detected. Alerts are generated and required the administrator to inspect them manually and take appropriate decisions. Therefore, there can be a significant delay in the process of dealing with an intrusion. With our system, a number of proactive capabilities can be implemented. For example, modify files permissions, kill processes, shutdown network connections or adding and modify firewall rules. As we have shown in[1], firewall rules can added in a safe way. However with traditional system, such automatic countermeasures could caused a deny of service thus number of positive false will increases.

These will improve performances of our system that can some intrusion, and becomes an intrusion prevention system "IPS". So, the analysis of the log file will permit to understand how the intruder could penetrate in the network and the modeling of this scenario will be used for updating of the knowledge database used in the first level security policies. Thereafter our system becomes more sure.

Potentially, this way presents a double advantage:

- A global security policy is explicitly defined, what is not the case with traditional methods.
- The observed audit being compared henceforth to a policy and not only to a knowledge database.

4. INTRUSION DETECTION SYSTEMS AND DATA CORRELATION

We have proposed a three levels intrusion detection system. Thus, every level will provide us some data as alert which is going to burden the administrator's task. In general, analysing all data collected from the network is very difficult and some of the data are useless. To reduce its volume we need to use the data correlation.

4.1 Definition

According to Arian Mavriqi: "Data Correlation means associating sets of events detected through various means and applying knowledge to determine whether they are related, and if so, in what manner and to what degree. This kind of correlation requires comparing observations based on different types of parameters, such as source and destination IP address, and identifianle network route; commands entered by suspected attacker, and the time when activity began or ended. Data sources can be intrusion detection systems, logs, databases"[13]

4.2 Data Correlation

Therefore to have some relevant results of detection, according to the definition, it is necessary to have a lot of data to be able to detect correlated events. To amass so much data as possible, we must use others methods called: Data Aggregation and Data Fusion.

For example: Let's suppose that an intruder arrives to penetrate in the network and attempt to reach a source of data by a targeted machine witch isn't authorized to use this data or resource. In this case, our three levels system L1, L2 and L3 will generate simultaneously alerts. Data fusion will help the administrator to mix alerts containing the same source/destination IP address and port to make only one alert instead of more. Thus, great number of the alerts of our different systems won't be treated.

4.3 Selection of Correlated Information

We can't correlate the totality of data that we collect from our network, because some of them are useless or less relevent and they will overloads the processing of our system.

The NCSA (National Centre For Supercomputing Application) [13], according to a survey done on the collected informations, listed and analyzed the log files of applications more used by network administrators, among these applications: Netflow, DNS, DHCP, http, FTP, SMTP, SSH, Telnet, IDS/IPS, Base of attacks. According to the NCSA, the most important attributes to correlate are:

- Date/heure
- Protocol
- IP source
- IP destination
- Port source
- Port destination
- Packet size

And in addition to our approach, we will need:

- User's name
- User's ID
- User access code
- User's Vlan

5. GENERAL ARCHITECTURE OF THE PROPOSED SYSTEM

5.1 Architecture

The figure 8 summarizes the important steps of our system base on a three level security policies. We need to gather events logs from the three different levels, then we can aggregate them, filter out the chronic alerts and finally we can correlate our data in order to reduce its volume for easy analysis and optimization of processing time looking for some intrusions.

In the case of an intrusion from the level L2 or L3, the administrator can piece data together in order to find out how events have exactly happened. This method is called "Event Reconstruction" and it is really useful for administrators, because they can, thus:

- Have a better understanding of the needs of there system network.
- Identify weaknesses of the system and perform the security policies.
- Prevent the abuse of these weaknesses by insiders and outsiders attackers.
- Update the knowledge base in level 1.
- Help us to solve the problem of positive and negative false, and reduce its number, and therefore reduce the number of alerts and accelerate the processing thereafter, because we can correlate data according to context there are.
- Improve continuously the performance of our system.

5.2 Diagram of the Proposed System

As shown in diagram of figure-9, when packet traffic arrives, it passes through the first level were the IDS is installed. If it is an intrusive packet and its scenario is included in the data-base's IDS, the packet will be rejected, if it isn't, it passes through the 2nd level where we check the type of service performed or requested by the user behind this machine, if he is authorized to use the requested service or not. If he does not have rights to access the requested services and / or resources, the request will be rejected and the network administrator will be notified by an alert to start the diagnostics, if yes, the packet goes through the 3rd level. In this level, we check if that user is present in the company or not. If yes, the user will have full access to services and/or to requested resources. If he is absent, and not allowed to remotely access, the packet will be rejected and the network administrator will be notified by an alert to start the diagnostics. The analysis intrusive packet provide the network administrator to determine the origin of the attack using event reconstruction in order to highlight what have exactly happened, and implemented countermeasures for this new type attack and thereafter, update the database's IDS in the 1st level.

6. CONCLUSION

We have seen that intrusion detection in networks doesn't come to replace the traditional detection security mechanisms but to complete them.

The first part of this paper provided an overview of intrusion detection systems and its role with regard to the network security mechanisms. These systems present its advantages and its shortcomings. To reduce these inconveniences, different ways of research are today explored. Among these, that aims to propose systems that are able to detect automatically security policies violations.

The second part, of this paper, described the different steps of the proposed three levels security policies system:

- Level 1: consist to apply an external protection.
- Level 2: consist in setting up functional security policies.
- Level 3: consist in setting up of operational security policies.

These three levels can help the administrator to prevent intrusion and implement proactive response for detected attack. The implementation

of our proposed three levels security policies system will be the subject of future work. To reduce the administrator daily tasks and take maximum benefit of huge volume of events, we will try to use data mining techniques and intelligent agents.

REFRENCES:

[1] M. El Marraki and A. Kartit, "On the Correctness of Firewall Policy Deployment", Journal of Theoretical and Applied Information Technology, ISSN: 1817-3195, Volume 19, n°1, pages 22 – 27, 2010.

[2] Mr B. Morin, Doctoral Thesis "Alert correlation derived from intrusion detection tools that take into account monitored system information", INSA Rennes, Feb. 2004.

[3] J.P. Anderson, "Computer Security Threat Monitoring and Surveillance", Technical report, Fort Washington - Pennsylvania - Technical Report Contract 79F26400, 1980.

[4] D. Denning, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, 13(2): 222–232, 1987.

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

[6] M. Sobirey, "Intrusion detection systems" page. http://www-rnks.informatik.tu-cottbus.de/sobirey/ids.html. Page web en évolution constante. 1999.

[7] A. Cuff, "Intrusion Detection Systems list". http://www.networkintrusion.co.uk/.

[8] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems", internal RZ 3030, IBM Zurich Research Laboratory, Saumerstrasse 4, CH-8803 Ruschlikon, Switzerland, June 1998.

[9] H. Debar, M. Dacier, and A. Wespi, "A Revised Taxonomy for Intrusion-Detection Systems", Annales des Télécommunications, 55(7-8), 2000.

[10] Revue Mag Securs Novembre 2005.

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

[12] Risks associated to the Internet uses - http://www.filhot.com/vaucelles/, article seen the 20/07/04

[13] B. Morin and H. Debar, "Correlation of Intrusion Symptoms: an Application of Chronicles", 6th International Conference on Recent Advances in Intrusion Detection (RAID'03). Sept 2003. Pittsburgh, USA.

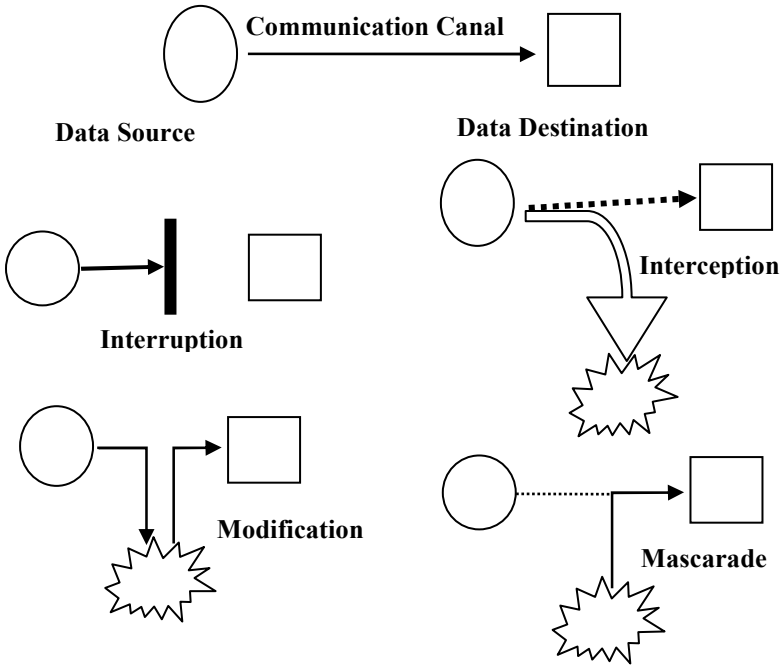

FIGURE 1: CATEGORIES OF SECURITY ATTACKS

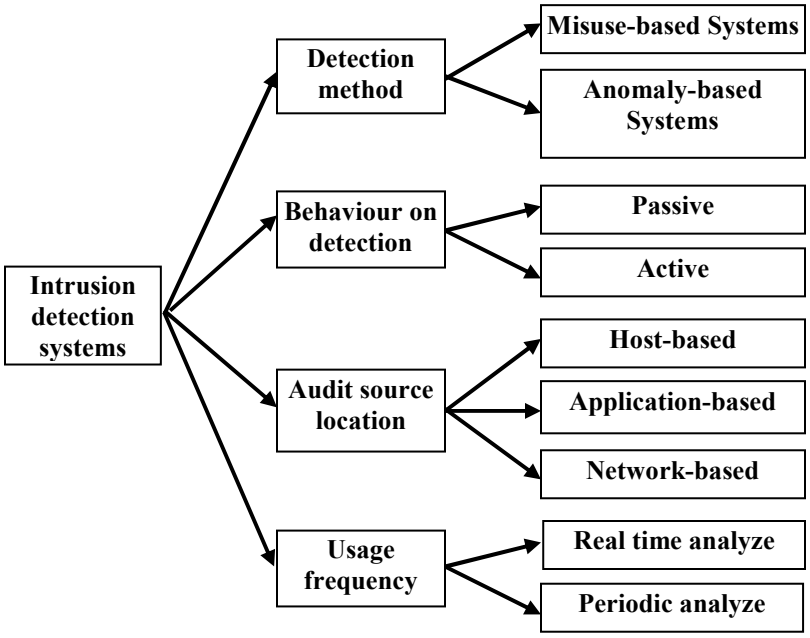

FIGURE -2: CLASSIFICATION OF INTRUSION DETECTION SYSTEMS

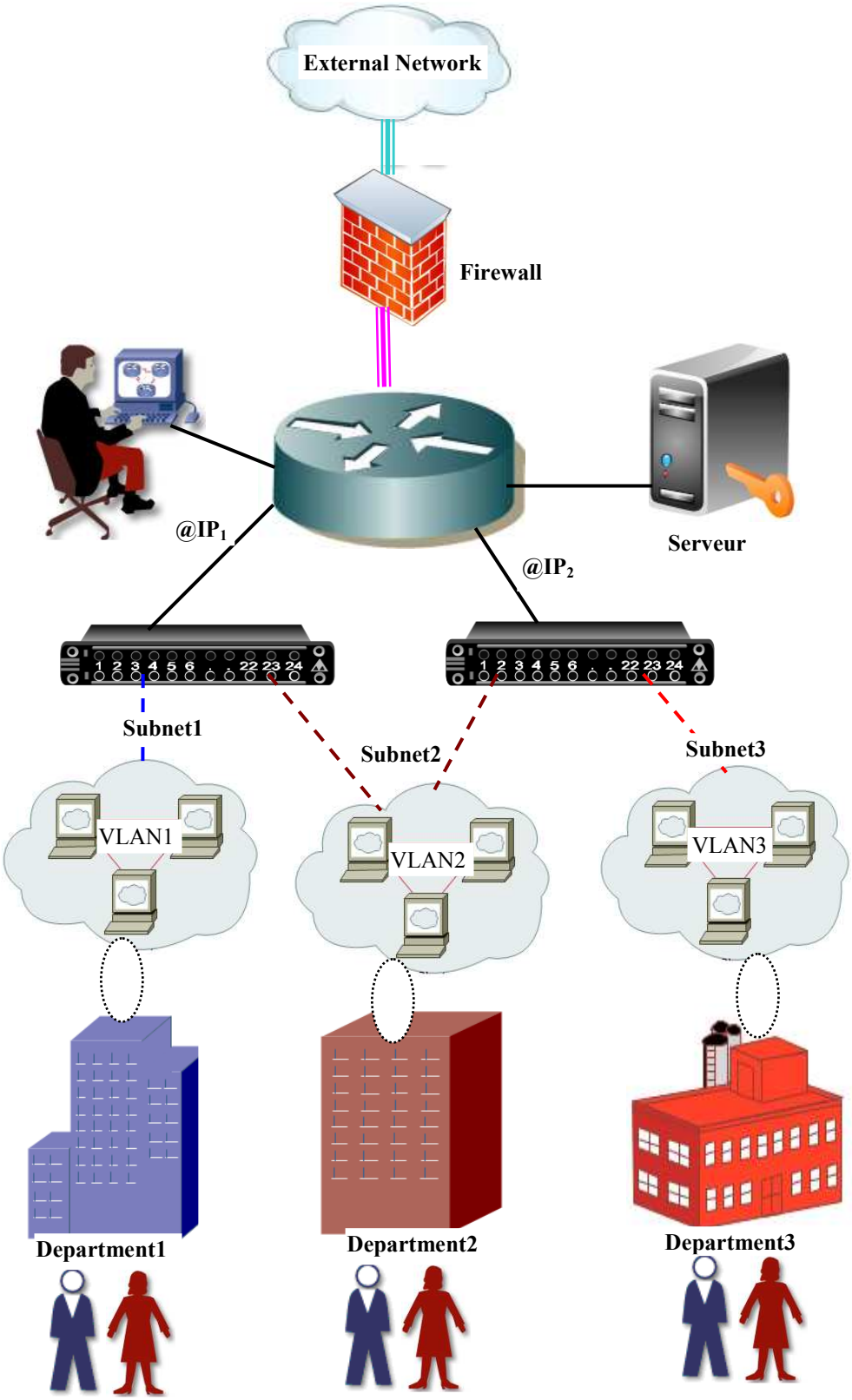

FIGURE -6: ARCHITECTURE NETWORK WITH VLAN

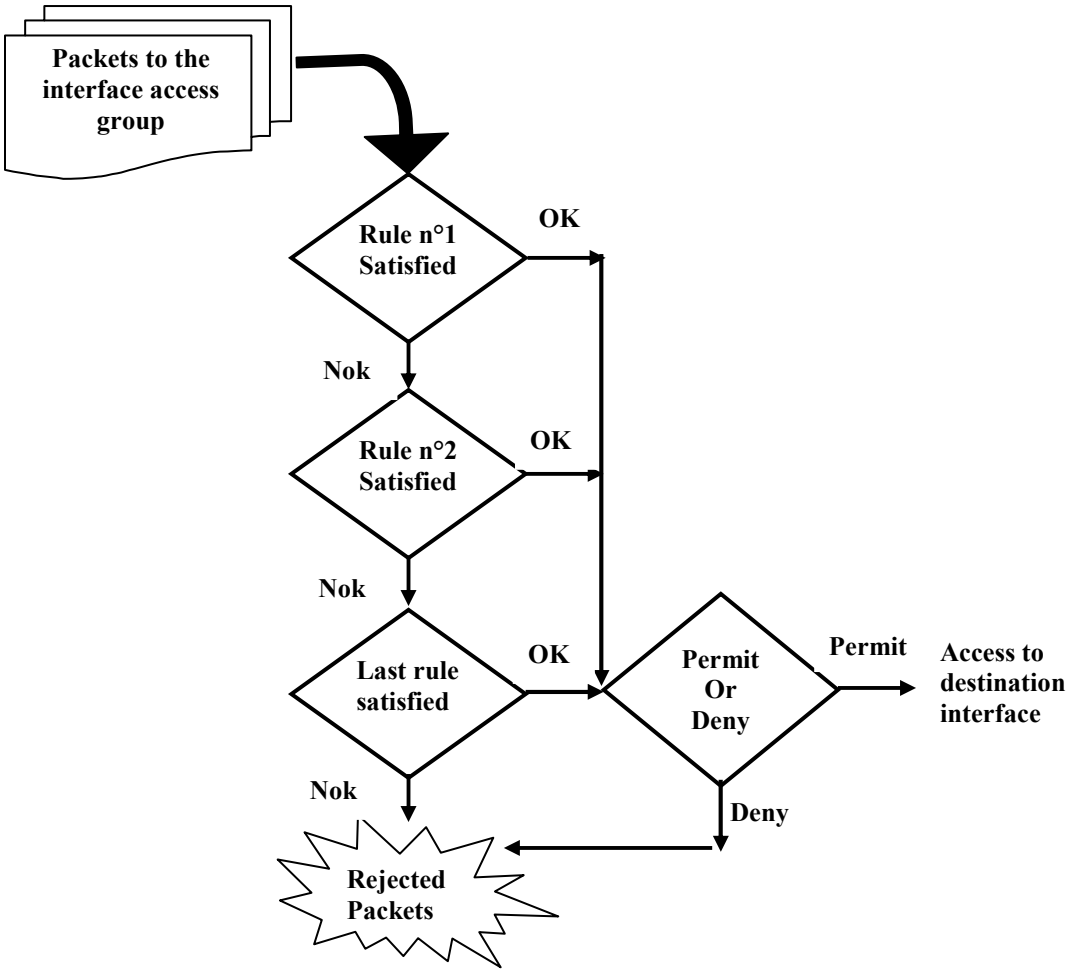

FIGURE -7: FUNCTIONAL ACL DIAGRAM

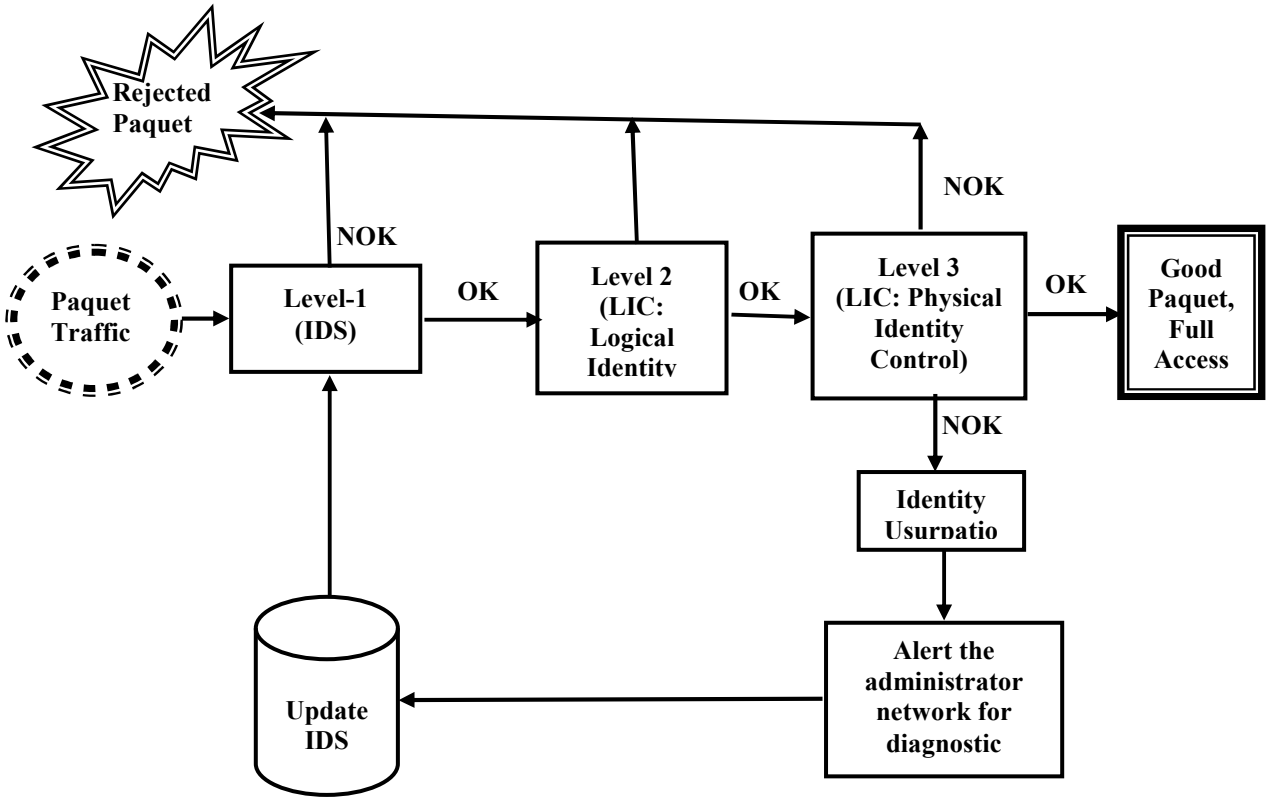

FIGURE-9: DIAGRAM OF THREE LEVELS SECURITY POLICIES ALGORITHM

\

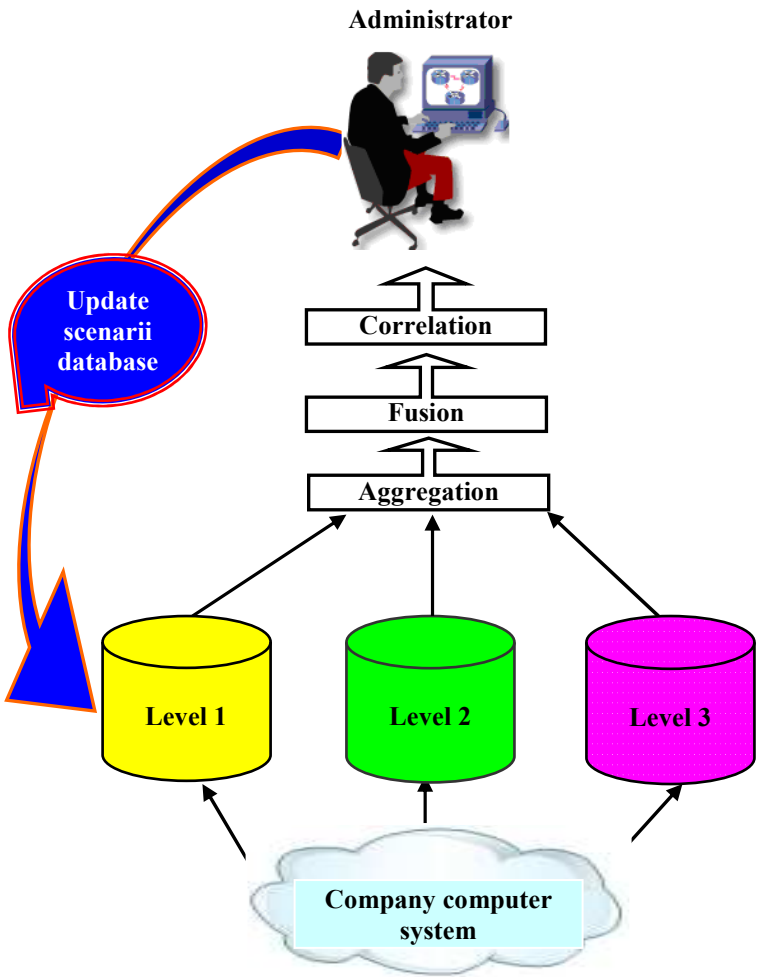

FIGURE -8: ARCHITECTURE OF THREE LEVELS SECURITY POLICIES