Research on Constructing an Internet-based Multi-step Security System

*Hoesung Ki * and Seongjin Ahn ***

*Sungshin Women's University, Office Information and Communication Staff
**Sungkyunkwan University, Department of Computer Education

Summary
Due to the side effects of the increasing Internet population and the proliferation of new cyberspace culture on the current Internet culture, this research seeks to construct a multi-step security system as a counter measure. This multi-step security system utilizes the existing legacy security solution firewall, intrusion detection system, and intrusion prevention system and virus wall to provide a new security system, which maximizes the effectiveness of the entire system, and also presents an ideal security system by enforcing security steps. It is also a momentous security system model which can successfully defend the system from hacking, worm virus, spam mails, and DDoS attack..

Key words:
Multi-step security system, firewall, intrusion detection system, intrusion prevention system, virus wall, security system construction model.

Introduction

The increased domestic Internet population and the construction of a nation-wide IT infrastructure have inspired a new way of life within the cyberspace, and the importance of an information-oriented campus culture is blooming. However, since the Internet is based on an open network and protocol and thus is vulnerable, the campus IT system is under constant and serious security threats, and is often exposed to misuse, destruction, forgery and alteration of the information by anillegal and malignant intrusions. Such problems not only affect individual students and the educational institutions, but can also damage the foundations of a nation, including major companies, research labs and government facilities, which could develop into a devastating social problem and may even be abused as a mean of cyber warfare. To detect and counter such weaknesses and intrusions, the Internet-based information protection technology is now a world-wide research subject, and the Korean government is already actively engaged in promoting the research with The Ministry of Information and Communication, The National Security Intelligence, The Public Prosecutor's Office, and various educational institutions and research labs. The protection technologies can be categorized into a system protection technology, an application service protection technology and a network security technology. The system protection technology includes a vulnerability analysis system, a virus vaccine, and an Authentication, Authorization & Accounting server. The application service protection technology includes a digital signature, key management, cryptographic technology to provide an authentication service, authentication seamless application services by preventing intrusions technology, PKI, and WPKI. Finally, the network security technology includes technologies to provide to the network infrastructure and paralysis of network nodes caused by abnormal behaviors. Such technologies include a firewall, an Intrusion Detection System, an Intrusion Prevention System, a Web-based firewall system, and a Virtual Private Network(VPN). However, such self-reliant and simple network security systems can only counter sporadic intrusions to individual hosts or local networks. Also, the self-reliant network security technologies provide very limited security functions like the isolation of malignant Internet addresses and the vulnerability detections, which are hardly effective in countering the recent diversified and complicated network attacks. The recent research has shown that the educational institutions are the most heavily troubled organizations from hacking, worm virus, and spam mail during the last few years. The educational institutions are locating much resource to secure information, but the awareness of the information protection by the management and the related professional personnel may have been insufficient. Currently, the information protection related projects are actively pursued in the developed countries like the United States, Japan, the United Kingdom, France, and Germany. Likewise, the Korean government is also pursuing such projects based on the “Legislative for IT network promotion and information security” in coordination with research labs and educational institutions, such that these organizations could take major roles in securing the nation from online-based attacks. In correspondence, this research seeks to construct a structured and efficient network security technology for the educational institutions to enhance the ability to counter security accidents more efficiently and intelligently.

Manuscript received December 5, 2006.
Manuscript revised December 25, 2006.
This paper was supported by Dr. Lee Sewoong’s studying Fund, 2004

2. Related researches

Until recently, the major focus has been on the single function security systems such as an intrusion prevention system, intrusion detection system, and virus vaccine, and the countermeasures have been dependent on a passive methods such as a simple address based isolation policies and a detection reports. However, to counter the recent diversified and complicated malignant intrusion methods, new types of security systems are under development.

2.1 Intrusion Tolerant System(ITS)

Most of the existing security equipments have been developed with the main focus on the intrusion prevention and detection. The intrusion tolerant system is a security system developed for the purpose of integrity and usability, in order to provide a seamless critical system services even under the effects of successful intrusions. The ITS has not reached to a point of commercialized level, but the research is under a major progress. The US DARPA's Information Assurance and Survivability, Organically Assured and Survivable Information Systems Program project is focused on this intrusion tolerant system and the Third Generation Security mechanisms. The European Malicious and Accidental Fault Tolerance for Internet Applications is also making progress in realizing the structure of the intrusion tolerant system and the related protocols. Domestically, the National Security Research Institution, Electronics Technology Research Institution(ETRI), and Korea Information Security Agency(KISA) are defining the concepts of ITS and carrying out related researches.

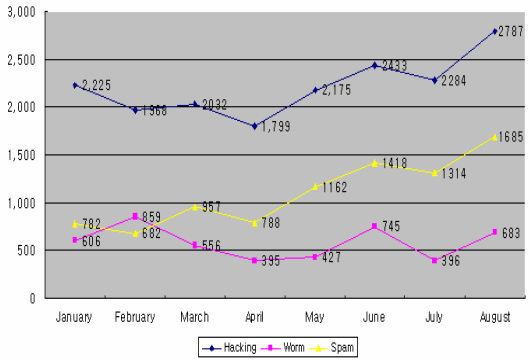
2.2 Enterprise Security Management System(ESM)

The enterprise security management is a system that manages appropriate security policies and monitors intrusion types after applying the security products to the network. Agents are installed to the distributed security systems and network nodes, and the ESM controls these agents through a centralized management module. Initially, different companies have been using independent APIs, but the international standardizing organizations have proposed a log and protocol standards that could be utilized to freely inter-connect heterogeneous systems. Besides the security functions, the ESM is developing into a system that could be integrated with the system's resource management, access authentication and verification, or even with the Service Management System and the Network Management System. Unlike the domestic products, which the main purpose of the development was to analyze logs or manage policies between heterogeneous security equipments, the HP Openview or the IBM Tivoli is developed from the traditional service management and network management system, and now adds security management functions to the existing system. Due to the unique characteristics of the integrated security management technology, a prompt establishment of the standard is hard to achieve. An OPSEC is an example of integrated security system standard, developed by the Check Point Co. In Korea, a few attempts have been made to develop independent standards such as the SAINT or the ASEN, but none have been actively pursued.

3. Current situations and types of the Internet security accidents

3.1 Current situations of the security accidents

Securing the Internet system is complex, which often is expressed with the word 'contradiction'. Especially in the campus environment, the system security must allow all members of the institution to freely access the Internet service for educational, research and administrative purposes. On the other hand, the system must also be protected from hacking such as critical data leak, data alteration and destruction.



[Fig 1] Monthly report on hacking, worm, spam relay intrusion accidents in 2006

The recent cases have shown that there have been multiple attack attempts originating from the United States, Germany, China and Japan, which were aimed to intrude into the critical campus systems. The spam mail and virus attacks counts up to tens of thousand cases per day. The [Fig 1] is a statistical analysis from the KISA on the attempts of reported hacking, worm, spam relay attempts from January 2006 to August 2006. The data shows that the IT security accidents are rapidly increasing.

Therefore, this research attempts to construct a new multi-step security system and maximize its efficacy by

analyzing the most frequently abused hacking attacks on the Internet, and proposing countermeasure technologies based on the current problems and management checks on the university campus security systems. This research also covers system vulnerability, constructing DMZ, methods to construct next generation security infrastructure and future trends of the security system.

3.2 Security accident types

3.2.1 Hacking

Hacking is a malignant act of intruding into a critical system through the network in order to extract or alter, delete data, or cause abnormalities to the system. The hackers can be categorized into a hacker, the good, and a cracker, the bad. Generally, the steps of hacking starts from collecting information, and then on to an illegal access by acquiring manager's rights, installing information gathering tools, installing backdoors, carrying out illegal actions and eliminating intrusion traces.

3.2.2 Worm/Virus

A computer virus is a destructive program that resides in the execution, the memory and the file areas of the system's operating system, and can multiply or reproduce itself. The recent trend of the virus is in the type of worm and trojan horse, that can execute itself automatically. Also, the viruses are developing into a mixed type of hacking techniques that abuses the vulnerabilities of other potentially accessible systems, which can cause various types of damage including the leakage of personal information or the destruction of data.

3.2.3 Spam mail

A spam mail is a massive advertisement that is indiscriminately sent to users with a commercial purpose, which causes an economic damage by inducing stress and causing network bandwidth loss. The types of spam mails include transmissions through self serviced mail servers, deceiving mail IDs and transmissions through mail relays.

3.2.4 Web attack

A web attack is an act of disturbing the workflow of the target system by abusing vulnerable protocol ports and altering or deleting data. According to the Gartner's survey report, most of the web sites on the Internet have shown security vulnerabilities, and 70% of the hacking actually abuses these vulnerabilities in the application program.

3.2.5 Backdoor

A backdoor is a secret pathway that is implanted by a cracker so that he/she could re-infiltrate into the system to acquire management access. The backdoor was initially and intentionally implanted by the system managers and programmers in order to get a convenient access to damaged systems. The types of backdoors include a network daemon, modified system utilities, a shell binding backdoor that uses TCP/UDP protocol, a modified kernel backdoor and a firewall detour backdoor.

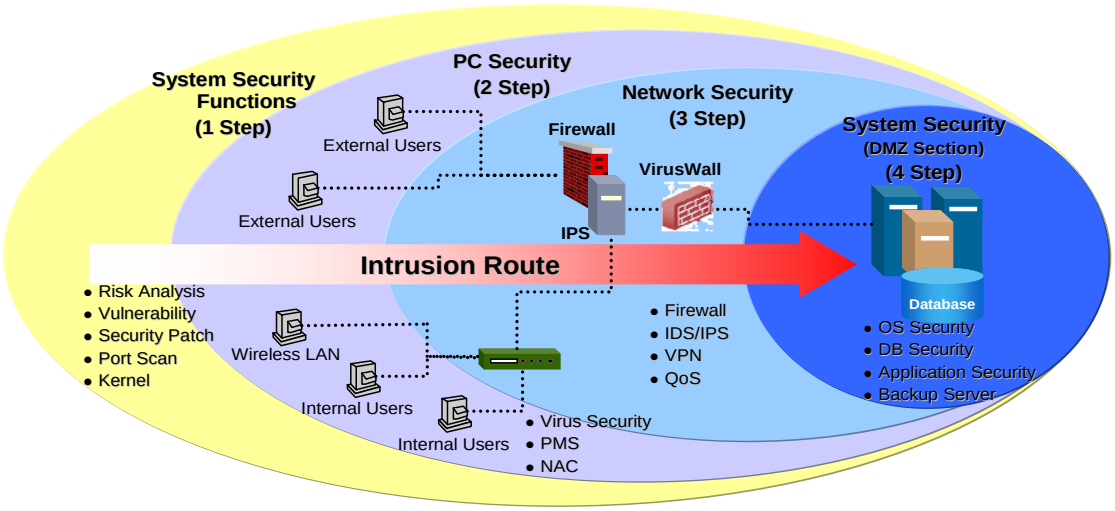
3.2.6 Phishing

A phishing is an illegal act of acquiring personal card information or account information through a fake websites, by deceiving multiple email users with forged emails from banking agencies or the like. The acquired information could be illegally abused.

4. Multi-step security system model

4.1. System concept

The existing security system utilizes various security products such as intrusion detection and defense system, an intrusion interception system, a VPN and virus vaccines to protect the network. However, many organizations do not own such basic security systems, and even if they do, these security products have limited functions. Also, many websites barely take preliminary security measures, and constructs security systems only after the vulnerability has been exploited. In order to complement the existing systems, an accurate analysis on the system must be performed and various vulnerabilities of information assets must be investigated, and the security products should be placed in the right positions so that each could complement for the weaknesses of the system. After then, an efficient security system can be constructed step-by-step, and security problems can effectively be prevented.



4.2. Security step 1 - Configuring system security functions

To construct a multi-step security system, an accurate preliminary analysis on the system environment must be performed, and the configuration of the security policies must be established through a structured risk management, risk analysis and vulnerability analysis. First, in the threat analysis, the risk factors of the systems must be located, and each of these factors must be analyzed based on its frequency and intensity. Natural threats such as a natural disaster, or intentional attacks and unintentional threats such as the users' carelessness must all be accounted for. Second, in the vulnerability analysis, the system attributes or conditions that could cause negative effects on the security of the system must be sited. The existing or the inherent vulnerabilities of the system, along with a threat analysis on the system must be performed. Third, in the security policy configuration step, the threat levels based on the threat analysis and vulnerability analysis step should be applied to the multi-step security system. The multi-step security system should be constructed based on the preliminary stepwise threat levels, or the expected cost once an accidents actually takes place, along with the methods of restoration. Also, the security functions of the server and the network equipments must be configured to establish security management system and minimize the intrusion accidents. In the first step of the security management plan, the up-to-date security patches and operating system upgrades can help to minimize the known vulnerabilities to reduce network intrusions. And by decreasing system management errors, and strictly managing user account passwords to control inappropriate system usage, and allowing proper user rights by user levels, the usability, the integrity and the reliability of the network equipments can be improved.

4.3 Security step 2 - PC security

The internal security can be constructed with the internal user-oriented virus vaccine, wired or wireless LAN authentication and an automatic patch management system. The forth mentioned security equipments can not provide protective measures against internally originated intrusion accidents. Once virus infected users or PCs that have not been patched connects to the network, or an unauthorized user connects to the LAN, the vulnerability within the internal network can cause serious intrusion damage. As a solution to this problem, a automatic patch management system and a security system should be installed to check virus and update OS patches automatically, and provide wireless LAN access to authorized personnel only. Even after constructing the multi-step security system, the security policy based on the analyzed threat factors must be strictly enforced and the security system must be managed systematically, in order to increase the effectiveness of the multi-step security system and to actively take security measures.

4.4 Security step 3 - Networks security

Based on the construction method of security system from the step 1, a gateway security system that connects the internal network system to the external network should be constructed. First, a basic network security system, a firewall must be installed. The firewall intends to protect the internal network users from the external attacks. The firewall should be installed in the pathway that connects two networks so that it can block vulnerable ports and thus deny and prevent illegal traffics. Also, an intrusion detection system should monitor traffics in order to identify abused cases and give warnings for potential

problems. The intrusion detection system is a preliminary security measure that protects the system before the system is abused or the information is leaked. Next, an intrusion interception system can be installed. The intrusion interception system analyzes the header of network packets as well as the data to detect and intercept malignant attempts, which could play a critical role in system security by supplementing the limitations of the firewall, which is merely a port based security system. To reduce the damage from viruses that can cause critical problems to the network and servers, a virus wall system is needed. The intrusion interception system has strength in intercepting DDoS and worm, but it does not perform protective measures against virus and malignant programs. Thus constructing a virus wall can provide more accurate restorations and interceptions against virus and spam. Gateway protection equipments such as described above perform an efficient interception and surveillance roles in protecting the internal network from the external, once installed appropriately.

4.5 Security step 4 - Server security

To preserve the security of the complicated high level web applications, the conventional network level security system has its limits. The major function of the web firewall is to intercept web hacking and to protect vulnerabilities of web applications. The web firewall, which intercepts the modification on websites through hacking and the access to illegal rights, effectively enforces the web security. And to strengthen the server security, the critical systems should grouped to form a DMZ. A server placed within the DMZ is a critical system that stores critical data for the entire system, and thus installing a server security solution should be seriously considered to protect critical data. The techniques for server security include a powerful user authentication and various access control methods, such as the digital signature authentication and cryptography. A DB security should also be considered to control and monitor access to DB, and to protect DB from hacking that abuses the inherent security faults of the operating system.

5. Conclusion

The importance of the Internet security is rapidly increasing as the Internet and the communication environment is constantly growing, and as such, the importance of network management is also increasing. Especially, the analysis of the security accidents and prompt countermeasures to minimize the damage is a critical issue. Under such circumstances, this research proposes a multi-step security system that can effectively counteract the new vulnerability attacks or attack techniques that abuses the regular services, such as the worm virus, hacking, and DDoS attacks by utilizing the existing security systems, including the firewall, the intrusion detection system and the intrusion interception system. The characteristic of this multi-step security system is that it fully utilizes the legacy security solutions so that it is easy to construct and provides an ideal security system. This system is an important model that can effectively protect the system from hacking, worm virus, spam mail and DDoS attacks. Also, with serious international hacking threats, this research provides a meaningful model to actively enforce the security system for the various organizations, as well as contribute to the safety of the system security by applying a new security response system technology. The research on the future oriented multi-step security system will be a corner stone to constructing an advanced security system in this information era, and an important step in guaranteeing the safety from the personal information leak and the modification, destruction and extraction of critical data.

References

[1] “Market Trends and Forecast for Firewall and IP Virtual Private Network Equipment: Worldwide, 2001-2006,” Market Trend, Gartner, Oct. 2002.
[2] NextGeneration Network Security Structure, ETRI, 2002. 11
[3] Lee, Y.C., “VPN Technology and Domestic And Overseas Market Trend,”Weekly Technology Trend, Issue 1075, 2002. 12. 4
[4] Chung, Y.S. et al, “Intrusion Interception System,” ETRI Tech Notes, 2002. 3
[5] Chung, B.H., “Intrusion Interception System Analysis,” ETRI Tech Notes, 2003. 4
[6] ETRI, Internet security system - Technology market report, 2002. 12.
[7] KISA, Hacking Virus Statistics and Analysis, www.certcc.or.kr :
[8] Lee, H.W., Paradigm Shift in Network Attacks and Countermeasures v1.0, http://www.securitymap.net /sdm/docs/netsec /attack-shift-final.pdf
[9] Lee, H.W., Future Trend of Internet Worm and Countermeasures, http://www.securitymap.net/sdm/docs/virus/worm-in-the-future.doc, 2001. 11
[10] A National Strategy to Secure Cyberspace, http://www.whitehouse.gov/nsc/nssall.html, 2002. 9.
[11] ETRI, Research on Next Generation Hacking Techniques and Analysis on Network Stability, 2001.

12
[12] ETRI, Research on Cyber Attack Mecahnism and Countermeasure Technologies, 2002. 1
[13] ETRI, Research on Security Interlocking of Legacy Network and Active Network, 2002.
[14] ETRI, Research on Network Node Intrusion Detection and Countermeasures, 2002. 11
[15] Sohn, S.W., "Present and Future of Network Security Technology," ETRI Report, 2003. 9
[16] The Future of All in One Type Security Solution, Information Security 21c, 2002. 7
[17] Lee, Y.S., "ESM Data Research," ETRI Tech Notes, 2002. 12
[18] http://www.netscreen.com
[19] http://www.network-1.com
[20] http://www.secureworks.com

Hoesung Ki received the Konkuk University Computer Engineering M.S, and Eh. D. Candidate in department of computer education from Sungkyunkwan University, Seoul, Korea, in 1994, and 2006, respectively. I was a researcher in KIST/SERI, Daejon, Korea. I am currently staff in the Sungshin Woman University Office of Information and Communication. ` My research interest include Internet management, network security, Computer Engineering, Computer education and Internet ethics.

Seongjin Ahn received the B.S., M.S., and Ph.D. degrees in In-formation and communication engineering from Sungkyunkwan University, Suwon, Korea, in 1988, 1990, and 1998, respectively. For more than five years, he was a researcher in KIST/SERI, Daejon, Korea. He is currrently an associate professor in the department of computer education, Sungkyunkwan University, Seoul, Korea. His research interests include Internet management, network security, and Internet ethics.