A Swarm-Intelligence-Based Intrusion Detection Technique

Zhou Lianying[†,††] *and Liu Fengyu*[††]

[†]*School of Computer Science and Technology, NUST, Nanjing, 210000, China*
[††] *School of Computer Science and Telecommunication Engineering, JU, Zhenjiang, 212013, China*

Summary
A Swarm-intelligence-based intrusion detection technique is proposed to in order to reduce the misjudgment & misdetection and increase the real-time response in the existing intrusion detection techniques show. Separating a huge and complicated intrusion detection system into severer independent detection units with unique function so that the amount of detection data processing and the complexity of detection signature selecting, which are the main factors affecting the application performance of existing intrusion detection techniques, are reduced significantly. Moreover, by utilizing the information from each independent detection unit, the complicated intrusion of the entire intrusion detection system can be detected. The key techniques for the implementation of the proposed system include the user trace under the environment of network, the interception and detection of real-time system calls, and the efficient access of shared information base. The according solutions are given in the article.

Keywords:
Intrusion Detection, Swarm Intelligence, network security

1. Introduction

In the recent years, as the second line of security defense after firewall, the intrusion detection technique has gotten rapidly development. It plays very an important role in attack detection, security check and network inspect. But with the continuous popularization of network application, the rapid broadening of network bandwidth and the rapid improvement, the problems of misjudgment, misdetection and lack of real-time response to attack that are inherent for the intrusion detection technique are becoming more and more thrown out, which have badly affected the practical value of intrusion detection product. We may analyze its root cause by the data resource of intrusion detection technique. There are two main data resource for the intrusion detection technique: network data packs for the network-based IDS (intrusion detection system) and system audit logs for the host-based IDS. The increasing speed of the former data traffic is greater than the one of processing capacity of IDS; the latter isn't designed specially for IDS and its recorded characteristic variables can't usually meet the need of IDS, more or less, and usually need complex processing algorithm for data mining. So Enormous processing data and complicated signature selecting are the main problems that make the intrusion detection technique get into difficulties and directly affect the performance and real-time characteristic of intrusion detection.

The biology immunity mechanism has brought much reference to network security. For instance, IDS based on the artificial immunity[10]. In fact, we may also draw lessons from biology "swarm intelligence" characteristic. It is found that gregarious insect like ant, bee, etc., as far as an individual is concerned, the intelligence is low and the action isn't inspected, but the colony can solve very complicated problem and show very high "swarm intelligence". For example, the ant can quickly find the shortest route approach to food resource from lots of possible routes. The research indicates that gregarious insect possesses "swarm intelligence" because they have the following characteristics[1,2]: (1) flexibility——the colony can adapt to varying circumstance; (2) stability——even though the individual failed, the whole colony can still accomplish task; and (3) self-organization——the activities needn't be controlled by a center or inspected by a local, which may be called independence. Moreover, among the three characteristics, the former two characteristics come from the third characteristic——just through the simple self-organizing and all individuals' mutual interaction, the complicated and high intelligent colony behavior is formed. And further analysis shows that the key to gregarious insect's possessing "swarm intelligence" is: on one hand, every individual all constantly contributes to the colony by leaving useful information (referred to pheromone); on the other hand, each individual's function realization is based on the utilization of other individuals' leaved information---this forms the colony predominance.
The thought of biological "swarm intelligence" has gotten more extensive application in the network technologies at

Manuscript received July 5, 2006.
Manuscript revised July 30 , 2006.

present[2,3,4,5], for example Liu Zhenyu from University of Birmingham proposed a network routing algorithm based on "swarm intelligence" [3]; Paul, Norwegian University of Science and Technology Norway, proposed a plan for the self-management of virtual paths in dynamic Networks[4]. This paper also tries to introduce the thought of "swarm intelligence" into the intrusion detection techniques. The concrete realization thought is separating a huge and complicated intrusion detection system into severer independent detection units with unique function so that the amount of detection data processing and the complexity of detection signature selecting are reduced significantly. The remainder of the paper is organized as follows. Section 2 discusses an IDS model based on "swarm intelligence". Section 3 presents the concreted realization of the model's "swarm intelligence" mechanism. We provide the solutions of the model's key techniques in Section 4. And conclude in Section 5.

2. Swarm-intelligence-based IDS model

From biology's "swarm intelligence" characteristic, we may obtain such inspirations as the followings: (1) In order to decentralize burden, the entity intrusion detection system should be separated into numbers of intrusion units that are independent, flexible and self-adaptive; (2) In order to improve real-time characteristic of detection, each detection unit should be lightweight—adopting simple algorithms and processing less data; (3) The most important thing is that a detection unit can't work alone, it should not only make the best of information but also leave information to others, which means IDS should also gather "swarm intelligence". Therefore, the swarm-intelligence-based IDS in this paper is proposed based on the following policies:

（1） Simplifying system organization structure and hierarchy to improve the efficiency of the whole IDS system;

（2） Constructing the IDS with severer detection units being independent and unitary in function to improve synchronously the efficiency and performance;

（3） Separating the data traffic according to the function of each unit to reduce the processing data;

（4） Enhancing the information exchange among units to detect complicated attacks.

The models of swarm-intelligence-based IDS are shown in Fig.1, Fig.2 and Fig.3[8,9]. The Fig.1 is the network-based model; Fig.2 is the host-based model. Both the two models are both based on the separating of detection data[6], the independence and uniqueness of detection unit in function and the information exchanging and sharing among detection units (as illustrated in Fig.3). The difference between them lies in the data source and concrete detection function. Because the network-based attacks are mainly against different network services and the attack aims and methods are often different for different web services, for example, the SQL and ASP attacks are against Web service while the replaying attack is against Email service. So we may design detection units according to network services and separate data traffic based on each server's IP address. Similarly, the host-based attacks may commonly come down to illegal access and modification to system key files such as user password file, system configuration file and system audit & log file. in the same way, we may design detection units according to system key files and separate data traffic based on correspond system call.

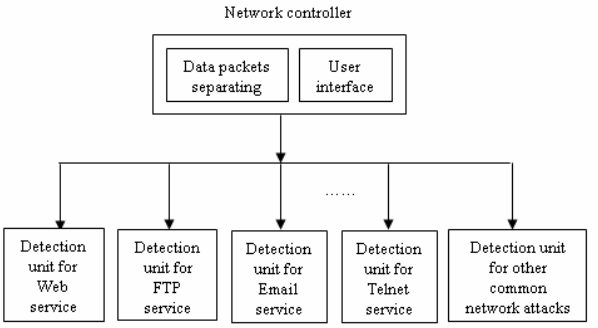

Fig.1. A network-based IDS model

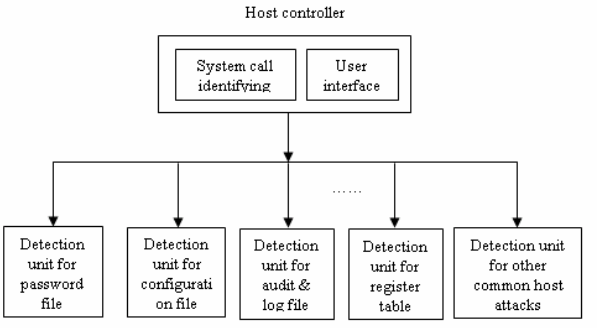

Fig.2. A host-based IDS model

Fig.3 shows the implementation framework of a detection unit in the two aforementioned models[7]. Both the network-based and host-based detection units have the common construction, but with each ingredient's data resource and processing logic. The signature selecting model is to filtrate data source and extract variables according to detection aims, including format conversion. Due to the oneness of each detection's function, the signature selecting is definite and the corresponding data

processing algorithm may be quite simple. The abnormal event-processing model takes charge to response as having detected abnormal network behaviors and system operations. Likewise. Due to the uniqueness of each detection's function, the response measures are also clear and may be designed in advance and needn't to ask the central controller. So independence and low interaction with above model may apparently improve the system's real-time characteristic and minimize the influence of attacks (the user interface of central controller is mainly responsible for the configuration and management of each detection unit).

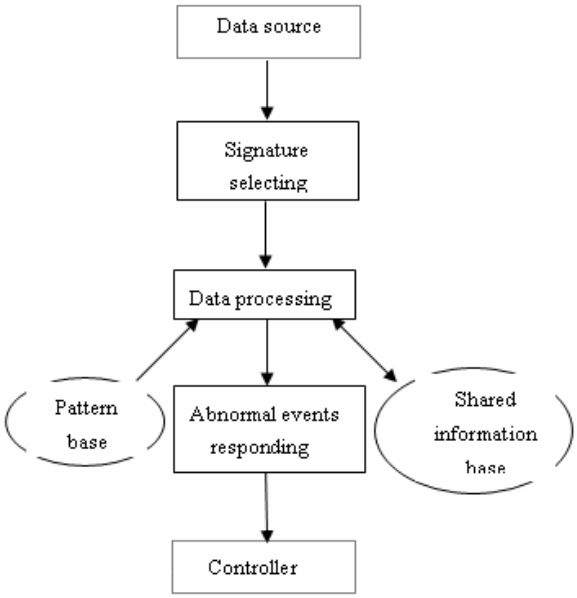

Fig. 3. The construction of detection unit

3 "Swarm intelligence" mechanism of model

As was previously stated, the "swarm intelligence" is realized by gathering each detection unit's information to the entire detection system and utilizing information from the entire detection system. Assuming that a detection unit Ai is responsible for supervising the part of network system resource Ri, the major steps of detection based on " swarm intelligence" can be described as follows[5]:

（1） To adopt certain method, such as rule match, to analyze the access data acquired at the moment t_{ik} depending on IP address, protocol, operation, and etc., and explain the suspicion degree $v_i(t_{ik})$ of analysis result;

（2） If $v_i(t_{ik})$ is greater than vilimit (the suspicion degree threshold), this access is judged as anintrusion behavior, and operations such as alerting, responding and recording should be done;

（3） If $v_i(t_{ik})$ is smaller than v_{ilimit}, the detection unit accesses the shared information base and sums up v_i ($v_i = v_i + v_i(t_{ik})$) based on access characteristic variable as IP address; I the current vi is greater than v_{ilimit}, the access is still judged as an intrusion behavior.

It is obvious that steps 2and 3 realize the information offer and utilization of each detection unit. The above process can be illustrated by two examples. One is for the host-based detection: it is assumed that a unacquainted user is found to access a key file in a legal user identity, then the corresponding file detection unit estimates this access and explain its suspicion degree. If the suspicion degree doesn't exceed the threshold (for example, the user isn't within the malice user lists), then it is added to the shared information base; and if the user is found to access another key file, then the suspicion degree is added continuously; and if the user further performs a suspicious system operation and the suspicion degree has exceeded the threshold, the user will be marked malice user and corresponding responses will be performed. The other is for the network-based detection: it is assumed that a scanning behavior's anomaly degree is 3 and the alert threshold is 9 in a network detection system. Obviously, when a detection unit detects a scanning behavior, it will not alert at once, but update the shared information base. If the unit "finds" the sum of anomaly degree of the scanning behavior has reached 9, it will send an alert message to the controller and trigger the responder in the meanwhile.

4 The realization of key techniques for model

4.1 The user trace under the environment of network

The attack method used by the current hackers, by using different IP addresses and different user identities against different aims and in different periods is frequently carried out. Due to dispersed sources and multiple identities, it is hard to perceive and detect such attacks. Thus, to prevent them, IDS must solve the problem of user trace under the environment of network, which is also the precondition of intelligent cooperation among detection units. The solution presented in this paper is to assigned unique network ID (NID, mainly based on its username) or a unique host ID (HID, mainly based on its IP address) to each user when the user first enters a network or a host. In this way, no matter how this user login in different hosts of the same network the same host, IDS will all assign the same NID and HID to the sequent user instances.

Therefore, using the assigned NID and HID as the signature identification, the IDS may implement cooperative intrusion detection among detection units.

4.2 Treatment of system call interception

The detection efficiency and performance of the host-based detection units depending on real-time system calls may be improved apparently in comparison to depending on redundant and hysteretic system audit logs. The Linux system is the current platform for network services and it is divided into the user space and the kernel-level. The system call interception can only be performed at the kernel-level, while the corresponding detection may be performed either at the user-space or the kernel-level. The user space implementation is often more portable but may suffer more performance impact. On the other hand, the implementation completely at the kernel-level is likely to be fast but less portable and may causes a significant increase in the complexity of the operating system. The proposed technique chooses a hybrid approach --the kernel-level part supports a fast path for system calls that should always be allowed or denied and the user space part provides a further detection for system calls.

4.3 Synchronization of network sharing information database

Different from the host-based detection units, the network-based detection units offen access the shared information base that isn't in the local host high frequently and it will affect the detection efficiency. An improved method is to use the distributed database model and synchronization technique of Internet OSPF（Open Shortest Path First）protocol for reference. In detail, we may set a shared information base in each detection host. As for the synchronization of share information database among different hosts, it can be realized through the periodical or uncertain information exchanging between the adjacent hosts. The uncertain information exchanging can be launched actively by the needer (only exchanging the needed information records), or by the changer (only exchanging the changed information records); the periodical information exchanging, then, can guarantee the entire synchronism of the shared information databases (the period of exchanging can be given a longer time).

5. Conclusion

Cutting misjudgment & misdetection rate and improving real-time characteristic are the main objects to solve for the current intrusion detection technique to produce practical value. The swarm-intelligence-based intrusion detection system model proposed in this paper better solves the problems by means of decomposing of detection functions, corresponding separation of data traffic and mutual information exchanging and sharing among detection units. In fact, confront to the more and more serious problem of network security, the distribution and cooperation may be utterly adoptable solution. Its essence is just "swarm intelligence", which is also consistent with the current hot technology——distribute computation &active network.

References

[1] Eric Bonabeau, Marco Dorigo. Swarm Intelligence: From Natural to Artificial Systems www.cs.virginia.edu/~evans/bio/slides/presentation.pdf. 2003.

[2] Tony White. Swarm Intelligence: A Gentle Introduction with applications, www.sce.carleton.ca/researchers/tony/index.html.1997.

[3] Liu Zhenyu, Kwiatkowska, Marta Z. A swarm intelligence routing algorithm for manets, Proceedings of the Third IASTED International Conference on Communications, Internet, and Information Technology, pp.484, 2004.

[4] Poul E. Heegaard, Otto Wittner, Bjarne E. Helvik. Self-Management of Virtual Paths in Dynamic Networks, Lecture Notes in Computer Science, Springer-Verlag GmbH, pp.417, Volume 3460 , 2005.

[5] Bianchi, R.A.C. Costa, A.H.R. a swarm intelligence approach to learn task coordination, Proceedings of the 16th Brazilian Symposium on Artificial Intelligence, SBIA 2002,Advances in Artificial Intelligence.2002, pp.195.

[6] Lam Kwok-Yan, Hui Lucas, Chung Siu-Leung. Data reduction method for intrusion detection. Journal of Systems and Software, Vo.33, No.1, pp.101-108, Apr. 1996.

[7] Zhang Yong, Zhang Deyun, Li Shenglei. The research and implementation of network intrusion detection system based on cooperative distributed agent,

Chinese journal of computers, Vo.l. 24 No.7, pp.1-6, July, 2001.
[8] Dale, J. A mobile agent architecture for distributed information management [Ph.D. Thesis]. pp.65-98. 1997.
[9] Staniford-Chen S, Cheung S. IDS: a graph based intrusion detection system for large networks. Proceedings of the 19th National Information System's Security Conference, Vo.l1. National Institute of Standards and Technology, pp.361-370,1996.
[10] A.Hofmeyr. Security. Steven. An Immunological Model of Distributed Detection and its Application to Network, Ph.D. thesis. University of New Mexico, May, 1999.

Zhou lianying is an Associate Professor in the School of Computer Science and Telecommunication Engineering, Jiangsu University, China. Zhou received her M.D. from Jiangsu University in 1997.Now, She is a graduate student for doctor's degree at the Najing University of Science & Technology, China. Her research interests include network security, intrusion detection, real-time systems, and distributed systems.