

Establishment of Improved Business Security Systems

Wookjae Cha, Dongho Won

Abstract—Many of recent security systems are used in linkage with previously defined security systems. In particular, access control functions are used in all security systems. Network access control systems have now become the basics of security systems. In this paper, an improved business security system using network access control will be proposed. The improved security system will be established to enable businesses that become to have security systems changed as their environments are changed into wireless environments to apply security systems more effectively. A system that can be applied to all environments will be established through the establishment of an improved business security system applied with modulization and plug in systems.

Keywords—Network access control, NAC, Security, business, security system.

I. INTRODUCTION

RECENTLY, with the development of information technology, various kinds of threats to security such as hacking have been increasing and this situation has been approaching business management as serious threats. In the past, hackings were done by hackers in order to show off their skills. However, recently, hackings aimed at taking monetary profits or political purposes are increasing rather than showing off skills.

Personal information leaks, game item hackings and financial transaction hackings occur frequently and businesses are being threatened against their survival due to cyber security accidents by personal information leaks or collective lawsuits raised by victims damaged in their properties etc. Not only hackings but also other threats such as paralyzing sites through attacks by distributed denials of service(DDoS) that paralyze sites by sending so many access signals to the extent that cannot be handled by the networks from multiple PCs to extort money in exchange of relieving the paralysis are also prevailing. If a business's information system is paralyzed or destroyed, major works of the relevant business cannot but be paralyzed also. In this case, the business can also become a target of other hackers and it will be difficult for the business to avoid direct decreases of sales, limitations in new businesses and the fall of the business's brand image values.

IT environments in modern society are changing day by day. We are living in an age where we cannot think of any life or food, clothing or shelter excluding information systems. The work environments of businesses are also changing rapidly and employees work from home using Internet, check e-mails using smart phone while they are moving and when they are in a meeting after moving to the meeting room, they access to in-house computer networks using wireless LAN. In these new environments, new information security problems exist without exception.

Businesses established network access control environments to minimize intrusion into internal networks by external parties and apply document security to all documents in order to minimize damage when the documents are leaked. For safe information protection environments of businesses, the businesses should clearly define the subjects to be protected. They should clearly define which pieces of information are important, which pieces of information are to be protected and what values the pieces information have and how the pieces of information exist in their organizations and should establish measures to protect the pieces of information.

For those pieces of information that have been defined as requiring protection, strategies for methods to access to the subjects of protection should be established through accurately grasping work flows. Since appropriate measures to respond are necessary to protect information, the business should know how the pieces of information to be protected are created, used, transmitted and discarded, that is, what their life cycles are and how they are handled in works in order to grasp how they can be leaked in their life cycles or while being handled. In addition, human security is essential to the establishment successful security management and measure to manage or appropriate measures to control persons who actually use internal information should be presented. Since information is handled and also leaked by persons, the key of all measures to protect information should be focused on persons first. However, human security cannot be achieved by education alone. The possibility of information leaks by internal users and external malicious intruders should be eliminated through systems and internal users should be controlled and inculcated with the sense of security through powerful security policies.

As shown in the above [Table 1], businesses' security properties are largely divided into data and networks. Important internal confidential data and information on customers are data to be protected and networks through which the data to be protected should also be protected.

TABLE I
CLASSIFICATION OF BUSINESS PROPERTIES

Property	Risk factor	Threat scenario	Countermeasure
Data	Malicious attacker	<ol style="list-style-type: none"> 1. Malicious attackers access to the communication network internal to the business from the outside of the business using their terminals and communication networks. 2. They access to the DB server internal to the business. 3. They access to confidential data and achieve their purposes through reading and/or falsifying the data. 	Firewall VPN DB security server Data coding technology DRM
Network	Malicious attacker	<ol style="list-style-type: none"> 1. Malicious attackers access to the communication network internal to the business from the outside of the business through their terminals. 2. They monitor data and networks internal to the business. 3. They achieve their purposes by collecting information on network users internal to the business and monitoring the flows of various data. 	NAC Firewall VoIP

Risk factors for businesses' properties are divided into internal ones and external ones and the most core risk factors are malicious attackers. Threatening scenarios refer to acts to access to confidential data and networks containing confidential data through any path that can be attacked by malicious attackers from the outside.

When data are targeted, the following threatening scenarios exist.

- Malicious attackers access to the communication network internal to the business from the outside of the business using their terminals and communication networks.
- They access to the DB server internal to the business.
- They access to confidential data and achieve their purposes through reading and/or falsifying the data.

When networks are targeted, the following threatening scenarios exist.

- Malicious attackers access to the communication network internal to the business from the outside of the business through their terminals.
- They monitor data and networks internal to the business.
- They achieve their purposes by collecting information on network users internal to the business and monitoring the flows of various data..

As for businesses' countermeasures for security, businesses already have security systems that can prevent attacks by malicious attackers. Businesses already have diverse security systems that can control access to networks for protecting data such as coding programs, firewalls and VPN.

II. RELATED STUDIES

The security systems that have been classified into countermeasures against attacks on properties in the previous chapter will be described. The principles of operation of individual security systems and their characteristics are analyzed

2.1 Intrusion blocking/detection/prevention systems

As the amounts of use of wireless/wired Internet rapidly increase and networks are widely configured, the necessity of organizations' internal networks (intranets) is increasing. Along with it, intruding attacks using existing worm viruses and those using new malignant codes combined with the vulnerability of Internet protocols and applications are increasing. In response to these, diverse solutions that block, detect and prevent new intruding attacks are being released. Individual solutions can be divided into intrusion blocking systems (Firewall), intrusion detection systems (IDS) and intrusion prevention systems (IPS) based on their degrees to respond to intruding attacks.

Intruding attacks refer to various behaviors that are against the security policies of systems and harm the integrity, confidentiality and availability of resources used by computers or networks. Initial solutions to respond to intruding attacks were intrusion blocking systems that block exogenous intrusions between internal and external networks. However, just blocking intrusions had limitations in detecting and blocking newly appearing methods of intruding attacks that were becoming more intelligent. In response to this situation, intrusion detection systems appeared that surpassed the level of just blocking exogenous intrusions by being equipped with functions to analyze file logs, monitor networks and systems in real time and warn managers against known patterns of intruding attacks or suspicious behavioral patterns. However, intrusion detection systems had limited abilities involving false positive detections and miss detections and thus users experienced difficulties in appropriately identifying attempts to attack. In addition, although intrusion detection systems could detect attacks on networks in real time but they could not block the attacks. Accordingly, intrusion detection systems have been developed so that they can detect intrusions and respond to the intrusions and monitor even packets that passed intrusion blocking systems to detect any intrusions. The functions of intrusion detection systems and intrusion blocking systems

developed as such have been developed into systems that can detect attempts to attack, prevent intrusions in real time and protect networks and hosts from attacks in unknown methods and these systems are called intrusion prevention systems.

Before intrusion prevention systems, only the attacks that successfully intruded into systems were deemed as intruding attacks. Therefore, preparation for attacks, unsuccessful attempts to attack and behaviors which could not be certainly determined as intrusions were not included in the scope of intruding attacks. However, intrusion prevention systems regard all intrusion related behaviors as attempts to intrude. Intrusion prevention systems block attempts to intrude in real time before any intruding attacks occur and protect internal networks and hosts from unknown intruding attacks. In this respect, intrusion prevention systems are equipped with functions such as authentication, access control, coding/decoding, intrusion detection, packet and intruding path tracking and intrusion prevention. As such, intrusion prevention systems the most advanced solutions responding to intruding attacks that include intrusion blocking and intrusion detection functions.

A. *Intrusion blocking systems*

These are part of computer systems or networks that permit network services to the outside while blocking unauthorized access to networks based on the security policies of internal networks. Intrusion blocking systems implement security policies to permit or block services or access in host systems or routers that constitute networks. Intrusion blocking systems can be implemented in any form including hardware and software and they protect internal networks connected to Internet from unauthorized Internet users. All messages going into or coming out from internal networks pass through intrusion blocking systems and intrusion blocking systems examine the messages to screen out any messages that are against the security policies of the organizations .

Intrusion blocking systems are normally called firewalls. Intrusion blocking systems are divided into personal firewalls, gateway firewalls and web firewalls.

1) *Personal firewalls*

These are applications used to prevent personal computers connected to Internet from exogenous intrusions of malignant programs. In order to protect personal computers' information, personal firewalls control programs to access to local networks and Internet in real time based on security policies. In addition, they provide functions to warn users against exogenous attempts to intrude and information on applications attempting connections to networks and destination servers to end users.

A difference from general firewalls is that whereas general firewalls are used by administrators to protect the entire internal networks, personal firewalls are used by end users to protect only the computers installed with personal firewall applications.

2) *Gateway firewalls*

Initial firewalls were in the form of packet filtering. They inspected packet headers that had information on destination addresses, signal transmitting place addresses, destination port numbers, signal transmitting place port numbers and protocols etc to control packet flows. However, in this case, since only packet headers were inspected, there was a problem that intrusions could not be blocked when there was vulnerability in other parts. In addition, since the inspections could not be done considering the characteristics of applications, the firewalls were vulnerable to attacks on application layers. In order to improve from this vulnerability, gateway firewalls are located in network gateway servers to serve a function to protect internal networks from other network users using the Stateful Packet Inspection method and the Deep Packet Inspection method.

3) *Web firewalls*

As Internet has been activated, intruding attacks using vulnerable points in designs and implementation on the Web have been rapidly increasing recently. This is because existing products such as intrusion blocking systems and intrusion detection systems do not appropriately respond to these attacks due to the lack of understanding of web protocols of the systems. The focus of web firewalls is using engines that understand these web protocols to provide security services optimized to web services and actively creating rules through the perception and studies of simple attack patterns to block intruding attacks.

B. *Intrusion detection systems*

These are software and hardware that detect in real time, unwanted attempts to access to, manipulate or damage computer systems based on the security policies of internal networks. Recently, activities to study and develop intrusion detection systems that can automatically respond to attacks are actively implemented. However, since there are limitations in coping with threats to security that are increasingly becoming more complicated over time, advanced systems equipped with functions to block and prevent intruding attacks are necessary. Accordingly, intrusion prevention systems that include both intrusion detection functions and intrusion blocking functions have been recently encroaching intrusion detection system markets considerably and this will continue.

Major components of intrusion detection systems are sensors for creating audit events, consoles for monitoring audit events and controlling sensors and central engines that use the systems of rules to record events logged by sensors in databases and receive information on audit events to create alarms. In most of actual intrusion detection product groups, the above mentioned three components are implemented in one device.

1) *Network based intrusion detection systems*

Network based intrusion detection systems (NIDS) detect malicious behaviors such as service denial attacks, port scans and crack attempts by monitoring network traffic. NIDSs serve the role of finding patterns suspected to be vulnerable among all packets coming into internal networks. They also learn

patterns suspected to be malignant codes from outbound traffic or local traffic.

2) *Host based intrusion detection systems*

Host based intrusion detection systems (HIDS) monitor and analyze the states or behaviors of internal computer systems rather than external interfaces. As with NIDSs that analyze network packets, HIDSs record the access of resources against the security policies of systems and abnormal behaviors in RAMs, file systems, log files or any other devices.

C. *Intrusion prevention systems*

Intrusion prevention systems (IPS) detect intruding attacks on networks from malignant and unwanted behaviors of networks or systems to actively block the intruding attacks and their concept is more active than the passive concept of intrusion detection systems or that of intrusion blocking systems. Whereas intrusion blocking systems cannot immediately handle problems when intruding attacks have occurred, intrusion prevention systems can block packets that act abnormally in advance by finding attack signatures and monitoring network traffic. Intrusion prevention systems can control abnormal behaviors of unauthorized users by automatically detecting and controlling abnormal behaviors of internal servers.

1) *Host based intrusion prevention systems*

Host based intrusion prevention systems (HIPS) include those that operate together with kernels to intercept and analyze the events of kernels and those that operate independently. The former ones can be classified into trust operating system products having access control functions and the latter ones can be classified into products that filter events that are against security policies using signatures and behavior based analysis algorithms. HIPSs should protect vulnerable applications through learning policies such as the rule-sets of firewalls or access patterns.

2) *Network based intrusion prevention systems*

In the aspect of technology, network based intrusion prevention systems (NIPS) should process packets in real time, minimize the rate of false positive detections, detect packet transforming attacks or misuse attacks, appropriately cope with individual situations in real time and block malicious sessions through diverse intrusion prevention methods. NIPSs use methods to analyze packet patterns to define the behaviors of traffic based on time and frequency and detect any traffic that behaves abnormally using the definitions of behaviors.

D. *Major security functions of intrusion blocking /detection/prevention systems*

The security functions of intrusion blocking systems are largely divided into stateful packet inspection methods below network levels and application inspection at application levels. The stateful packet inspection methods serve the security functions to block unauthorized traffic and control data. On the other hand, packet detail inspection methods serve functions

such as authentication, authorization, billing and access control through proxy servers.

1) *Stateful packet inspection methods*

- Data link layer filtering

This is a function to communicate with Dynamic Host Configuration Protocol (DHCP) servers convert hardware addresses into IP addresses. In this stage, intrusion blocking systems inspect and filter the specific converted IP addresses. The data link layers of individual virtual LANs can also be filtered.

- Dynamic Rule-set Inspection

Dynamic rule-set inspections serve the function of connecting individual packets to connection streams. In this case, after coming into intrusion blocking systems, the packets create entries on state tables. Where, the state tables can be configured as hash tables to enhance the speed to find rules from rule sets. The vulnerability known in this stage is that when the state tables have been completely filled, the state tables are vulnerable to SYN flooding attacks and DoS attacks.

- Legality Checks

Legality checks serve the function of checking packets to make the lists of packets that do not conform to protocols and check anti-spoofing, reserved IP addresses, IP/TCP options, short IP packets and UDP packets (whether UDP packet lengths correspond to IP packet lengths). In actual product implementation, the checks are not conducted by the packet but by the data stream. As a result, legality checks have a weakness of not being able to accurately check the packet headers of some intrusion prevention products.

- IP/port filtering

This is an inspection to check packets if they conform to formats and screen out those that do conform to formats. In this stage, intrusion blocking systems send TCP RST packets or ICMP packets to connected hosts to treat errors.

2) *Application inspection methods*

- Header Rewriting

Network address translation (NAT) and port address translation (PAT) determine network performance and these address translations are implemented in table structures like state tables. In this stage, TTL Preservation and TCP sequence rewriting are conducted. A weakness of this stage is that if attackers know TCP sequence numbers, the reliability of TCP will be damaged. Therefore, if TCP sequence numbers are initialized so that attackers can estimate them, the TCP sequence numbers can be easily exposed to attacks.

- Application level filtering

Analyses at application levels are conducted on data diagrams and the filtering in this stage is called Proxying. In this stage, the entire protocols are broken down for proxies to translate all packets and serve the function of checking the packets whether they conform to protocol rules and conduct

any behaviors that are against security policies to screen the entire TCP.

- Routing Decision

After going through the above processes, packets move to intrusion blocking system operation systems. Intrusion prevention system operation systems serve the role of sending the destination addresses of the moved packets to send them to the identified IP addresses. In this stage, functions to reset packet directions and select destination ports are also provided.

3) Major security functions of intrusion detection/prevention systems

The security functions of intrusion detection systems are largely divided into anomaly detection methods and misuse detection methods. The anomaly detection methods detect intruding attacks using databases containing the results of analyses of state transition diagrams or users' normal/abnormal behavioral patterns and send security warnings to the administrator. The misuse detection methods monitor known attack patterns or attack signatures to detect attacks and then control access to IPs and ports and issue security warnings. The security functions of intrusion prevention systems include blocking known intruding attacks and attempts to intrude, minimizing false positive detections, detecting packet transforming attacks and misuse attacks and blocking malicious sessions.

2.2 Web firewalls

Web firewalls (WAF; Web Application Firewalls) are purposed to inspect web traffic in order to block web traffic that contain malignant codes or attacks. Whereas network firewalls, IDSs and IPSs prevailed in previous IT environments, as web hackings that attack on web services are increasing in the present situation where Internet has been activated, WAFs have become necessary as devices to exclusively inspect web traffic only. As shown in the following figure, WAFs exist between web servers and Internet and serve the role of detecting and blocking abnormal user requests and server responses.

Major security functions of WAFs are largely divided into request inspections, contents protection, disguising functions and adaptive learning functions. Request inspections refer to application access control, form field inspections, excessive request control, cookie protection, buffer overflow blocking, upload file/request form inspections and inspection avoidance blocking functions. The contents protection functions refer to credit card information leak blocking, resident registration number leak blocking, bank account number leak blocking, web falsification prevention, question-response type inspection and code exposure blocking functions and the disguising functions refer to URL information disguising and server information disguising functions. Finally, adaptive learning functions refer to application access control learning, form field learning, cookie learning, SQL/script (XSS) learning and shell code learning functions.

2.3 DB security

DB security refers to methods to protect databases that are the final and core subjects in information protection management from events that may cause unauthorized changes, destruction and information leaks. DB security methods are largely divided into access control/audit products that monitor the input/output paths of databases and coding products that code data per se in databases.

A. DB access control

DB access control/audit product establishment methods are divided into Sniffing methods, Gateway methods and Agent methods and the characteristics of these are as follows.

- Sniffing method

The Sniffing methods sniff packets between clients and DBMSs through port mirroring at switch terminals. These can be easily established and do not affect actual works even if sniffing servers are down. However, packets may be lost or access control may be impossible in this case and thus these methods are suitable only for monitoring in most cases.

- Gateway method

Gateway methods are methods to be located between clients and DBMSs to receive client data in the middle and send them to DBMS and thus these methods completely control access but may cause problems due to reduced network speeds in cases where large traffic should be processed.

- Agent method

Agent methods are methods to be installed in DBMS to process all data at the front terminal of DBs and thus these methods can process all SQLs processed in DBMS and thus can completely control access. However, services may be stopped if a problem occur in agents and agents should be installed in every DBMS.

B. DB coding

This is a method to code data per se and store the coded data in DBs. Methods for DB coding include coding solutions supported by solution suppliers and coding solutions provided by third parties in the form of DB wrappers. However, products released thus far have a problem of reduced performance due to technological limitations and thus their effectiveness is considerably reduced. Components for DB coding are as follows.

- Coding engines

These are code modules loaded with coding algorithms to serve coding functions.

- Key storages

These are storages for safely managing all keys used in coding.

- Key lists

These contain detailed information on coding keys.

- Key managers

These are managers that manage keys in key storages and key lists.

- Protected data

These are data that are protected through coding.

- Code consumers

These are entities that manage and process data that should be coded/ decoded.

- Code providers

These are entities that connect between coding engines and code consumers.

2.4 DRM document management system

Unlike existing paper documents, electronic documents should be managed differently from existing methods as the use of electronic documents is being generalized. Documents that have been stored in cabinets and hard files thus far have become to be stored through file servers etc and registrations and readings by responsible managers have been changed into those through networks. In addition, instead of the document security methods that have different security grades by document, security methods operated through document file authentication and access control have become necessary.

Document security methods include access control methods that block unauthorized persons' direct access to information, PC security methods that prevent information from going out of PCs and other security methods that use DRM to block all paths (copying, paste, original copy storing, mail sending and screen capture) through which information may leak while documents are being used. Of them, the methods that can fundamentally protect documents per se are the methods using DRM. General operation processes of DRM document management are as shown in (Figure 1-2). These methods use a mechanism where clients obtain licenses through appropriate procedures in order to use certain contents (file), and access to the contents based on the obtained licenses.

The DRM document management system generally provides coding, key management, policy management and tamper resistance functions.

A. Coding

1) Coding (Encryption)

Coding functions are used to protect contents (document, data etc) from unauthorized users. The intensity of security of contents becomes higher when the length of the key used in coding is lengthened or the key is safer against tampering attacks.

2) Packager

The packager is a function to code contents so that only authorized users can use them and package them in coded file structures which are safe file formats. The packager can be divided into pre-packaging (packaging in advance before

requested by users) and on-the-fly packaging (dynamic packaging based on users' requests) based on the time points of conducting packaging.

3) Coded file structure (Secure Container)

Coded file structures mean certain file formats made by coding contents and any additional information on the relevant contents. Coded file structures should satisfy the following functional factors.

- Functionality

Should support diverse contents

- At least one contents packaging should be conducted
- Meta data management should be easy

- Security

- Should have functions to ensure integrity
- Should have functions to ensure confidentiality

- Easiness to distribute

- Online distribution and use should be possible
- Distribution through offline transmission media should be possible

B. Key management functions

Key management functions are important functions to manage the distribution and control of secret keys that will enable decoding coded contents. Key management functions are more important for security than the lengths of the keys used in contents coding and indeed, businesses that develop DRM document management products do not disclose key management functions. Key management methods can be divided into centralized key management methods to manage keys from the center and enveloping key management methods to manage keys in files based on the entities that manage keys.

C. Policy management functions

1) Policy management

This is a function to actually reflect the policies of the domains that manage the authority to distribute and use contents. The authority to use contents is determined by the policies of the domains including billing policies in the case of charged contents. In the case of business contents, document authority policies etc are implemented through this function.

2) Rights enforcement

Rights enforcement is a control technology to ensure that contents are used within the authority to use specified in licenses. This is a function that serves an important role for continued protection and management of contents.

D. Tampering resistance function

This is a function that serves an important role along with coding to ensure the security of contents. In general, this function is implemented through clients' software to serve the

role of preventing malicious users from changing software or incapacitating security.

2.5 Single Sign On

Single sign on (SSO) is a security application solution that enables users to access to various work systems of businesses or Internet services with only one log-in and demand for this has been increasing recently as integration of diverse different systems such as ubiquitous, e-government and digital convergence etc has become an issue. SSO is currently divided into business type SSO that provides SSO functions using the access authority server managed internally by businesses and clients' integrated ID management systems that provide SSO functions by using the IDs/passwords used when using web services in linkage with web servers.

A. Background of the appearance of SSO

1) User side

- When using multiple applications, work efficiency is reduced due to repeated input of different IDs/Passwords
- Passwords are memorized or made easy to be remembered and thus the confidentiality of passwords is hampered.
- Erroneous inputs increase and system security is reduced
- The possibility of the exposure of user information increases due to frequent ID/Password inputs.

2) Manager side

- The necessity of unified security policies for expanding systems and management of standard user information
- Due to the lack of unified authentication methods, it is difficult to switch to reinforced authentication mechanisms
- Due to the lack of integrated management systems, central control of user information management systems and security management is difficult
- Consistent grouping by user of entire company's system resources, access control and policy application are difficult.

3) Operator side

- The productivity of HelpDesk is reduced due to many requests for password resets etc
- Since IDs/Passwords should be managed by system, security becomes vulnerable and total management costs increase
- Skills for new systems should be learned for password management.
- It is difficult to apply single security policy for passwords en bloc

4) Developer side

- User authentication related modules and login screens should be separately developed every time
- Other systems' application environments should be analyzed for sharing authentication information.

B. SSO operation process

General SSO configurations form a method where managers set up SSO related policies in advance and then users implement authentication by the SSO policy.

1) Process of managers' SSO policy set-up

- ① SSO policy managers configure SSO policies in SSO policy management servers
- ② SSO policy servers provide SSO audit functions in linkage with SSO policy databases

2) SSO user authentication process

- ① Users request web pages for SSO subject systems
- ② User authentication checks are conducted based on the SSO Agents installed in user PCs
- ③ The SSO Policy information of the users attempting authentication through SSO Agents is transmitted to SSO authentication servers
- ④ The SSO authentication servers check the user qualification certificates transmitted in linkage with integrated ID storages
- ⑤ User qualifications have been identified.
- ⑥ When user qualifications have been identified, the SSO Policy information is stored in SSO policy databases for audit logging
- ⑦ When user qualifications have been identified, responses regarding SSO Policies are transmitted to the SSO Agents.
- ⑧ The SSO Agents check the SSO Policies received from the SSO authentication servers and then provide services to the users

2.6 VoIP security system

The VoIP (Voice over IP) is IP (Internet Protocol) based voice communication services that provides diverse services including not only voice calls but also multipoint conference calls and image calls. The VoIP has advantages that IP based structures which are packet networks for existing data communication can be used as they are without any change and that expenses to be paid separately for using lines are small and thus the number of subscribers is rapidly increasing recently. However, not only threats existing in IP based structures but also threats existing in VoIP communication itself are becoming problems. Therefore, recently, methods to add functions to existing IDS etc have been used in order to prevent the threats originating in IP based structures and methods to use coding techniques have been used in order to protect the VoIP itself. Of them, methods to use coding in order to protect the VoIP itself are largely divided into methods to code SIP messages using TLS and methods to code RTP itself.

A. Major security functions of VoIP security systems

1) Security functions to protect systems from IP based threats

VoIP security systems provide security functions that can block DoS/DDoS attacks, packet spoofing and transformed messages. In addition, VoIP security systems also provide security functions that can block voice fishing and spam message mainly through the mechanisms of security policy application, authentication and identification. These are similar to the operation methods of general IPS security functions.

2) Security functions to protect VoIP communication protocols

To protect signaling protocols, VoIP security systems provide coding security functions. In this case, methods to apply TLS to SIP are mainly used. In addition, VoIP security systems also provide security functions to prevent tapping of the RTP of actual telephone conversations with the other party mainly using SRTP protocols. The following Figure shows a telephone call algorithm applied with SRTP.

2.7 Network access control system

NAC solutions are user access control systems that ensure that users with appropriate authority access to internal network resources through safe computers verified on safety. These solutions establish integrated security systems in entire internal networks by combining end point security technology with existing network security systems.

Through the network access control flow presented by Gartner, the network access control model is divided into seven functions. The baseline function is to establish security policies and compare the condition of the accessing terminal attempting to access to the network with the security policies to see if the terminal conforms to the policies. These procedures should be implemented regardless of the methods used by accessing terminals to connect to the network. NAC solutions control network access while serving reducing/relieving functions, monitoring functions, suppressing functions and maintenance functions.

A. Operation principles

- Authenticate users regardless of access channels.
- Inspect users' computers for integrity.(inspection of OS patches and configuration information (in particular, virus programs), the existence of personal firewalls etc)
- Compare the results of the authentication and integrity inspections with the policies set up in the policy management server.
- Based on the results of the authentication and integrity inspections, determine policies for the subjects accessed by the user.
- Authenticate network access of some types of equipment that may be permitted, denied or isolated. Without this procedure, user traffic can be tampered.

B. Entity

An overall TNC (Trusted Network Connect) is composed of three entities (access requesters (AR), policy evaluation points (PEP) and policy decision points (PDP).

1) AR(Access Requester)

This refers to general user terminals that serve the role of requesting for access to servers and networks and are composed of NAR, TNCC and IMC.

- NAR(Network Access Requester)

NARs are network access requesters that are used by ARs to examine network access and one AR may use multiple 의 NARs.

- TNCC(TNC Client)

This is a software entity operated by ARs to serve the role of collecting the resultant values of integrity checks (Integrity Check Handshake) received from the IMC.

- IMC(Integrity Measurement Collector)

This is an entity of ARs that checks the integrity of security matters. In general, this checks integrity such as the conditions of personal firewalls and OS patches.

2) PDP(Policy Decision Point)

This is to receive ARs' requests and compare them with access policies in order to decide whether to allow or deny the requests and this is composed of NAA, TNCS and IMV.

- NAA(Network Access Authority)

This is an entity that makes decisions on ARs' requests for access referring to the evaluation of security integrity by the TNC server.

This is included in most AAA Servers although not necessarily required.

- TNCS(TNC Server)

This is an entity that manages data streams between MVs and IMCs to serve the role of collecting the values of IMVs in order to send information on whether the access control policy of the PDP is observed to the NAA

- IMV(Integrity Measurement Verifier)

As an entity to check integrity, this checks the integrity of AR's requests based on data received from the IMC.

3) PEP(Policy Enforcement Point)

This implements access control policies referring to decisions by the PDP. For instance, this serves roles as an authenticator of 802.1x.

Major security functions of network access control systems

- Security channels between access requesters and policy decision points

To communicate integrity values and parameters between clients and servers, security channels should be set up without fail between the NARs of ARs and the NAAs of PDPs without fail. Security channels are composed of applications and network configuration environments.

- Access to NAC Clients, NAC Servers, IMCs and IMVs

In general, TNCCs (TNCS) should be designed to communicate with authorized IMCs (IMVs) only without fail. This is indispensable to prevent DOS attacks on TNCCs/TNCSs.

- Check of the integrity of ARs and PDPs themselves

The checks of data exchanges between ARs and PDPs are very important. However, to prevent wrong system modulation, the checks of the integrity of ARs and PDPs themselves are also necessary.

- Quarantine program

ARs (clients) that have been isolated because of their violations of integrity and security policies should be updated in relation to integrity by communicating with the quarantine server. In addition, powerful and safe security environments should be set up for the RS (reducing/relieving server) because, if RS is invaded, the ARs may be updated with wrong data and the entire network may be subject to serious troubles.

- Protection of information properties and interfaces

The most important thing in NAC structures is the protection of information properties transmitted between many interfaces. The states of information properties transmitted and changed in individual interfaces should be notified to the administrator quickly. When designing and implementing interfaces, the spoofing of, DOS attacks on and falsification of IMCs/IMVs should be also considered.

The security systems mentioned above are also systems that protect networks and data simultaneously. As data and networks to be protected by security systems, environmental factors to be treated are also increasing rapidly. Meanwhile, DB security systems have been installed with firewalls and network access controls to become new DB security systems. Recently, security systems are being established as these interlocked systems.

Systems that are interlocked with the subjects of protection and can manage diverse subjects of protection effectively are necessary. To review actual applications of security systems used by businesses, systems that control security are in the lime light. Network access controls (NAC) mean control systems. Given the present policy operation methods or system management, network access controls can best control the security of business.

III. PROPOSED SYSTEM

The security systems described in chapter 2 are basically installed with at least access control functions. Businesses will be able to use security systems more suitably to their environments by using a system having modularized or plugged in security functions rather than using an NAC interlocked with other security system.

3.1 Modularized in Security functions

A. Methods to modularize functions

Methods to modularize functions or software can be divided as follows; procedure modules, Procedure-based modules, block-structured modules, data modules, information hiding modules, object-based modules (ADTs: abstract data types), object-oriented modules (Classes), task modules and thread-based modules (Concurrent tasks).

1) Procedure-based modules

These are modules that have encapsulated algorithms serving single function. Data exchanges between these modules are made through parameters or global variables. Functions under the C language or procedures under Pascal correspond to these modules. The interfaces of these modules are defined by the names of single modules and their parameters

2) Block-structured modules

These are modules where procedures are permitted to contain other nested procedures inside them.

3) Separately-Compilable Modules

These are modules that can be separately compiled by compilers. These modules are composed of mutually related procedures and data structured gathered in one source file.

4) Information-Hiding Modules

These are modules that hide detailed data structures and concrete processing processes to be accessed only through operations that are made as abstracts of data types. The interfaces of these modules are defined as sets of operations composed of names and parameters.

5) Object-Based Modules (ADT: Abstract Data Type)

Modules that have the same data structure and operation are not individually defined but are defined as an abstract data type (ADT) abstracted into one module type and individual modules are created as instances of the ADT when necessary.

6) Object-Oriented Modules (Classes)

These are made by a method that analyzes similarity and differences among ADTs to factor out commonalities and abstract them into separate ADTs and then when defining similar ADTs, make them have the separate ADTs as common factors. ADTs that have common factors that can be defined by inheritance are called classes. In this case, concrete certain modules are created as objects which are the instances of classes.

TABLE III
FIVE LEVELS OF MODULE COUPLING

Level	Cohesion	Overview
5	Data coupling	Modules that serve only one function
4	Stamp coupling	Cases where data are shared by two modules by parameter passing but only a part of parameter data structures is used by called modules
3	Control coupling	Cases where, when a module calls another module, the information to control the codes to be executed by the called module is passed to parameters by the calling module
2	Common coupling	Cases where two modules access to and use the same global data
1	Content coupling	Cases where one module directly access to codes or data in another module to execute, use or change them.

B. Assessment criteria for software modularization

The suitability of modularization of software modules can be assessed by analyzing the cohesion and coupling of the modules.

1) Module cohesion

Module cohesion means the intensity and intimacy of interactions in modules. The cohesion can be divided into seven levels and it can be seen that the higher the level, the better the modularization that has been done.

2) Module coupling

Module coupling refers to the intensity of interactions between modules. Module coupling can be divided into four levels. Lower levels mean lower mutual dependency between modules.

3) Ideal module cohesion relative to modularization methods

C. Procedure to design modules

1) Procedure to design procedure modules

- ① Divide modules into specification parts and design parts.(SDU: Specification/Design Unit)
- ② Specify the types of the modules.(procedure, function, block structures etc)
- ③ Describe the names, functions, summaries of input data and output data of the modules.
- ④ Determine the algorithms necessary for implementing the functions and data structures at the higher level of abstraction.
- ⑤ Define the specification part of the modules. (Names, parameters etc)

TABLE II
SEVEN LEVELS OF MODULE COHESION

Level	Cohesion	Overview
7	Function cohesion	Modules that serve only one function.
	Information cohesion	Modules that have multiple functional factors implemented on the same data. Each of the functional factors is composed modules that have independent codes and only one entry point.
5	Communicational cohesion	Modules that contain functions that are implemented in certain orders for the same data
4	Procedural cohesion	Modules that contain a series of functions that should be implemented in certain orders
3	Temporal cohesion	Modules that contain functions that should be implemented at the same time
2	Logical cohesion	Multiple functions that are not related with each other are implemented. The functions to be implemented are selected at the time point of calling The interfaces of the modules are complicated and are difficult to be repaired or maintained.
1	Coincidental cohesion	Multiple functions that are not related with each other are implemented. Modules of which the functions cannot be easily defined. Modules that can be explained by logics rather than functions The maintenance and reuse of the modules are very difficult.

⑥ Define the design part of the modules. (PDL description)

2) Procedure to design data modules

- ① Divide modules into specification parts and design parts. (SDU: Specification/Design Unit)
- ② Specify the types of the modules.(information-hiding, ADT, object class etc)
- ③ Describe the names, functions, summaries of input data and output data of the modules.
- ④ Determine the algorithms necessary for implementing the functions and data structures at the higher level of abstraction.
- ⑤ Define the specification part of the modules.
-module interface (module name, public operation)

-module function (functions and mutual relations of public operations)

© Define the design part of the modules.

-data structure design
-operation design

3.2 Plugged in Security Functions

These are computer programs that mutually respond to host application programs and provide certain “customized” functions.

There are many reasons for application programs to provide plug-in functions; for instance, to make third party developers make functions to expand application programs, to support unexpected functions, to reduce the sizes of application programs, or to separate source codes from application programs due to incompatible software’s license issues.

A. Examples of the application programs and related plug-ins

- E-mail clients use the plug-in to code encrypt e-mails and decode codes. (Pretty Good Privacy)
- Graphic software uses the plug-in to support file formats and process Figures. (Adobe Photoshop)
- Media players use the plug-in to support file formats and apply filters. (foobar 2000, GStreamer, QCD, VST, WinAmp, XMMS)
- Packet sniffers use the plug-in to decode packet formats. (OmniPeek)
- Remote sensor programs (Remote sensing applications) use the plug-in to process the data of other kinds of sensors. (Opticks)

TABLE V
IDEAL MODULE COHESION RELATIVE TO MODULARIZATION METHODS

Modularization methods	Ideal module cohesion	Reason
Procedure-based modules	Functional cohesion	Constructing procedures as a single-entry, single-exit module is the most ideal.
Information-hiding modules	Informational cohesion	Constructing procedures so that access to data structures hidden in modules is permitted only when the access is made through the interfaces of operations in the form of single-entry, single-exit is the most ideal.
Object-based modules	Informational cohesion	These modules are defined as abstract data types made by analyzing the similarity and differences between information-hiding modules to abstract them and thus they have the same cohesion as the modules set forth under item 2

- Software development environments use the plug-in to support programming languages. (Eclipse, jEdit, Mono Develop)

- Web browsers use the plug-in to play moving images and presentation formats. (Flash, Quick Time, Microsoft Silver Light)

- Digital mixers use the plug-in to expand functions such as reverberation effects, pitch adjustment and compression.

B. Securing expandability using a Plug In method

1) Program in the Agent & Manager method

The Net SNMP applying the NMP protocol will be the most representative case. Since the Net SNMP has been already taken as an example, a program to make SMS in the Agent & Manager method will be developed.

If an Agent program is to be made in this system, one thing that must be considered to be the most important should be securing expandability because, since the scope of system management is very wide, management factors may be added continuously. The CPU, Memory and Disk should be considered first. Of course, all management factors can be completely predicted before designing the program. However, too much time may be spent for design in that case. Even if that is the case, new management factors may be added in the middle of designing. Management factors may be added even when the program has been completed.

In this case, development time can be saved by modularizing each performance by the Plug-In method and adding it to the program. In addition, flexible and highly expandable systems can be made. To understand this system, technologies for controlling function pointers, STL, libraries should be understood.

2) Dynamic Module Loading

Basic technical requirements for implementing the Plug-In method to load modules dynamically are not very complicated. The method can be easily implemented by using dynamic libraries. One thing important in this case should be unifying interfaces between the modules and the Agent because modules should be loadable without any revision of the source codes of the Agent and the Manager no matter what functions are added in the form of modules.

Identifying the interface names will not be a problem. The problem will be the data moving the interface. This is because the information to be shown may be different by performance, for instance, the rate of use should be sent in the case of CPU, device names, mount names and the rate of use in the case of Disk. Therefore, methods that can handle all expectable data should be prepared. This problem can be solved by around three methods.

a) String transmission

Strings are sent simply. They can be sent as performance=value1, value 2. The format will be roughly as follows. The reason why performance names are included is

that when the information is delivered to the manager later, the performance name will be used as a key to load the relevant module in the Plug-in method.

b) Structure transmission

The strings can also be transmitted as structures. Since the Agent does not have to process data but may just send to the Manager, the Agent does not need to know what member variables are in the structures. The Agent just needs to know the size of the structures and related performance names. After receiving the structures, the Manager just needs to load the Plug-in modules corresponding to the performance names to process the values of the structures.

c) XML data transmission

If defined well, this may be flexibly used. If the fact that the size of data is enlarged is not need to be considered, this is considered to be the best method.

IV. CONCLUSION

Currently, NACs which are access control systems basically interlocked with security systems can be said to be the basic of security systems in businesses. NACs can be reborn as security systems optimized for businesses using modularization functions and plug in functions. In addition, they can be improved into systems that can reinforce the sense of security by applying CAM. In this paper, further improvement of NAC made through customizing functions and CAM products is proposed. This study proposes security systems for businesses thereby proposing security systems in business environments that approached one step toward ubiquitous environments in the hope that this will help the development of security systems.

REFERENCES

- [1] C.C. Tan, B.Sheng, and Qun Li, "Serverless Search and Authentication Protocols for RFID", *Pervasive Computing and Communications 2007(PerCom 2007)*, pp.3-12, August. 2007.
- [2] Jung-Ho Eom, Seon-Ho Park, Tai-Myoung Chung, "A Study on Architecture of Access Control System with Enforced Security Control for Ubiquitous Computing Environment", 2008. 10
- [3] Mikko Hypponen, "Malware goes Mobile", Technical Report, Scientific American, INC, 2006..
- [4] Role Based Access Control, American National Standards Institute, February, 2004.
- [5] Sejong Oh and Seog Park, "Task-role-based access control model", *Information System*, Vol.28, No.6, pp.533-562, September, 2003.