Security Technologies for Dynamic Collaboration

By Hiroshi MIYAUCHI,* Ayako KOMATSU,† Masato KAWATSU‡ and Masashi SUGIURA†

ABSTRACT Security is an essential issue for Dynamic Collaboration. NEC has developed the iBestSolutions/Security framework as the security basis of Dynamic Collaboration. The main components of iBestSolutions/Security are security management, cyber attack protection, integrated identity management and information disclosure management. NEC is also developing new security technologies including privacy protection that will be necessary in the future ubiquitous society.

KEYWORDS **Information security, Security management, Cyber attack, Authentication, Authentication federation, Privacy protection**

1. INTRODUCTION

Security is one of the most important issues in Dynamic Collaboration that allows wide area collaborative use of computation resources. Security technologies are needed in system development such as BtoB and e-Government, since security functions are essential not only to protect systems but also to realize new services. For example, electrical voting, biddings and lotteries are expected to be carried out in e-Government. These applications cannot be realized without efficient security technologies.

To keep systems secure, total security consideration is essential, because a security hole in a system component can make the whole system vulnerable. NEC has developed a security framework "iBestSolutions/Security," to realize totally secure systems. It protects systems from numerous kinds of threats such as cyber attacks via the Internet. The iBestSolutions/Security is based on four major functions. The first one is Security Management which ensures the synthesis of security measures. The second function is Cyber Attack Protection that prevents attacks such as illegal accesses. As the third function, Integrated Identity Management is a technology that can combine multiple authentication areas together. The last function is Information Disclosure Measurements that prevents information leaks. It is also necessary for iBestSolutions/Security to develop some new technologies to meet the future security environment. The most important one is privacy protection. If authentication is adopted in every service, the privacy of Internet utilization can easily be broken. In other words, authentication is opposed to privacy, in some degree. NEC is developing a number of privacy protection techniques to realize adequate coexistence of authentication and privacy protection.

The following sections of this paper introduce technologies of iBestSolutions/Security. The four major functions of iBestSolutions/Security are discussed in Sections 3 to 6. Privacy protection technologies are introduced in Section 7 as an example of future technologies.

2. SECURITY MANAGEMENT

There are various measures against security incident. However, it is not effective to conduct those measures separately. To ensure security measures, we have to consider synthetically the protection of what information asset, from what threat, by what execution. To carry out these measures is security management.

Security management is the fundamental of security measures. Security management is achieved by selecting and properly combining security measures, for example to assess security risk, to plan security strategy, to institute security policy, to build security promote framework, to conduct security audits, and so on.

When implementing security management, it is useful to refer to documents such as "The Security Policy Guideline" made by the Government, "ISO/IEC 17799," and "ISO/IEC TR 13335." To implement security management, it is necessary to be familiar with these documents and standards. Moreover, much knowledge and experience of IT security are indispensable. Having high-level competence in IT security areas, we can achieve security management following the documents and standards. Furthermore, we provide a variety of useful services such as assessing security risk, planning security strategy, instituting security policy, building security promote

*Internet Systems Research Laboratories
†IT Platform Systems Development Division
‡System Platform Software Development Division

framework, and performing security audits.

3. CYBER ATTACK PROTECTION

3.1 Conventional Arts

There are many tools intended to secure our network by preventing illegal accesses from the Internet. We choose one or more of them according to our purpose and the required level of security, sometimes making use of a number of them in combination (**Fig. 1**).

However, operating such tools separately is not sufficiently effective.

For example, even if an IDS (Intrusion Detection System) has been installed, a considerable amount of work is still left to human beings: the administrator has to determine if an alert indicates a real attack or not, for it only detects "suspicious" accesses, and if so, has to re-configure the firewall manually to block the illegal access.

Furthermore, it is difficult to completely prevent attacks aimed at security halls in operating systems or applications only with a firewall or an IDS. We have recently seen attacks which aim at vulnerabilities in Web servers, SQL servers, RPC and etc. Such an attack cannot be blocked by a firewall, nor even detected by an IDS until provided with the "signature" (matching pattern for an attack sequence) specifically addressing the attack method.

Most of the conventional security tools have focused mainly on blocking illegal accesses and preventing penetration. Thus we can see limitations in their ability to address recent attack methods. As the next generation of security measures, we need some new technologies to avoid being targeted and to minimize damage even if penetrated.

3.2 Development of Express5800/SG300a

Blocking illegal accesses is still essential in the pursuit of network security, and we consider that firewalling plays the fundamental role there. Our point of view is that adding security functions to firewalling and making them cooperate closely enables a security gateway that totally protects our network.

Standing on this concept, we have developed a completely new appliance firewall product "Express5800/SG300a" (hereinafter "SG300a") as the first step, our final goal being to develop a security gateway system around this firewall, which will provide total security.

We have implemented in SG300a not only functions to prevent illegal accesses and penetrations but also functions to avoid being the target of attacks and to minimize damage following penetration. Specifically, as ways to avoid being the target of an attack, we implemented:

- server faking function which intercepts a request directed to a non-existent server, fakes the server

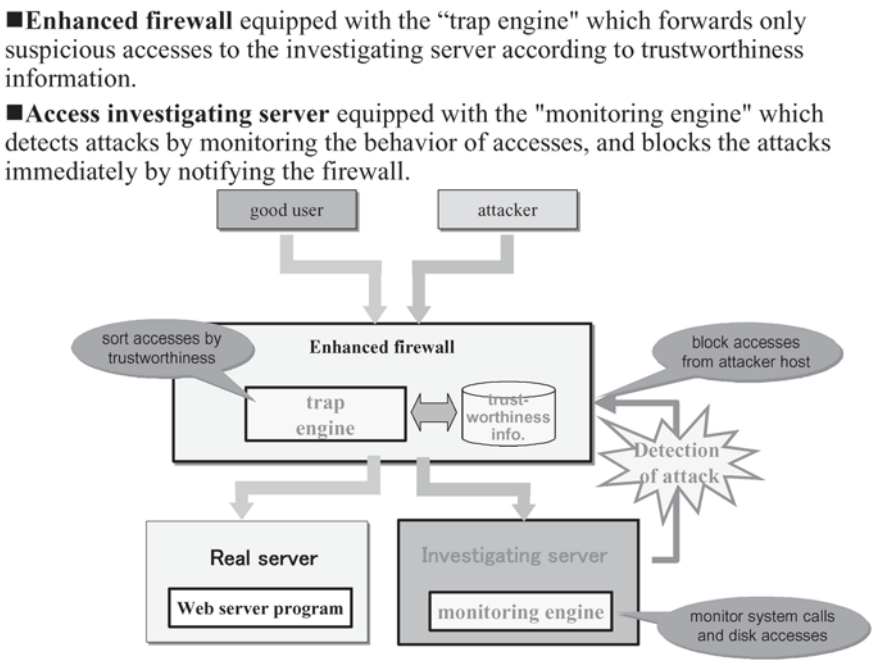

Fig. 1 Enhanced firewall and access investigation server.

reply and convinces the attacker that the server exists,
- self hiding function to avoid being the target of an attack itself.

As ways to minimize the damage of an attack, we implemented:
- host-based intrusion detecting function which protects the firewall itself,
- network-based intrusion detecting function which detects an attack or the preparation thereof, like conventional IDSes.

With these features together with the core firewalling technology, the system addresses each step of the procedure of an attack, starting from searching target hosts through the execution of attack.

3.3 Future Work

Extending the concept of damage minimization, we are currently carrying out the development of "server protection system," which works as an additional component to SG300a and protects Web servers. It minimizes the damage of an attack and guarantees the services' continuity for good users, even if the attack succeeded.

In this system, "investigating server" is added next to the real server. Communications are checked in terms of "trustworthiness" calculated in a certain algorithm, and suspicious accesses are forwarded to the investigating server. The investigating server monitors the behavior of the forwarded access and determines if any harm has been done. If nothing illegal has been done, it returns the access to the real server, or otherwise tells the firewall in front to block succeeding accesses from the same source host. Combining this architecture with SG300a makes it possible to keep the real server untouched.

As already mentioned, we see that network attacks aimed at security holes in operation systems and applications are showing consistent increase, and the conventional concept of "protection" is no longer sufficient. Damage minimization and rapid recovery will be the fundamental concepts. Providing solutions based on such concepts and on SG300a, we are planning to carry out further research and development to maintain the safety of our network.

4. IDENTITY MANAGEMENT

Integrated ID Management is the new AAA solution which consists of Authentication and Authorization, Administration. This section describes authentication and directory technologies. It also mentions ID federation which combines multiple authentication areas together with the NEC Integrated management Platform.

Directory is a useful technology as a repository sharing data between different systems because data format and protocols for accessing are specified by a standard body. LDAP (Light Weight Directory Access Protocol) is the most popular standardized access protocol. There are many products supporting LDAP including NEC's Enterprise Directory Server. With the LDAP server, ID, attributes, and authorization attributes are stored and administrated thought Directory Services. In order to satisfy the requirements of Dynamic ID management, the Directory federation shown in the **Fig. 2** is applied. However, it needs a unified policy and strict operation agreements between organizations.

ID Federation is a technology that enables single-sign-on and dynamic access control. The specification of ID Federation is promoted by Liberty Alliance and WS-Federation. NEC joined Liberty Alliance as a sponsor member in Oct. 2003. **Figure 3** shows an example of single-sign-on of ID Federation, in which the user can access SP (Service Provider) after authentication by IDP (Identity Provider).

4.1 Authentication Federation

Authentication Federation is applied in the case of collaborated organization in which multiple IDPs exist. The user is identified by federated IDP, and authorization is then enforced on federated application resources based on attributes belonging to ID. It is important to enforce access control based on

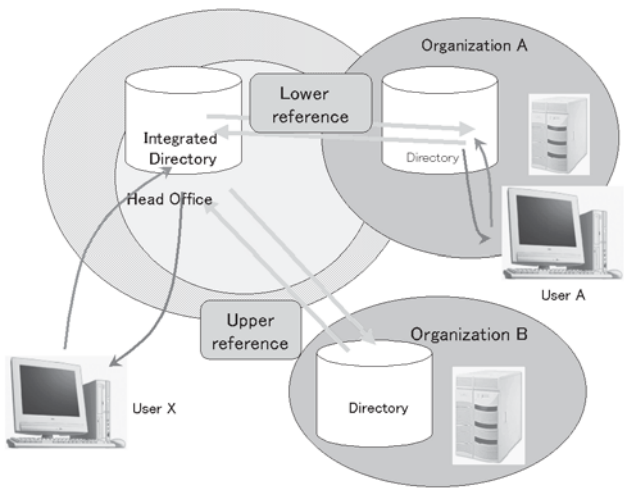

Fig. 2 Directory Federation.

attributes, so Privilege management is an essential core technology.

4.2 Distributed Privilege Management

Since privilege management handles various items of attribute information, it is required to be consistent with privacy. The distributed privilege management system returns Boolean to privilege based on access policy without extracting attributes. In this case, different types of attributes are managed distributively by different organization or services, so it is necessary to inquire about possession of privilege in order to enforce a different policy (**Fig. 4**).

A location service which provides the location of adequate attributes and an audit mechanism for record of attribute modification are important components of the privilege management system.

5. INFORMATION DISCLOSURE MEASURES

According to the present state of measures against information leaks, 80% of them are considered to be attributed to problems within an organization, and most of them depend on the operational rules. Moreover, the overwhelming majority are caused by many examples of human errors rather than disclosures performed with malice.

5.1 Classification

Measures against information disclosure are as shown in **Fig. 5**. There are two effective deterrent measures, as a result of measures. To obtain those effective measures, restrictions, protection, monitoring, defense, and public announcement measures are required.

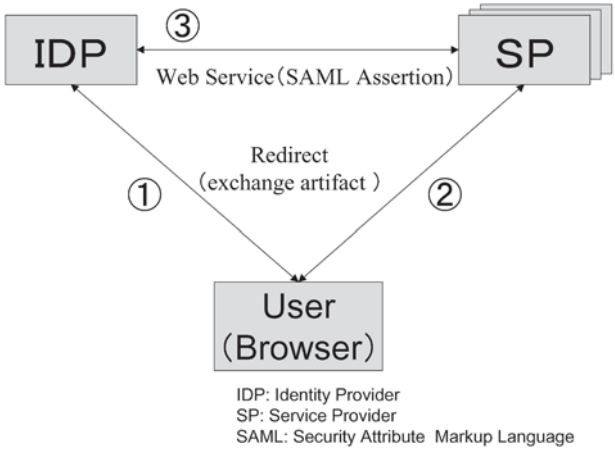

Fig. 3 Example of ID Federation.

It is important to consider what effect is expected after taking countermeasures.

5.2 Measures

It is considered that general functionality such as access control will be valid to measures. Figure 5 shows a map of specific measure against information disclosure.

1) Access control

From the viewpoint of information disclosure, print out, file attachment on mail or capturing image of screen should be restricted as well as general resources, files or server.

2) Desktop security

Client PC environment needs restriction or protection to prevent information disclosure.

3) Detection of abnormal activities

From packet records on network or operation log on client PC, it is possible to detect doubtful activities with prompt IT assets management tool.

4) Encryption

Since human operation causes 80% of information disclosure, it is effective to encrypt disks or files as a defense against theft of PC. It is also valid to encrypt all data on a server.

5) Mail sending /Web access filter

Filtering is a valid method to leak information from the internal organization to the outside. It is important to set adequate policies on filtering.

6) Audit log

Logging is considered a most effective deterrent measure. It is necessary to take audit action on the

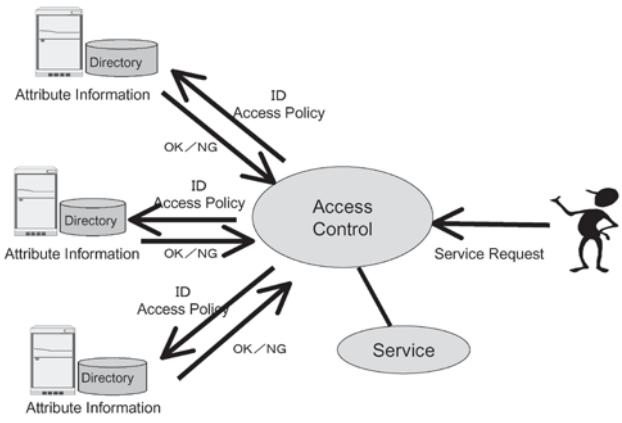

Fig. 4 Distributed privilege management.

log information and to take correct actions on the audit reports.

6. PRIVACY PROTECTION TECHNOLOGIES

The technologies shown in the previous sections make it possible to develop secure systems at high level. However, highly secure systems would lead to violation of privacy of users. For example, Internet providers can know who accesses which Web pages, by watching the access logs. Anonymous access methods can avoid this type of privacy leak, but they allow 'crackers' to use the Internet without showing their identities. It is necessary to realize traceability for emergency, as well as protection of user privacy.

In this section, two privacy protection mechanisms are introduced for examples. One is for e-voting that maintains authentication and anonymity. The other is a privacy protecting signature scheme, called "Group Signature." This technology realizes anonymous signature that allows administrators to trace the signer in emergencies.

6.1 Electronic Voting

The electronic voting law, established in 2002, allowed electronic voting in local governmental elections, but it is limited to voting in a pre-determined site. The laws also prohibited electronic communication between voting sites and the tally center.

Electronic voting via the Internet allows high speed and accurate tally as well as "location-free voting," in which a voter is able to vote in any voting site, or any computer can be connected to the Internet. However, it is difficult to keep vote secrecy, because every voter must be authenticated for voting.

A few cryptographic mechanisms have been developed to apply to both the authentication and vote secrecy[1]. The most effective one, called "Mix-Net method" is shown in **Fig. 6**. Each voter encrypts his vote and make a digital signature with it. The tallying center verifies the signature and sends it to "shuffle centers." In Fig. 6, there are three shuffle centers. A shuffle center decrypts the encrypted votes partially and changes the order of the votes (shuffle). The outputs of the last shuffle center are votes in plain text. Shuffling hides the correspondence of signed votes and decrypted votes, and anonymity of voting is thus protected. Each shuffle center proves the correctness of its procedure, to prevent malicious acts such as modification of an encrypted vote. The proof is carried out with "zero knowledge proof" technology, which allows proving correctness without revealing the direct correspondence of input votes and output votes. NEC has developed a high speed zero knowledge proof technology that enables a tally in a realistic time.

The software product "digishuff-pro" was developed based on this scheme.

6.2 Group Signature

To avoid privacy violation by system administrators, a group signature technology is useful. Group signature has the following properties[2]:

- Only members of the group can sign messages.
- The receivers of the signature can verify that it is a valid signature from the group.
- The receiver of the signature cannot determine which member of the group is the signer.
- In the case of dispute, the signature can be opened

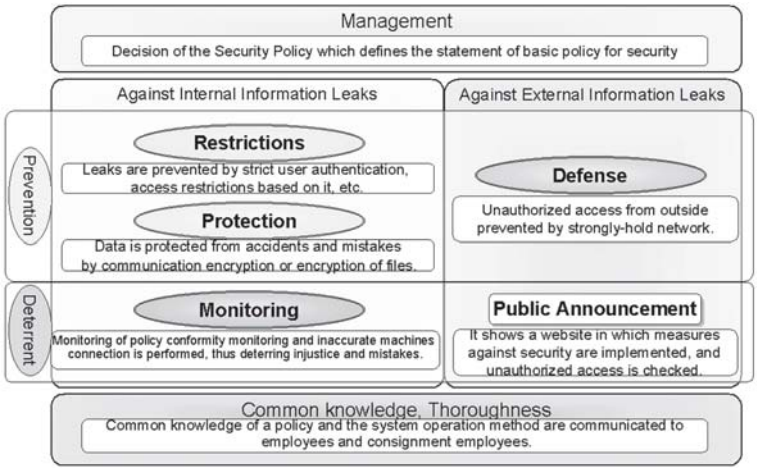

Fig. 5 View of measures against information disclosure.

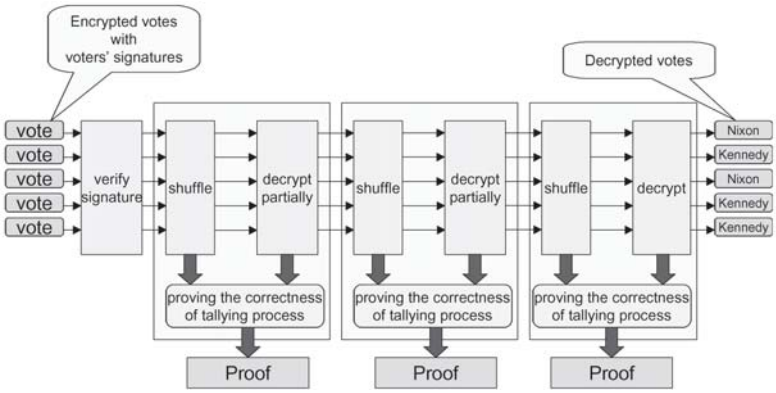

Fig. 6 Electronic voting system using Mix-Net.

to reveal the identity of the signer.

With this technology, a user of a system can show his authority without revealing his identity. This function means that a group signature can be used for an adequate combination of authentication and privacy protection.

However, there remain a few problems in management of group signature schemes, such as management of membership; every member has to update his private key when a member withdraws from the group.

We are developing a new group signature scheme to enable practical system management. We are also proposing a new signature scheme, in which signatures of a member are limited to predetermined times. This technology is expected to apply to privacy-protecting services such as ticket services, and e-voting.

7. CONCLUSION

In this paper, four key technologies of iBestSolutions/Security have been introduced as the essential foundation of Dynamic Collaboration. The privacy protection techniques are also proposed as new technologies for the future security environment. NEC plans to utilize these technologies effectively to develop secure ubiquitous societies.

REFERENCES

[1] K. Sako, "How to Secure Network Application Systems Using Cryptographic Protocols - Electronic Voting Systems Case," *NEC Res. & Develop.*, **43**, 3, pp.191-194, July 2002.

[2] B. Schneier, "Applied Cryptography, 2nd edition", Jon Wiley and Sons, 1996.

Received February 5, 2004

* * * * * * * * * * * * * * * *

Hiroshi MIYAUCHI received his B.S degree from Tokyo University in 1983, and his M.S degree in 1985. He joined NEC Corporation in 1985. He is engaged in the development of computer animation, artificial intelligence, and information security technologies. He is now a Senior Manager at NEC Internet Systems Research Laboratories.

Mr. Miyauchi is a member of the Information Processing Society of Japan.

Ayako KOMATSU graduated from Japan Women's University and joined NEC 1981. She is responsible for developing security products and services in terms of PKI.

Masato KAWATSU received his B.S degree from Kyoto University in 1987. He joined NEC Corporation in 1987. He is engaged in the development of electronic mail systems, authentication servers and security system products. He is now a Manager at NEC System Platform Software Development Division.

Masashi SUGIURA joined NEC Corporation in 1983, and is currently Consulting Manager of the Security Technology Center, IT Platform Systems Development Division.