GIDRE: Environment of Detection and Answer of Intrusions based on GRID

Olimpia Olguín[†] and Manel Médina[†],

[†]Catalonia Polytechnic University, Department of Computer Architecture, Barcelona Spain

Summary
In the early days the intrusions to data processing systems were little sophisticated but nowadays with the great advance of the new technologies, the intrusions be a lot more difficult to detect causing the need to create capable tools of detecting them as soon as possible, here arises GIDRE, it is innovative development tools for the exhaustive network traffic monitoring of suspicious activities, the data analysis related to these activities, taking decisions and regarding the related security measures establishment to those threats, all it inside the network environment based on GRID. This is a new mechanism, and will be gifted of an express train and efficient answer to the new attacks that appear in the network (for example internet), in the shape of packages filtered (firewalls) that correspond to distribute attacks or not, or they be discovered by the Intrusion Detection Systems(IDS) that they will form the mechanism. It will be obtained, to identify new attacks related to virus and denials of service (DoS); subsequently create update reports about the security state in the network, bringing to light to the community from Internet the information on the new discovered attacks, and in this way take security measures regarding the incidents produced in the systems. Some of the technologies will be utilized are data mining for the analysis of data, and GRID for the compartición of resources in the joint work of the anomalies detectors teams and in their take of decisions. Besides this it will generate countermeasures against these attacks, so much to internal level of the network, as for the international community and finally, they will be generated tools to evaluate the own system efficacy and the structure propagation to other environments. The network traffic capture will be carried out constantly, by means of ADSH (hybrid anomaly detection systems) assembly, which will be distributed through the network. The IDS agents will share information about the anomalies detected in the network, being able to deduce if an global attack is produced in certanly moment.
When an agent monitoring anomalous traffic, it will notify to the other agents, then all agents will analyze the data, and they will decide new politics to apply to the firewalls. These politics, if does not affect to certain system as critical ports, will apply automatically; otherwise, will be done of manual form, informing the administrators and taking the most adequate action.

Keywords
GRID, attacks**,** Firewalls, IDS, ADS.

1. Introduction

Recently, the point of view in the referring to the use of the informatic networks has changed considerably. In recent years, the number of data processing systems has multiplied, and we have passed to an absolute dependence of the these. Unfortunately, the violations of the security of the networks are frequent. The intrusives can burst in a network of many ways –by means of the mail, FTP, NFS or web servers–, eliminating subsequently every trace of its presence. These intrusives can be industrial espionage agents, employed "bribed" or "displeased", suppliers, etc.
Of the previous thing we have observed that the main problem situates in which to the administrators they lack the necessary tools to know when an attack is occurring, how and when the intrusive one is entering the network, what a time ago inside, and how to stop al intrusive immediately or in a future intent.
Nowadays, it given the quantity of incidents occurred, seems increasingly more necessary to observe them of global form and not individually. The stastatistics of incidents detected on the Internet stem from "worms" and "virus" that affect to millions of machines, and that they can serve as platform for another type of attacks that need a large quantity of resources synchronized, like the Denegation of Service Attacks (DoS) whether this an individual attack or distributed. Be faced to this type of threats, that affect not only to individual machines but also to complete networks, turns out to be necessary to include tools that permit a global vision of the problem in real time. This problem only can be resolved creating some system that by means of the aid of the architecture GRID recopile multitude traffic data from diferents points and to centralize all this information in an only point. In this way they would be able to create statistics, to correlate data and to detect massive attacks, attacks synchronized or suspicious activities. The system that permits us to cover all the needs mentioned previously we call GIDRE: Environment of Detection and Answer of Intrusions based on GRID.
In the present is exposed of way detailed in which consists GIDRE, considered as an assembly of machanism for the improvement of the networks. In the section 2 are detailed

the elements that constitute the architecture of the system, subsequently in the section 3 we show the employed topology, in the 4 the operation of the system is explained, in the section 5 the Distributed Architecture is explained, subsequently in the section 6 the graphics of the results are shown obtained and finally the future work, the conclusions, acknowledgmets and references.

2. Architecture of the System

In this section they are defined each one of the elements that form the system architecture: IDS, ADSH, data mining, GRID and Firewall, which they are described subsequently:

a. The Intrusion Detection System (IDS).

The IDS, It began as instrument for the filtered of data in the networks of computers. The IDS include some agents (software) that monitoring the traffic of the network and it activate some alarms when this traffic is anomalous. The type of detection will depend on the IDS that have; the IDS are mainly divided into two types:

a) Host IDS (HIDS), which they protect to final systems or applications of network, auditing systems and the logs of the events.

Network IDS (NIDS), that monitor the traffic of the network to detect attacks.

Our project use the Network IDS. The activity of the NIDS is at the same time divided into three areas [1], that are:

b) Detection of the firm, or protection of known threats.

c) Negation of Service detection: protection against the overload of the network and of the system.

d) Anomaly detection: protection before unknown threats. This last area will be object of our work, since one of our purposes is to find attack unknown and that be not based on existing bosses.

Our proposal will contain various IDS that will be based on the detection by firms and the detection of anomalies; they will be therefore ADSH (Hybrid Anomalies Detection Systems) -in the successive, we will call ADSH to the IDS of our system-. These ADSH, when they detect a suspicious activity (not habitual) in the network, they will communicate among them, and in function of the number of agents that detect anomaly activity, will be concluded that an distributed attack is being produced. On this point, the ADSH´s will analyze the anomalous traffic to discover the nature of the attack and to be able to propose a countermeasure that catch it, through a tool of takes of decisions that will develop.

b. Data Mining.

The data mining, arises like a technology that tries to help to understand the content of a database, seeking patterns, behaviors, groups, sequences, tendencies or associations inside the database that can generate some model that permit us to understand and to interpret better the data to help in a possible one takes of decision.

The data mining meets the advantages of several areas as: the Statistics, the Artificial Intelligence, the Graphic Computation, the databases and the Massive Process, mainly using like commodity the databases.

1. In general terms, the data mining process is composed of four main phases:

2. Determination of the objectives. Tries the delimitation of the objectives.

3. Pre-processed of the data. Refers to the selection, the cleaning, the enrichment, the reduction and the transformation of the databases.

4. Decision of the model. It begins carrying out some statistical analysis of the data, and later a graphic viewing of the same is carries out to have a first approximation.

5. Analysis of the results. It verifies if the results obtained are coherent and the match with them obtained by statistical the analyses and of graphic viewing. In the reference [2], explains of more detailed way the techniques and analysis using in the data mining.

The data mining, will help us mainly to create filters applied to the databases of traffic to detect possible intrusions.

c. ADSH and Data Mining.

The Data Mining[3] use tools specialized to find regularities and irregularities inside a great database. Subsequently some points are mentioned in which has helped the mining industry of data to the intrusions detection systems:

- To Identify generators of false alarms.
- To Find the anomalies that cover the real attacks.
- To Identify the logs, entrance patterns (different types of directions, same activity).

To be able to carry on the previous points, the data mining uses the following techniques:

- Viewing: presentation of a graphic summary of the data.
- Separation (clustering) of the data according to certain categories.
- Association of the rules that go discovering, defining the normal activity and activating the discovery of anomalies.
- Classification: prediction of the category to which a registration belongs particularly.

.

Since an answer in real time to some detections of anomalies is needed, the functionalities of the database should be high: should be it sufficient fast to store alarms and to produce answers to consultations in a simultaneous way.

Besides, large quantities of data will be stored, and will be needed to bring up to date these data regularly.

The integration of the ADSH and the data mining would be generated by the following sequence:

1. The ADSH agents do the capture of the traffic on our GRID that shows you suspect or indications to be of intrusive.

2. These data are stored.

3. These data pass for a prior filter built with the aid of data mining, for the selection of the traffic that be considered anomalous and that be necessary to analyze, to be able to identify the type of a possible attack or a possible intrusion.

4. Subsequently, they are obtained the exit of the filter, which are data that identify a possible intrusion.

The system proposed is an innovative system in the field of the detection of anomalies, since will permit to detect distribute attacks and that be not necessarily attack previously known; that is to say, will permit to discover new attacks or to stop possible suspect of accesses to the network of information before they exist for them patterns that permit to the IDS conventional to detect them.

The team of investigators of the research team in Signs and Communications of the University of Granada is one of our collaborators in the development of this project.

At present the University of Granada has carried out some tests that reflect the integration of the ADSH and the data mining that have as an objective the previus detection of intrusions, these detections have been carried out utilizing models Markovianos [4] and stochastic processes [5] applied to the http protocol in principle and for the future intend that they apply to other protocols.

d. GRID.

A Grid is an infrastructure of hardware, software and services, that provides a cheap, persistent access to capacities of computation and of data. It has as an main objective to share resources, conectividad and heterogeneous among the different networks that conform it.

The architecture Grid is very useful and becomes vital when we need to utilize the functionalities and services of networks that handle different platforms, like they are Linux, Unix, Windows, Solaris, etc. It permits us to see all the system as one alone although be heterogeneous, with which transparency is achieved and homogeneity for the user (to see [6] and [7]). The following figure (courtesy of GRIDCAT-UPC) illustrates the architecture of the GRID. Beginning to describe the Fig. 1 of down up we have that:

- The architecture GRID can be implemented to level of LAN or WAN, among all the organizations that participate.

- Hardware Layer (HW), it does not matter the type of hardware that itself this employing.

- Operating System Layer (SO), the Operating System that be utilized, can be UNIX, LINUX, Windows, etc.

- Middleware Layer is a resources abstraction layer that is executed to level of user (on the operating system) and takes charge of providing the API basic of access to the resources of said machine and to the inverse one, to agree to resources of other machines.

- GRID Applications Layer (Grid Applications), in this layer the applications are placed GRID generated by the developers.

- Web Portals Layer, are the entries developed by users for the friendly management and way Web of the applications Web based on GRID.
- User Layer (User), is the interface for the end user.

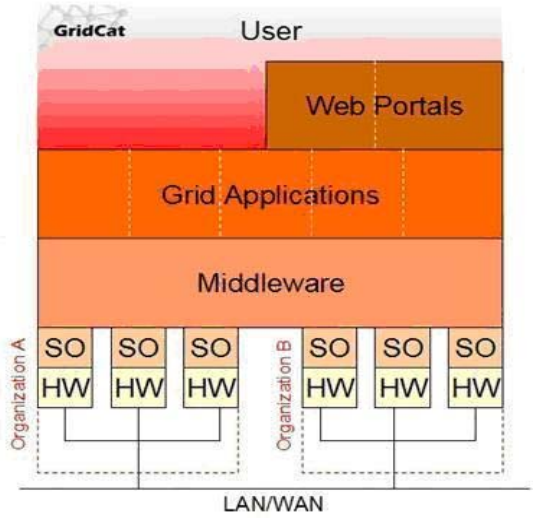


Fig. 1 GRID architecture

The Grid is a structure. Therefore, an interface with the user is needed, so that the users can be handled the resources and services in a transparent way. This it is achieved with the called software Globus Toolkit. That provides services, bookstores and utilities; its documentation and the code are open (to see [8] and [9]).
The version of Globus that we have implemented in our system it is 4.0. The GRID will allow us in our project to have systems heterogeneos systems and in this manner to be able to implement ADSH exactly estrategic points of the net, to obtain a high level itself security in the manipulation of our data, work load distribution al moment to process the data of traffic, immediate answer to the possible violations of security, implementation of the new rules in the firewalls in a way fast and effective, etc

3. Topology

The main topology that be planted for their development is the following one, they will have IDS + ADS distributed for example among various universities as they are: Barcelona University, Barcelona Autonomous University, University technical college of Catalonia, the University Ramón Llull, CERT, etc., (the name of these universities is utilized to illustrate the operation, since for the moment has done only with the local Web Server is inside the esCERT-UPC).
It has a Central Console that is the responsible for carry out all the processes of takes of decisions, that is to say defines if a Global alarm has been caused, distributes the work toward the other elements of the distributed system, distributes the new rules has to be implemented etc.
Besides it has an additional computer that takes charge of generating a copy of the central console, obtaining in this manner high availability in our system. The distributed system was implemented by means of the technology GRID that mainly helps to the distribution of the load of work of some nodes, besides helps to increase the velocity to obtain in a way more fast the results of possible traffic anomalous.

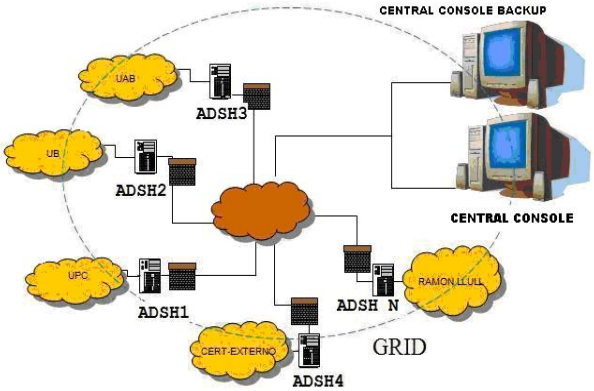


Fig. 2 Topology.

a) ADSH

The ADS will realize some of the following functions, depending on the availability of its resources: ·

- The traffic capture by means of the sensor that has every ADSH.
- Analysis of the traffic that it is capturing to detect one or several Local Alarms. This analysis is realized passing the traffic primarily by the IDS where surely some known attacks will be detected, , subsequently the remaining traffic passes through the ADSH where some possible intrusions are located in a prior way.
- Processing of information from other ADSH that it has excess of work, eliminating hereby the load of work of some ADSHs. ·
- Every ADSH will must analyze a type of protocol and to store the statistics for one time, of the protocol assigned to one entrusts realizing several tasks.

b) The Central Console (together with the backup console)

It is the principal contribution. It coordinates the global operation of the system, of generating the opportune answers and of providing the mechanisms of necessary supervision. Some of those tasks are:

- To Assign an ADSH responsible for each protocol, this ADSH will have a Console of the protocol that was assigned it.
- Supervise operation and connectivity of the ADSH platform.
- Characterize the networks.
- Central Log of Global Alarms of all the protocols that are being analyzed.

c) Firewall

The Firewall will be entrusted mainly to protect the private network by means of the activation of rules that will be modified in a manual way or automatic. This modification of rules will depend on the activation or not of the Global Alarms that be found in all the system. They will be the elements to the ones that they will be directed the majority of the actions of answer.

4. Operation

We will Utilize NIDSs with anomalies detection techniques, which we define previously in the point 2. 1. This type of IDS (Anomaly Detection System) identifies the unknown threats, through the comparison among the traffic of the network in a moment given and the respected traffic as normal activity in the network. When traffic with certain degree of anormality is detected, is activated an alarm and it is identified as an attack. If the attack is also registered for a little high percent of ADSH´s is analyzed, and of this analysis some type of countermeasure will arise to protect the system by means of a change in the firewalls rules, that is to say, the basic data will be generated for generate subsequently a politics of reaction to the attack.
The basic operation of the system is described in the following points (Fig. 3):

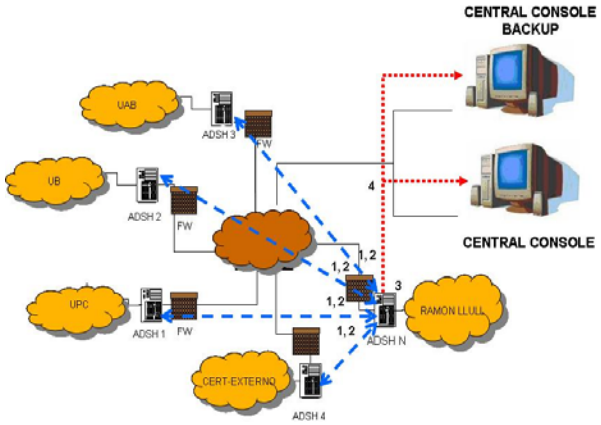


Fig. 3 Operation

a. Assignment of Protocols to the ADSH corresponding

The Central Console will assign to each ADSH a different protocol, since the ADSH1 to the ADSH N.

The Console of the protocol located in each ADSH will generate and collect the Local Alarms and to generate the Global Alarm (AG) of the protocol that was assigned to it.

b. Traffic capture in the networks to protect

- Each ADSH will carry out the capture of the traffic of the network where have it established.
- This ADSH will be located among the network to protect and the insecure network (Internet). It will capture all the traffic of the protocols to analyze that to circulate among both networks.
- Subsequently each package is analyzed using data mining techniques to find the correlation among the events and to try to find the elements that would form that possible attack.

c. Analysis of the traffic inside the ADSH

The ADSH has certain patterns of action and they will have the necessary filters for not saturate the system with false alarms or old alarms, when discover a new attack automatically will be added to the filter so that it not going to be detected again as a new threat.

1. The first traffic is filtered for the NIDS with firms (S-NIDS).Here is detected the traffic that is similar with the firms that you have itself stored in the database of firms of the ADSH.

2. Subsequently the remaining traffic is filtered utilizing the NIDS with anomaly detection (A-NIDS), to find the correlation among the events and to determine which traffic is anomalous, that is to say, on this point they will be detected the suspicious traffic that can generate vulnerabilities causing intrusions in the systems.

To carry out the networks traffic analysis where flows a large quantity of information, we will help us of the technology GRID, since this load of work will be able to be distributed toward the elements of the GRID free of work load in that moment, which will help the ADSH to process the great quantity of traffic to search new attacks.

d. Phrase and Message Generation.

When an ADSH detects anomaly traffic should generate a registration that will call phrase (Fig. 4), this phrase detailed the main characteristics of the traffic The elements that interesting of that traffic they are you defined in the following way:

A phrase is considered a fluctuation on the normal traffic.

The phrase is formed by: protocol, TSAP (transportation service access point (TCP)) and a pattern of attack (that has permitted to identify anomalies). This phrase shows the local alarm characteristics detected and its importance by means of percentage of frequency of the phrase in the

network.

- The ADSH will generate a Message (Local Alarm-AL) formed by:
  - Phrase, the previously described.
  - The phrase percentage, which is the percentage of appearance of phrase on the normal traffic in a single ADSH. Each ADSH will send the messages to a database of the Protocol Console (CP).
- A registration of the messages will be kept (AL) in each ADSH, depending on the protocol that touch it to store.

Fig. 4 Phrase and Message

e. Registration of the message in the Protocol Console

When a message to the Protocol Console arrives (ADSH):
It verifies if other ADSH have sent the same message (AL),

i. If this it registered and already we had data of the same one ADSH,
   a) Update the %phrase

ii. If we did not have data of that ADSH,
   a) is kept the% phrase and the Mark of Time in which was generated.

iii. If not this it registered the AL,
   a) Entrance for that message is created (AL).

iv. The process to recalculate the global frequency is throw

f. To get the global alarm in the Protocol Console

To get the number of ADSH that has sent Local Alarms toward the Protocol Console in the last minutes.

2. To determinate a rank of time from the last mark of time detected, to generate a Lower Rank and an Upper Rank and the elements that be found inside these ranks.

3. Recompile all the% phrase of the ADSH' s that have reported in that period.

4. Calculating global frequency of each protocol phrase analyzed according to in function of the weight of each ADSH that have it reported, that varies in function of the network characterization that protects.

5. If the percentage is greater that the threshold of phrase possibly there is a Global Alarm.

6. If we detect concentration of TSAP in Local Alarms, they will be given an Global Alarm.

7. It sent the AG detected to the Central Console.

When it has been determined that a Global Alarm exists the necessary data are generated to generate a skeleton rule that will be implemented in each corresponding Firewall.

g. Generate of the Reaction rule for the Firewall.

Once sent the skeleton rule from the Central Console of the system, each ADSH will adapt it to its firewalls. It is necessary a database of elements for each Network.

- To adapt the rule to external users with another type of Firewalls.
- Critical services of each network will be defined.
- If the rule includes a critical service will not be established automatically.

Generic Rule

The generic rule [10], will be adequate to the different types of Firewalls that we have in the network (Fig. 5).

Steps:

1. The ADSH will send to the application-fw the RG that have found.

2. The application-fw finds the devices in which the RG results, by the type of service (critical or not critical).

2a Not critical service: The rule itself to apply directly.
2b1.Critical service: The administrative is notified by means of email and sms to its mobile one.

2b2 The administrator should be connected to the application Web to accept or to deny the new rule.

2b3 If the administrator accepts it, the rule can be applied to the firewall.
3a, 3b, 3c. The system creates the specific rule for each type of firewall to be able to add it to its card index of configuration. Each one of the rules will be adapted to the different firewalls they will be in different networks (RED1, RED2, RED3, etc.).

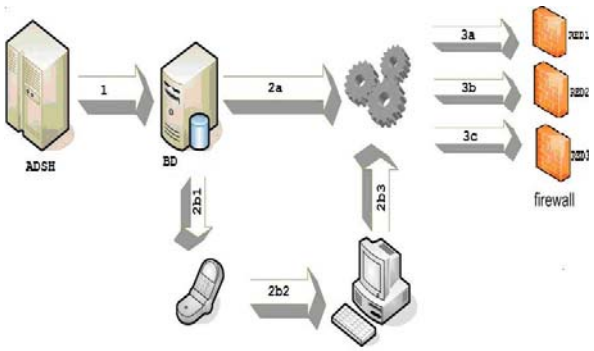


Fig. 5 Generic Rule Distribution

Insertion of critical rules

When the rule treats to a critical service for a device, the administrator receives an e-mail and a message to his mobile to notify him that he should visit the website due to that there is a pending rule that would be able to cause insecurity in the Firewall.

When the administrator enters the Web he should enter to separated part of pending Rules to insert and he will visualize the pending rules for each device in a specific format.

Insertion of not critical rules

In the Web the administrator will be able to observe the last rules applied automatically to have always controlled the changes.

5. Distributed Architecture

The architecture distributed is another of the contributions that I do and arises in response to the lack of resources in the ADSH to process traffic and/or to store the logs of anomalies generated. GIDRE requires computational process an intensive way for the discovery of the possible intrusions and attacks and besides the distribution of these results in an immediate way toward the other users, but in many cases possibly themselves he have not al reach this power of calculation required, for which with the Architecture Distributed he manages to meet resources of CPU of other ADSHs that are not utilized during a time sum during Day and/or the night, in such a way that will take advantage of the available time of other ADSH' s al maximum without invading the processes in own execution of the computer. This Architecture Distributed is implemented in our system with the following purpose:

1. Distributed the ADSH work load, toward others ADSHs available. Negotiating and to synchronize the nodes of the network, verifying its connectivity.

2. Security increment in the network when information among the elements of the GRID be transmitted, for example to react if there is denegation of services (DoS).

3. Generate a database of all the elements of the GRID, in which its characteristics be included, availability, work load, to characterize the networks, assignment of rolls and management.

4. High availability, that is to say availability 24hrs (7 days), integrity of the information, high reliability of the system, high performance.

The high Availability

The High Availability, permits that always we have active the services that provides the Central Console, in this manner without interruption the traffic that arrives from the ADSH will be analysed. Subsequently the operation is detailed:

To implement the function of High Availability in our system we will utilize a replica of the Central Console, through HEARTBEAT version 2.0, this is illustrated in the Fig. 6.

HEARTBEAT is free software distribution that permits to a service or assembly of services to be established in two servers to elevate the level of availability of the service or services, making possible that failures in one of the servers be tolerated without compromise the utilization of the service. It is installed in the master and in the slave of the system.

In the following figure the employed structure is shown.

The main objectives that intend to obtain with the establishment of the high availability in our system are:

- High Performance, in case of some failure, the recovery be in the smaller possible time affecting very little the results of the system.
- Availability 24hrs (7 days), permits the effectiveness in the premature detection of attacks to the data processing systems, having available the system in every moment.
- The high availability of the service: backup in every moment all the information that is in our system principally the service that is offering (prior detection of intrusions).

- Integrity of the information means that the data did not loss because the recovery of the services would be immediate and automatic.
- High reliability of the system.

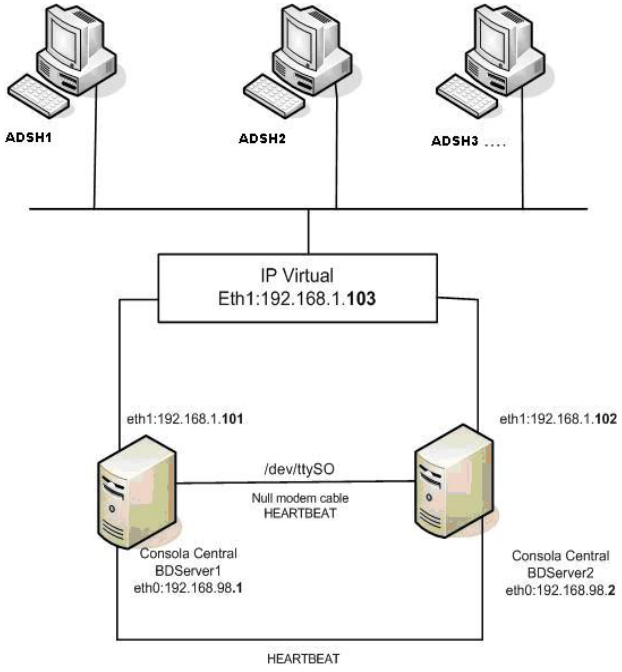


Fig. 6. High availability

The high availability operation

The high availability, permits that always we have active a Central Console, the Central Console has as main functions the next: to analyse the data that arrives from the ADSH in search of a possible intrusion, distribution of the load of work inside the GRID, etc. Subsequently the operation of the heartbeat inside the system is detailed [11].

To obtain the cluster of high availability in our system we will utilize other Server that is the backup of the Central Console, and the heartbeat, the Fig. 7, illustrates the procedure and elements that constitute the cluster of high availability.

The directions IP that are illustrated in the operation, are not the ones that really will be utilized in our system, they are used to illustrate of clearer way the high availability operation. The elements that constitute the heartbeat are:

a) Two servers BDSrv1 (databases Server 1) and BDSrv2 (database Server 2), that will be the Central Console and its backup, the master and the slave.

b) A Virtual IP direction (eth0:192.168.1.103), configured through the Heartbeat, that will be like the switch to use the BDSrv1 or the BDSrv2, this direction is transferred to slave when the master fails and the petitions to server are done through virtual IP direction.

c) The heartbeat that is found in the check the master, listening the heartbeats sent throw the MODEM wire toward the master.

d) The directions eth1:192.168.1.101 and eth1:192.168.1.102, they are used to management the two servers.

e) The directions eth0:192.168.98.1 and eth0:192.168.98.2, they are used to configure the heartbeat between the two servers.

f) The ADSH1, ADSH2, ADSH3, etc., that will be the ones that will send the information toward the Central Console and toward its backup..

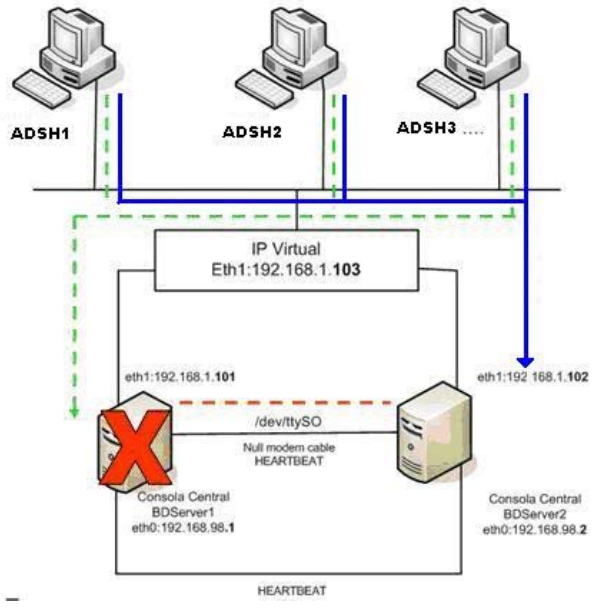


Fig. 7 Heartbeat operation

Use of the GRID in our system

The main tasks [12] that help us to resolve the GRID in our system they are:

- It Resolves certainly and intensive tasks.
- When generate a high speed data flow this need to be analysed and processed in real time.
- The needs of storage can arrive at overflow the capacity of storage of an only node, for which the data are distributed for the entire GRID.

- The data distributions allow the access to the same of distributed way.

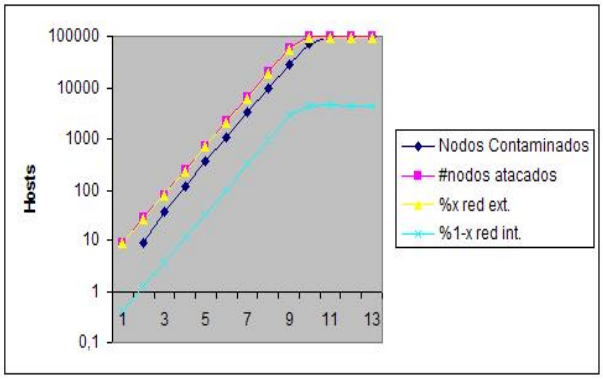
6. Results

Subsequently the next graphics show the result of the experiments. In these graphics we can see the advantage to have an ADSH Distributed Architecture against an ADSH unique.

SPAM

In these first two graphics is analysed the SPAM behaviour, which is directed to the email address book of the users that goes attacking. In both graphics (1 and 2) we analyse and we compare the process of contamination of the nodes (black line), the nodes attacked (line rose), the ADSHs network distributed (yellow line) and a single ADSH (blue line).

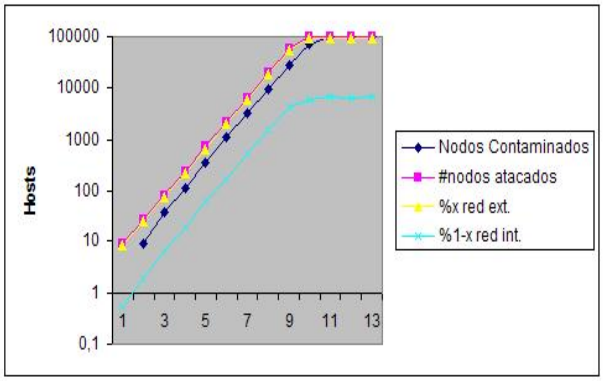
1. In this alone graphic can be attacked at most 100,000 nodes, that is the total in the proposed architecture to this test, and we compare it with a single ADSH belonging to the architecture and represents the 0.045 with regard to all the network distributed, this ADSH protects a private network that contains 9000 nodes.



Graphic 1. The Spam propagation

Total of interior Nodes 9000
Total of exterior Nodes 100,000
Interior Percentage 0.045

2. In this alone graphic can be attacked at most 100,000 nodes, that is the total in the proposed architecture to this test, and we compare it with a single ADSH belonging to the architecture and represents the 0.07 with regard to all the network distributed, this ADSH protects a private network that contains 7000 nodes.



Graphic 2. The Spam propagation

Total of interior Nodes 7000
Total of exterior Nodes 100,000
Interior Percentage 0.07

These graphics show the utilization of an ADSH distributed architecture, it let us to detect attacks or possible intrusions to the systems faster than it was done with ADSHs remote among them, this we can see in each of this graphic when we compare the external network (yellow line) and the internal network (blue line).

The percentage of internal network with regard to the external network when it decrement represents that has greater probability to detect fast the new attacks, this we can see in both graphic to compare the internal networks (blue lines). In this case the percentages are similar then the difference is seen very little.

7. Future work

The future work is defined by the following points:

- Generation and implementation of the new rules in firewalls.
- To get Local Alarms Statistics.
- Generic rule.

8. Conclusions

In this project we development a set of innovative tools for the anomaly detection in the network produced by unknown distributes attacks.

Developing a takes of decisions tool by means of the analysis of data that offers the data mining for the generation of filters that help us analizer the trafic to discover possible intrusions to the system.

The use of the technology GRID, because it permits to distribute the work load of the sensors (ADSH) to others ADSH free.

- Efficient Mechanisms for the broadcast of the new discovered attacks information inside and outside of the distributed architecture .
- Mechanisms that will permit to analyze large quantities of information to detect possible attacks and in this manner to prevent them.
- High availability that will permit in every moment to be monitoring the GRID for the detection of attacks.
- Scalability in nodes ADSH and protocols.
- Activation of different security forms appropriate for the services offered.

The points previously mentioned have given us the possibility to generate a strong system to protect and to give solution to the computer security of nowadays.

Acknowledgements

The development of this project is partially supported by the Spanish government through the Department of Education and Science in the National Plan of I + D + I (2004-2007).
To the "Instituto Politécnico Nacional" Mexico, for its support in the development of this project and finally to be grateful for the anonymous revisers for their critiques that have helped to reinforce the development of the article**.**

References

[1] Sistema de Detección de Intrusiones, Emilio José Mira, Enero 2003.

[2] Data Mining: torturando a los datos hasta que confiesen, Luis Carlos Molina. Coordinador del programa de Data Mining (UOC).

[3] Data Mining in Intrusion Detection Systems, Vishal K. Nayak., 2004.

[4] Detection of web-based attacks through Markovian Protocol Parsing, Juan M, Estevez-Tapiador, Pedro García-Teodoro, Jesús E. Diaz, 2005

[5] Stochastic Protocol Modelling for Anomaly Based Network Intrusion Detection, Juan M, Estevez-Tapiador, Pedro García-Teodoro, Jesús E. Diaz, 2003.

[6] The Grid Today. Daily news and information for the global grid community, Sun Microsystems, 2005.

[7] Grid computing, High Performance Computing, Dr. Simon See. Sun Microsystems, 2005.

[8] Análisis de la Arquitectura de Globus Toolkit 4.0, José Luis Vázquez, Noviembre 2004.

[9] Draft. Everything you wanted to know about Globus but were afraid to ask. Describing Globus Toolkit Ver 4.0. Foster, Agosto 2005.

[10] Implementación de regla genérica para cortafuegos (Firewalls) Proyecto Fin de carrera, Elena Galván, Manel Médina, Facultad de Informática de Barcelona, Universidad Politécnica de Cataluña, Barcelona España, 2006.

[11] Entorno de detección y repuesta de Intrusiones basado en GRID, Olimpia Olguín, Manel Médina, XVII Jornadas de Paralelismo, septiembre 2006, Albacete España.

[12] GIDRE: Entorno de detección y respuesta de intrusiones basado en GRID (avance), Olimpia Olguín, Manel Médina, IGC 2006, Barcelona España.

Manel Medina, Dr. and Professor of Computers and Internet Security in the "Universidad Politécnica de Cataluña (UPC)", Barcelona Spain. Head of esCERT-UPC: Spanish Computer Emergency Response Team. Technical manager of DEDICA project (Telematic Enginer) Distributed EDI Certification Authority. Member of ICE-TEL project (Telematic Education). Infrastructure for Certification Authority in Europe. Member of PITA (Public-key Infrastructure with Time-Stamping Authority) project, belonging to the Infosec/ETS (European Trusted Services) program.

Olimpia lguín received the Engineering in Computer Science degree by "Instituto Politécnico Nacional", Mexico, in 1998. Homologation of her degree to Engineering Computer Science by Spain. Specialization in Computer Sciences by "Centro de Investigaciones en Computación", Mexico, in 1999. Master degree in technology and security of the information by "esCERT- UPC, Barcelona Spain, in 2004. PhD Student by "Universidad Politécnica de Cataluña", Barcelona Spain. Her research interest includes Computers and Internet security, GRID Computing and their application.