Security-Based Intranet Structure

S. M. Lee*, P. J. Lee**

* Penta Security Systems Co., Ltd.
** E.E dept. POSTECH

Abstract

Intranet is an enterprise network using Internet protocols as communication standard and HTML as content standard. The Internet is like a house built on information water. It has a lot of strong points as a future enterprise network[1]. However, companies wish to have confidence in its functional and economic effectiveness and security before adopting it[2]. The security issue especially is a problem to solve inevitably. Enterprises will hold back to adopt Intranet unless there are enough security counter plans and countermeasures against vulnerabilities of Intranet(it is the wise decision !). Nevertheless the researches related to Intranet has been concentrated on techniques for building it.

In this paper, we focus the security aspect of Intranet. Intranet security must be considered on the whole from structure design to users' services. We propose a security-based Intranet structure and security management system.

1. Introduction

There is no doubt that Internet has become the largest information reservoir and communication network in the world. Due to the Web, the number of its users has increased explosively. After the Web revolution enterprises which have remained indifferent to Internet have rush to access it.

Internet is also used as an advertisement board which worldwide users can watch at any time. In aspects of profit-pursuit and management-rationalization, Internet has become an important variable to companies. Companies began to view the Internet business as an image ad. and electronic commerce. In other aspect they hope to use Internet infrastructure for company affairs. Now, they are in front of the VPN (Virtual Private Network).

These requirements and desires are stimulating the structural change of enterprise networks. Intranet, a new concept supporting the above requirements is spotted as the

next generation enterprise network[1][3]. It is a private network based on Internet. It uses the Internet TCP/IP protocols as the communication standard and HTML as the content standard. This means that users can navigate Internet and dispose their company jobs on a web browser. By advent of Intranet, Internet gained another function, common infrastructure of enterprises.

As deciding to change our network to Intranet, we are confronted by practical problems, the implementing technique and security problem. The implementing technique, as Internet technique and HTML-to-DB transform technique are realized rapidly even though roughly. On the other hand, the security problem remains in a vulnerable state than ever before.

Requisites for future enterprise network are integration, simplicity, availability, and most importantly, security.

If a company does not come to the security level it wants to reach to, it may be better off not opening Intranet.

In order to enhance the security level of Intranet aspects of management, structure as well as technique should be considered all together from the beginning.

In this paper, we propose a security-based Intranet structure regarding the above three aspects.

2. Preliminary Concepts

2.1 Intranet Requirements

- Integration : It means that internet services, groupware services, DB and so on can be well connected and their data transformed easily. It take off the extraordinary job in managing the same data in different servers and users can access to various kinds of network services easily.

- Simplicity : On one interface, web browser user can navigate Internet, deposit his company job. There is less effort for users to learn to handle new groupwares.

- Availability : Intranet should be able to accommodate new communication protocols and be suitable to EDI/EC systems easily. It is especially important that Intranet can support EDI/EC as one of the future global network services.

- Security : Partially or entirely, Intranet opens itself to Internet (the untrusted). Intranet is very attractive not only to skillful Internet hackers but also to its employees. Of course, damage by the attacks would be serious.

2.2 Aspects for Intranet Design

Three aspects that we design Intranet on need to be introduced.

- Policy and Management : Currently it does not seem that current enterprise networks, even closed networks, are well managed. The poor management of the network lets the efficiency fall and impedes the progress of the networks. Of course, it would exert the bad influence on the competitiveness of company. In fact, after companies have invested considerable fund to build computer network systems, almost all of them have taken meager care of their networks. Most company jobs are accomplished on their computer networks, to manage a company may be considered as to manage its computer network. Therefore the computer network policy should be established in accordance with the company management policy. Intranet, an enterprise network, should be designed based on the company management policy, computer network policy, and security policy[4][5].

- Security Structure : Structure of the computer network effects the security level of the network. We can get the best security level when all of the computers are isolated; however, we can think that this is no longer then . It is important that functions and security are harmonized adequately.

- Functions : Each enterprise can choose the functions that it needs. Intranet should be designed to serve the functions effectively. Intranet can accommodate more merits than any other enterprise network concepts.

3. Security-Based Intranet Structure

In this section we propose a security-based Intranet structure. We explain this model in aspects of structure, management, and technique.

3.1 Structure

Our Intranet model consists of four server groups(type I ~ IV), DB, and security management system [fig.1]. Each server group constitute a subnet in Intranet.

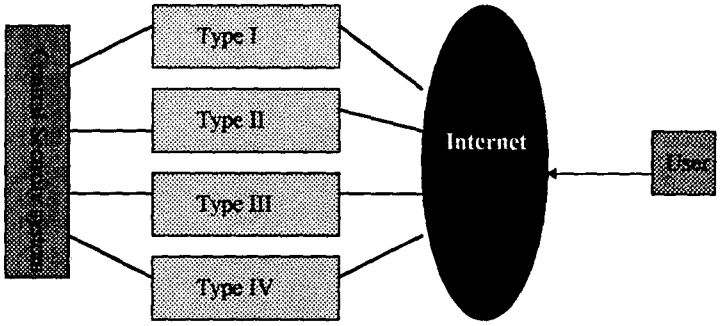

Fig. 1 : Proposed Intranet structure

- Resource Organization

Our Intranet model consists of servers, DB, and security management system. Is it strange that it doesn't include clients ? Intranet is a kind of VPN (Virtual Private Network). Intranet authenticates user only by his ID and his secret data. Even legal user has no advantage before logging on the system.

We categorise Intranet servers into four types according to function. Type I is the group of servers for public information and advertisement. Type II is the group of information servers just for employees. Type III is the group of servers to support company jobs in each department. Type IV is the group of servers to offer special information or programs, which may be sold.

- Security Requirements

Type I : These servers hold public information of the company or its products. These servers hope that many watch the contents. Though these servers do not seem to need any security countermeasure, this is not true. We hope that worldwide users access the servers just for reading but in vain, there are a lot of hackers to ransack the servers. When attacking a network, hackers try to get into the server with vigilant hostility at first because the server's security is relatively weak. If they

would succeed, the server(maybe the network) fall into his hands since the time. Therefore the server managers should block the access but have it available only for reading. They should also check the integrity of the contents from time to time.

Type II : These servers are for supporting information only to the employees of a company. These servers also allow only read right privileges. In VPN, employees may be scattered in different places of Internet. The server manager (document manager) should authenticate all accesses thoroughly. Next, these servers need an intrusion detection system[6] which is used to protect the server manager's illegal actions. Even though the server manager is responsible for the security of the server, he(she) should be checked by someone. In our model, special action (suspicious) of the server manager is monitored by a central security system.

Type III : These servers correspond to current servers for company jobs. The servers need secure user authentication and access control. Since the servers handle almost all of company jobs, action of the legal users should be audited. Intrusion detection, digital signature, data encryption could be used to strengthen its security. These servers can be the private network servers in narrow meaning.

Type IV : These servers can be used for the selling of software or for the distribution of special programs. Users who access the servers would like to authenticate the object (even the server) when they buy it. The servers should serve as a mutual authentication service and data integrity checking function.

3.2 Security Management Structure

In our model, security management is controlled by four kinds of groups : central security manager(s), group security managers, server security managers (document managers), and users [fig. 2].

Central security manager(s) : This group is a top class responsible for Intranet security. They establish the security policy of their Intranet, manage the security mechanism, audit group security managers and server security managers.

Group security managers : These are responsible for the security of company departments. Each group security manager(s) manage security of a working department.

Central security manager(s) hand over authority related to group security to group security managers. The group security managers of a department set up the security policy of their department, control security services, and audit users. These are security managers of type III.

Server security managers : Servers in Type I, II, IV permit the access for reading or downloading. The main treat on these servers is illegal operation of resources (documents, programs etc.). The resource operator must be the only person who is able to handle the resources. Therefore, it is effective that the resource operators become server security managers. They are responsible for the server security, and the central security manager(s) audit their commands.

Users : Users of type III are responsible for security of their accounts and documents.

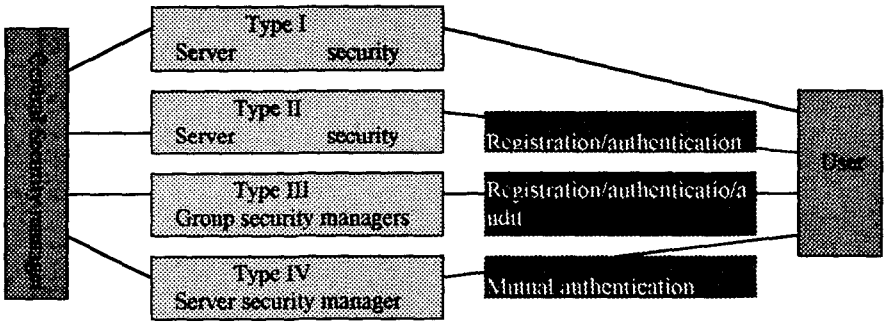

Fig. 2 : Security management structure

3.3 Security Techniques

Four types of our Intranet servers require different security services respectively [fig. 3]. Though type I does not need special security services, it should be able to block remote login and other network services. Type II needs user authentication service. When the number of the servers is over than a few, it is desirable that the user authentication service be implemented on firewall. Type III needs security functions of user authentication, digital signature, data encryption, and intrusion detection. Firewall can be implemented on each group (department). Type IV needs mutual authentication and

data integrity check. Central security system requires monitoring, and an alarm. It should support a key management system in order to use cryptosystem.

In the proposed Intranet structure, each server groups (type I ~ IV) are managed independently, even though the security management is based on the central security system. All users are authenticated only by his ID and password or cryptographic authentication scheme, not by domain or access route.

The following is features of the proposed Intranet model.

- Server-based security structure : One of the merits of the Intranet is to be able to construct VPN. In this case, the security object of the enterprise network is the server (including DB) rather than the LAN. The "internal"and "external" concepts in an enterprise network are meaningless. It is a well known fact that the threat by internal users are more dangerous than the thing by external users.

- Classification of servers : Intranet includes several kinds of servers. Each of them require different security policy and service. It is neither secure nor effective to adopt a firewall as a safeguard for Intranet. It is a requisite to classify the servers in aspects of function and security. Each type will need different security levels. Managing server groups independently minimizes the consecutive attacks.

- Central/distributed security management : In the proposed Intranet, central security manager(s) convey almost security management authority to server security managers. Central security manager(s) hold audit authority. In this model security managers are able to cope with security accidents swiftly.

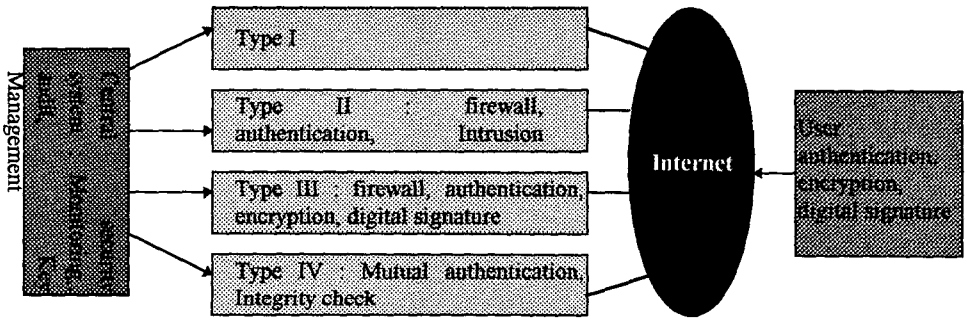

Fig. 3 : Security techniques on Intranet

4. Security Issues

In the proposed Intranet structure, security management is handled by server security managers primarily. Security accidents would happen in a server, a server group, or a security service. Security countermeasures could be set up in the server group or the security service independently. The responsibility for security management is belong to server security manager primarily and central security manager finally.

- Security Issues of type I : Threat to these servers is log-on by a non-security manager. Even security manager remote log-on through general password should be prohibited.

- Security Issues of type II : Threats to these servers are access of illegal users, trying for prohibited authority. Access of illegal users is checked by authentication service, and trying for prohibited authority is controlled by controlling network services in the server.

- Security Issues of type III : These servers require the highest security level in Intranet. The security issues of this type are accesses of illegal users, attacks to data on cable, unauthorized action, and attack on the security manager. The first security problem depends on the authentication system of firewall because users should pass firewall to get hold of type III servers. The second problem, unauthorized action of legal users, is difficult to prevent. To diminish it, logging and digital signature scheme can be used. Attack of security manager is so serious and almost impossible to prevent it before. In the proposed model, we reduce the authority of the security manager within the limits of the possibility and allow him the passive authority like monitoring and audit.

- Security Issues of type IV : The services provided in type IV are programs for execution and paid data. Therefore, the provider (server) should assure users that the provider itself and its resources are true and not unchanged. In the servers of type IV, mutual authentication and data integrity are necessary.

5. Conclusion

Though it seems to not be risky that enterprise networks were constructed without considering security issues in a closed environment, worldwide-open private network (Intranet) should hold enough security counter plan and it be reflected from its construction. Security counter plan include security policy and security management plan. Intranet can be built on various models, but it is better to take on security-enhanced model. We designed a security-based Intranet model. Our Intranet model shows that the distinction of internal users and external users is meaningless in VPN. Network security depends on its structure, security management system, and technical security components. We considered two of these factors. In the future, we expect that research on development technical security system for Intranet will follow.

References

[1] Process Software Corporation, "Intranets : Internet Technologies Deployed Behind the Firewall for Corporate Productivity", http://www.process.com/intranets/wp2.htp, 1996.

[2] Kathryn Esplin, "8 important issues to consider before building an intranet", http://www.sun.com/sunworldonline/swol-03-1997/swol-03-intranet.html, 1997.

[3] Steven L. Telleen, Amdahl Corporation, "Intranets and Adaptive Innovation", http://amdahl.com/doc/products/bsg/intra/adapt.html, 1996.

[4] Steven L. Telleen, Amdahl Corporation, "The IntraNet Architechure", http://amdahl.com/doc/products/bsg/intra/infra.html, 1996.

[5] Steven L. Telleen, Amdahl Corporation, "Intranet Methodology", http://amdahl.com/doc/products/bsg/intra/offering.html, 1996.

[6] William Stalling, *Network and Internetwork Security*, Prentice Hall, 1995.