슈퍼컴퓨터 보안 이슈 및 대책

홍성혁*
백석대학교 정보통신학부

Supercomputer's Security Issues and Defense: Survey

Sunghyuck Hong*
Baekseok University, Division of Information and Communication

요 약 슈퍼 컴퓨터는 20G 프리플롭을 처리 할 수 있는 용량을 가진 컴퓨터를 말하며, 과거에는 슈퍼 컴퓨터로 복잡한 과학 계산을 처리하였으며, 지금도 많은 클라이언트 컴퓨터가 복잡한 계산 처리를 요청하면 빠른 처리 속도로 클라이언트의 요청을 처리하고 있다. 슈퍼 컴퓨터가 바이러스에 감염될 경우 연결된 많은 클라이언트 컴퓨터에 영향을 미칠 수 있기 때문에 최근 사이버 공격은 슈퍼 컴퓨터에 초점을 맞추고 있고, 따라서, 본 연구 논문은 슈퍼 컴퓨터 보안 문제를 분석하고 슈퍼 컴퓨터의 보안 레벨을 올리기 위해 현재 문제점과 생체정보를 이용한 방어책을 제시하였다.

주제어 : 슈퍼 컴퓨터 보안, 네트워크 보안, 분산처리 보안, 침입탐지, 침입방지

Abstract The super computer calls usually as the super computer in case the computing power of the computer is 20 G flops (GFLOPS) or greater. In the past, the computer equipped with the vector processor (the instrument processing the order having the logic operation and maximum value or minimum value besides the common computer instruction) processing the scientific calculation with the super high speed was installed as the super computer. Recently, cyber attack focuses on supercomputer because if it is being infected, then it will affect hundreds of client PC. Therefore, our research paper analyzed super computer security issues and biometric countermeasure to develop the level of security on super computer.

Key Words : Super computer security, Network Security, Distributed Security, IPS, IDS

1. Introduction

The information analyzed through this annual production supports the optimum decision-making for the policy decision of nation or natural disaster and crisis management like the disaster [3]. The various information which is observed like not only information about the weather which the general publics know just but also marine, creature, public heath, and etc. The total global system is utilized and the information is produced. It is used for not only environmental field having an effect on the personal life and property protection and people's health and welfare including the weather information from the natural and artificial disaster the information in which the super computer is produced with all sorts of energy resource managements, administration, protection of the

Received 1 April 2013, Revised 20 April 2013
Accepted 20 April 2013
Email: shong@bu.ac.kr
ISSN: 1738-1916

ecosystem of the earth including management of water source, and etc. Through the understanding about the active reaction about the climate change and hydrological cycle are various.

Presently, this super computer is introduced to Korea. Meteorological Administration and the numerical weather forecast model is performed in Chung-buk weather super computer center, and the operation speed corresponds to 55 the upper parts with the capability calculating the amount which 600 million people will calculate with 758 Flops for 1 year in 1 second among the global super computer on June, 2012.

If we assume that security vulnerability of this super computer is generated, the optimum decision-making is not supported to the natural disaster as well as the policy decision of nation and crisis management like the disaster [1]. The exposure of the personal information of the people including the people's health and welfare, at the same time, the damage including the human life, property, and etc. is possible to be nationally serious because the energy resource management is not smooth. Therefore, we need to do research on the security problem of the super computer.

2. Problem

The super computer, it has the network structure as the general computer. The network structure receives the service request of the client and the server does by the client and server and mutual interlocking service between DBs to perform this in being the server. As to the server, the power management and safety have to be efficient because of is being stormlessly used for the long time. The client refers to the single workstation which requests the service to the server and receives the service from it. The user can control the various functions through this and moreover we can perform. Building the server. The client server system is one among the thing changed to the fast speed like the network. In some way, the exaggeration is not even if the computer whole field is remarkable developed. The client/server computing can be said to be the environment which it makes so that the several connected to the network computers can, can work together. In addition, in this way, if it disperses well and the connected several computers are arranged, it can have an effect on the work effectiveness.

The attack, in which the super computer, having this network structure moreover, the network security vulnerability problem is generated and which uses the Dos attack or Ping remarkably smurf attack (Smurf Attack), Fraggle attack, SYN Flooding attack, distribution service attack (DDos Attack), and attack of the Tribe Flood Network (TFN) etc. can be made. In addition, in order to order that this attack is made, the scanning including the port scanning (Fort Scanning), TCP connect scanning, TCP SYN scan, Stealth scan, IP fragmentation scanning, TCP opposite IDENT protocol scanning, FTP bounce attack scanning, UDP ICMP port reach impossibility scanning, DNS HINFO record, The Bogus Flag Probe, and etc are necessary.

Therefore, the encryption algorithm, crack, electronic signature, certificate and certificate authority, fire wall, and various countermeasures of the intrusion detection system (IDS) etc. showed in order to cope with the network security vulnerability problem.

3. The Objective of Research

Because of being used as the core social overhead capital leading the crisis management and industrial technology innovation and knowledge-based society, the complex problem that solution is difficult is still in existence due to the super computer of the existence highest performance in the science and field of the commitment and the situation which can be insufficient comes with the existing exclusive super computing system. Therefore, the best super computing resource is provided to the domestic researches due to the

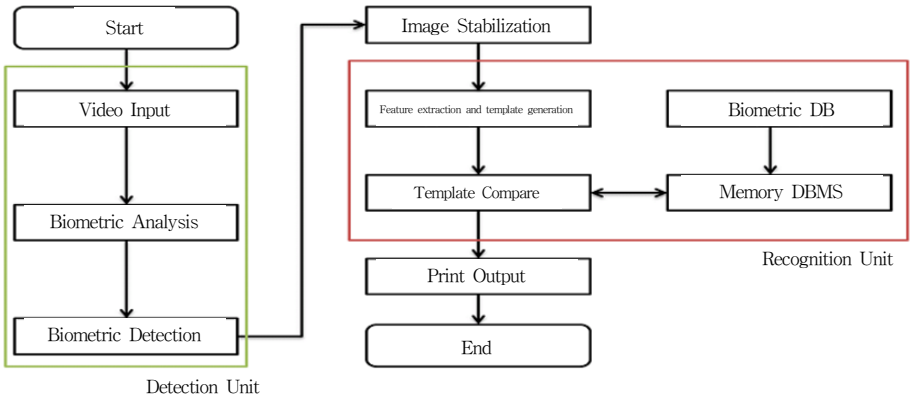
establishment of a strategy which the super computing resource 2,012 supplies with the standard over 1 PFlops level with the domestic researches which that promoted the country super computing public use on the effort for enhancing the efficiency of the extra-large super computing resource for science and technology innovation lead and it did the blotting paper security (the entry world the 10th range) of national science and technology strong power entry with the super computer 4 expiration construction of the world-class more than 250 TFlops class but the utilization maximization is the insufficient actual condition with the exclusive self application. Against this, all countries of the world intensifies the cutting edge super computing foundation of the infrastructure the reciprocity connecting the awareness, super computing and cutting edge science technology equipment, leading edge application soft ware, and etc. the super computing infrastructure to the essential element of strategy of science and technology development and securing of national competitive edge through the high-speed research network. And U.S. operates the super computer scattered through the share cyber infrastructure (Shared Cyber infrastructure) program with and it builds U.S. with T grid (TeraGrid),that is one extra-large super computing system,. It provides the user convenience is consistent environment including the user service and applied web portal, which and etc. to the scientific technicians.

Our country grasps the advanced trend of technology about the super computer and cluster, performance estimation, international change of strategy, and etc. for the solution which can manage the PFlops class super computer and which it can monitor technology acquisition and successful ultra high performance super computing system construction. Research and development of the super computer operational technique reflecting positively this are needed.

Therefore, it will be a research field of the user authentication through the network super computing and biometrics′ in this middle as the certification field about the, that is the field of brash, field of networking and user and the user convenience technology development which can approach to the super computing infrastructure in which the user is unified into the user authentication through the network construction and biometrics used exclusively between the super computer which each engine holds in order to use the a little more efficient network super computing with the high band research network and which it can utilize is done with the object.

4. Contents of Research

The safe network is built and the development direction which is various with the research implementation system construction about the numerical weather forecast and field of the super computer is the safety assurance about the national computer network, connected with the prevention capability security about the various information production line is quick construction and which is safe and cyber threatening which is serious due to the information protection system construction and personal information exposure and super computer and not only information system but also Korea Meteorological Administration supercomputer because of the hacking information system property protection and risk management coping ability improvement, and super computer public use system (the super computer network) improved as the destroyer and information protection system construction operate with the user automatic isolation and patch management system, which is contrary to the construction, web site attack and preventing forgery and alteration, protecting personal information and containment, monitoring of the web fire wall operational state and register, and security policy with the duplexing vaccine program, and prevention of information leaking system and all networks and prevent Defense Security Command



[Fig. 1] Proposed Biometric System

high-danger at the prior [2]. In addition, in the central, the system has to be comprised so that all controls and administration can be possible. And systematically the control procedure is established. By using the biometrics Signature base filter, approved it distinguishes. The quick filter automatic upgrade function is provided in the new weakness and offense pattern detection and VPN comprises over the IPSec or SSL VPN and supports the firewall function built in and various algorithms for the super computer public use. Figure 1 shows the proposed biometric system on supercomputer system.

5. The Problem and Improvement Plan

The DoS (Denial Of Service) is exactly the service denial attack. The attack which doesn't provide the service in which the system is normal is altogether included and it can be said to be the Dos attack. As to the attack of kind of this, the attack of the form doing the illegal action (whether the root authority is obtained or the password file is picked out, the connection, that is the illegal connection, is made. The back door is planted.) in the server is not. As to the DoS attack, the numerous attack methods exist and moreover the defence is difficult. Furthermore, the trace is difficult whether it attacked where. And or not the program attacking the Dos attack at Internet easily can be found and the directions is simple. For example, there exists many method of the etc. in which the DoS attack in the local consumes the hard disk space all.

```
#include<stdio.h>

void main()
{
    while(1)
    fork();
}
```

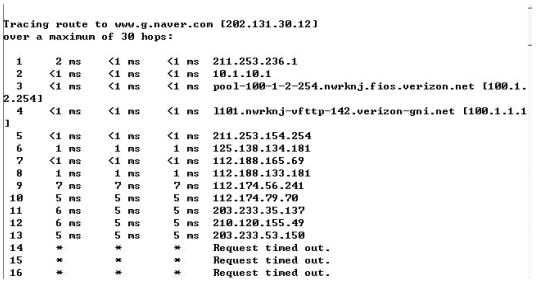
```
#include<stdio.h>

void main()
{
    char c;
    while(1);
    c = malloc(1000);
}
```

[Fig. 2] Sample of Source Preying Code

Figure 2 is the source preying on all memories of system, and figure 3 is the source in which the unlimited, that makes the process and which passes the script which it makes to cannot make any more process round. The attack is possible with the simple source of this several line.

The attack using Ping is the order which sends the request for echo (Echo Request) to the other host and gets the echo reply (Echo Reply).Therefore, the packet of the quite small size is loaded and sent. In other words, one datagram can be sent and in order to see the other host state here the maximum size of data which can be actually included in one datagram is generated the problem in case of Ping by 65,507 bytes. The most of operating systems was not due to compare more than 65,507 bytes case and be the maximum data size included in the Ping datagram designed [3]. Because since being data size which cannot be

transmitted to one datagram if it sends more than 65,507 bytes data by using the window 95 of Ping, there is no problem in the place where it splits in 2 and it transmits this (IP fragmentation) and it sends but the paid side assembles IP combination and to unite again the datagram divided into 2 there is no comparison in the UNIX series system about more than 65,507 bytes datagram, while uniting this, the overflow occurs and the system goes down.



```
Tracing route to www.g.naver.com [202.131.30.12]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  211.253.236.1
  2    <1 ms    <1 ms    <1 ms  10.1.10.1
  3    <1 ms    <1 ms    <1 ms  pool-100-1-2-254.nwrknj.fios.verizon.net [100.1.
2.254]
  4    <1 ms    <1 ms    <1 ms  1101.nwrknj-vfttp-142.verizon-gni.net [100.1.1.1
]
  5    <1 ms    <1 ms    <1 ms  211.253.154.254
  6     1 ms     1 ms     1 ms  125.138.134.181
  7    <1 ms    <1 ms    <1 ms  112.188.165.69
  8     1 ms     1 ms     1 ms  112.188.133.181
  9     7 ms     7 ms     7 ms  112.174.56.241
 10     5 ms     5 ms     5 ms  112.174.79.70
 11     6 ms     5 ms     5 ms  203.233.35.137
 12     6 ms     5 ms     5 ms  210.120.155.49
 13     5 ms     5 ms     5 ms  203.233.53.150
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
```

[Fig. 3] Traceroute Command Practice

The Smurf attack refers to the attack which all hosts in the network which receives the moment attack the hacker sends ICMP echo request packet much, and it deceives the source address send the echo response packet to the request for echo for the departure of this packet, it reaches through like that many routers in order to reach from the office rum departure to the destination. If the router receives that packet, it analyzes the packet and determines and whether its own inside network is the destination or not if it is its own inside network, and it accepts this packet and if not, then it sends the other router. However, while it is going to the destination, the network dies due to any kind of problem or in case of having the routing table which is caused by for a certain reason and in which the router becomes wrong this packet is unable to be gone to the destination in perfect. That case, finally, because the router receiving the packet has the source information of the packet, the host who sends the request for echo (Echo Request) which is ICMP 8 number type with the departure of this packet and receives 2 packets sends the echo reply (Echo Reply),that is the type No. 0, to the host sending this packet again. It is the attack by using the point.

6. Proposed Model

As mentioned in the above, if we assume that security vulnerability of the super computer is generated, the optimum decision-making is not supported to the natural disaster as well as the policy decision of nation and crisis management like the disaster. The exposure of the personal information of the people including the people's health and welfare, at the same time, the damage including the human life, property, and etc. is possible to be nationally serious because the energy resource management is not smooth [4]. Therefore, we have to study the security problem of the super computer. In this paper, we would like to the physical security problem will assume that preparation plan will be sufficient. It will propose on the security method of the responding method about the user authentication and data transmission technology.

The user authentication is certain in order to prevent the access of the third. Because he is unable to be approached if it authenticates as the method that is the user authentication certain through the biometrics, the invasion from the outside can be first prevented.

Therefore, since doing the biometrics (the face, iris, fingerprint, and etc) of the super computer administrator by the plan for reaction about this once more, it is the user authentication more certain.

Since it codes to the packet itself although the attacker attacks the spoofing attack through this cipher system exposed data are returned to the original copy. However, because the cancer · decoding of data becomes possible in case for the user biometrics KEY (symmetric key), is exposed through the sniffing attack of the attacker, to make the communication between server and client, the share of the symmetric key is needed. Therefore, the value of the symmetric key is

re-code with the public key of the server. Since transmitting the symmetric key encrypted to the server, the share of the biometrics KEY (symmetric key) between the server and client can be done. In this way, if the share of the symmetric key is comprised, when the cancer · decoding is decoded to the symmetric key value after and the transmission/receipt can data.

Nevertheless, if there is the sniffer, the network administrator or security administrator has to search whether the sniffer is periodically in the network. Or not. And the stable network plan has to be done by the confrontational policy about the last DOS attack. The stable network plan method is the variety. When the packet of over certain amount comes into the router, it is the good method to this or greater packet is not passed or operate the backup server.

REFERENCES

[1] Jiabin Deng; Juanli Hu; Liu, A.C.M.; Juebo Wu, "Research and Application of Cloud Storage," Intelligent Systems and Applications (ISA), 2010 2nd International Workshop on , vol., no., pp.1,5, 22-23 May 2010

[2] Joel Scambray, Caleb Sima, "The hacking and security", 3rd Ed. McGraw-Hill Osborne Media, 2010

[3] French, W.L., "Supercomputer network selection: A case study," Supercomputing '90., Proceedings of , vol., no., pp.154,159, 12-16 Nov 1990

[4] Fukazawa, K.; Umeda, T.; Miyoshi, T.; Terada, N.; Matsumoto, Y.; Ogino, T., "Performance Measurement of Magnetohydrodynamic Code for Space Plasma on the Various Scalar-Type Supercomputer Systems," Plasma Science, IEEE Transactions on , vol.38, no.9, pp.2254,2259, Sept. 2010

홍 성 혁(Hong, Sung Hyuck)

· 1995년 2월 : 명지대학교 컴퓨터공학과(공학사)
· 2007년 8월 : Texas Tech University, Computer Science (공학박사)
· 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
· 관심분야 : 네트워코 보안, 해킹, 센서네트워크 보안
· E-Mail : shong@bu.ac.kr