

A Diversified Dynamic Redundancy Method Exploiting the Intrusion Tolerance

Huang Zunguo, Lu Xicheng, Wang Huaimin
National laboratory of parallel and distribute processing
Changsha, Hunan, P.R.China, 410073

Abstract: Redundancy is a well-known effective method for fault tolerance designing in the computer world; however, this RAS oriented fault tolerance method cannot solve the intrusion tolerance problem in two ways. Firstly, the identical systems may have the same type of vulnerabilities, so they cannot withstand the same type of intrusion. The second one is that incident with little probability will be bound to happen due to the hacker's intentional arrangement. The Diversified Dynamic Redundancy (DDR) Method can solve such problem because it featured diversified architectures, diversified function, diversified management and diversified implementation.

Keywords: Diversified Dynamic Redundancy (DDR), Intrusion tolerance, Unbounded environment, Computer network security, Drifting of the service.

1) Introduction

The network security issue is becoming more and more concerned. For a people who wanted to dive into the network economic sea, two questions may dawn on his mind. The first one is that shall I have to face on such an open environment like the Internet? The second one is that how can my systems survive in such a hackers ridden cyber world?

The answer to the first question is quite sure. Every one will be bound to face to the open environment during the network economy going on. The answer to the second one is just the question of how a system can perform its mission while being attacked. This is just the survivability issue, including detection of intrusion, assess of damage, recovery from disaster and adaptation or revolution. Intrusion tolerance is an important aspect of the survivability researches.

Redundancy is a well-known effective method for fault tolerance designing in the computer world; however, this RAS oriented fault tolerance method cannot solve the intrusion tolerance problem in two ways. Firstly, the identical systems may have the same type of vulnerabilities, so they cannot withstand the same type of intrusion. The second one is that incident with little probability will be bound to happen due to the hacker's intentional arrangement. The Diversified Dynamic Redundancy (DDR) Method can solve such problem because it featured diversified architectures, diversified function, diversified management and diversified implementation.

2) Intrusion and its counter measure

A hacker may intrude a system through the following steps:

A. Probe. Probe is just like a thief taking the lock of the door and trying to find the way to open it. The ordinary method is scanning for system fault in the network.

B. Exploration. The hacker has intruded into system exploring the system resource.

C. Exploitation, The hacker finds something useful and begins to make use of them to realize his purpose of his attack. Examples of this include get the confidential information, plant a daemon for further usage and even destroy the whole system.

So, the counter measure against intrusion may also be focused at the following points:

A. Resistance. It uses the necessary tools of encryption and authentication to prevent the system from being accessed by hackers. This is just the topic of the security research and it is suitable against probe and exploration. However, it is very difficult to be fully implemented due to the following reasons: firstly, the system is faced to the open environment like the Internet and the hacker's attack techniques are in the way of development; secondly, the number of intruders are deeply increased while the basic knowledge required for a hacker to intrude the Internet is vastly decreased. This means any ordinary people may be succeeded in doing network attacks.

B. Detection and evaluation. Detection is the process of identifying the malicious activity targeted at computing and networking resources. The IDS research is a very common direction in recent security research and many products appeared in this respect. Evaluation is just an assessment of the degree of damage caused by the hackers. This is just the preparation for the site to response.

C. Recovery and drifting. These are two method often used for responding to disasters. Recovery is for those whose damage degree is relative small. Ordinary way for that is just recall from the backup messages. Drifting is another way for those whose damage is very deep and cannot be restored instantly. So the best way to do is drifting the current service to another one that was standing by, leaving the working site being recovered for further use.

D. Evolution and adaptation. This is the further measure to respond to the disaster. Actions include adding the attack mode to the IDS library; patch the hole that caused the attack to be succeeded, and enhance the security policy that was challenged and so on and so forth.

It is just another version of the PDR strategy, that is, Protect, Detection and Response.

3) The DDR skeleton

We propose the DDR skeleton based on our experience of many years research on the computer network security. The system is composed of four models: ID is the first block of it. In this system it is responsible for finding the intruders and report the attack to the survivability system. The assess model is for identify the degree of the damage. The system use it to determine what path will go for the next step. Drifting is for the high degree of damage for which the system cannot be restored in time, and just drift the current service to the backup site leaving the working site being repaired carefully. Recover is for the low degree of damage and the system can be restored instantly. After that, the adaptation model is for adding functions to avoid further damage while under the same type of attack modes. Among the models the intrusion detection system (IDS), directory based access and distributed storage (DADS) and drifting of service (DSV) models are playing the key action.

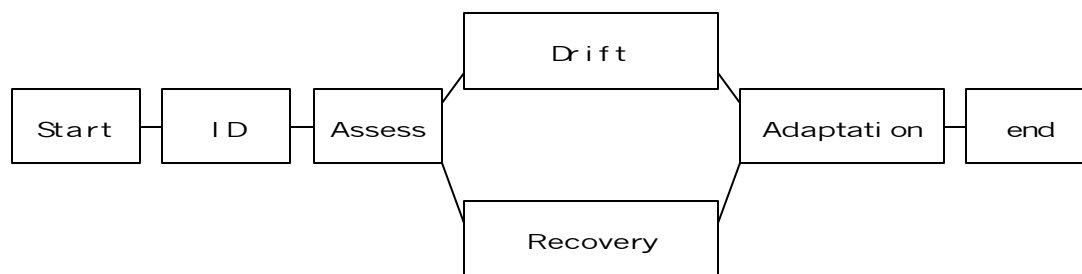


Fig. 1. The DDR skeleton

A. IDS: The eyes of DDR

The IDS based on network function through catching the packets passing through the specific node, and try to find whether there are attack modes in them. The advantages of it are fast of detection, hardly of being attacked, and widely of sight. Strategy and architecture play important part in the IDS systems. The main point of research in this area is how to develop a distributed IDS and try to improve the performance of operation and precision of intrusion identification. So our recent works include the IDS architecture based on agent technique, The ID technology and the strategy implementation. The final purpose is to make the cute eyes of our DDR system.

The simplest measures of response include on time warning and log recording. Further measures are detailed in the next step.

B. Directory based access and distributed storage (DADS): the feet of DDR

Directory, which is featured a set of object arranged on a specific rule, is widely used in the current computer software products. We can consider it as a special database storing the attribute of many objects. These attributes can be accessed by the supervise objects.

The DDR system makes use of it to build a jungle structured distributed backup system. That is, at the leaves of every tree, functions are classified into basic service that are supposed to be destroy free, and other service which can be restored on time by the basic functions while being destroyed. At the root of every tree, the backup of basic service of its children is stored as the other service information. And it in turn has its own basic functions for restoring the service of itself. In case the basic service of its children is destroyed, the root can restore them through the network. Why use the jungle? This is just a higher layer of redundancy incase the basic service of the root being destroyed; the roots next to the victim in the jungle can help it to restore the service timely.

C. Drifting of service (DSV): The key point of DDR

Drifting is the uttermost measure that a system has to be made while being heavily destroyed. There are two ways to do this.

The switch mechanism How can a destroyed site be switched to its mirror site in a smooth way? And can the newly assigned site stand out the same attack mode the victim site has just suffered? These are the common problems the DSV model has to solve.

We develop our system with a two-layer hierarchy. In the first layer, we use the cluster structure which the mirror sites have a root as their supervisor. Only the IP address of the root can be seen from the user. The root performs the switch between the mirror sites. In the second layer, the neighborhood supervisors can be drifted to each other use the IP switch technique.

The implementation issue. To avoid suffering the same type of attack mode, the efficient way to do is making the most of systems of different type as the mirror sites besides the adaptation measures being taken. So we emphasize diversified architectures, diversified function, diversified management and diversified implementation.

4) Conclusion

Incident response and disaster recovery is an important aspect challenging the current networked cyber world. Requirements for this are very large in the IT market. Our research for that is just a start point. We propose it just for calling the attention for the coming days, and we will try our best to do it in the future.

5) References

1. Ellison, B. etc, "Survivable Network Systems: An Emerging Discipline", <http://www.sei.cmu.edu/97tr013abstract.html>, 1999.
2. R. C. Linger, etc, "Requirements Definition For Survivable Network Systems", <http://www.sei.cmu.edu/97icre.pdf>, 1999
3. Anotai Srikitja, etc, "On Providing Survivable QoS Services in the Next Generation Internet", supported in part by NSF grant NCR 9506652 and DARPA under agreement No. F30602-97-1-0257
4. Robert. J. Ellison, etc, "Survivability: Protecting Your Critical System " <http://www.sei.cmu.edu/organization/programs/nss/protect-critical-systems.html>, 7, Feb, 00