# OS with Enhanced Security Functions for Protecting Information Systems against Unauthorized Access, Viruses, and Worms

*Jumpei Watase*[†], *Yoichi Hirose, and Mitsutaka Itoh*

## Abstract

As information-network technology progresses, it is becoming increasingly difficult to protect information systems from network security threats using only firewalls and other existing measures. We discuss an operating system with enhanced security functions that can make unauthorized access difficult and reduce the risk of infection from viruses and worms. It can also minimize and confine damage if unauthorized access should somehow occur.

## 1. Importance of information security measures

In parallel with the advancement and spread of information-network technology, the network has become a conduit of important information and vital services such as electronic commerce, online banking, and electronic government. At the same time, the risk to information security is rising due to increasingly diversified and complicated applications, an increasing number of computers with insufficient management, and an abundant supply of information and tools related to unauthorized access. Likewise, denial of information services, leakage of information, and other types of damage caused by malicious programs like viruses, worms, and Trojan horses are becoming serious problems. Under these circumstances, it is becoming increasingly important to strengthen information-security measures from both managerial and technical points of view. The NTT Group, a provider of extensive network services, information services, and IT (information technology) solution services, recognizes the urgency of this situation and is placing considerable importance on achieving in-house security while also providing advanced  security services and safe and reliable network services.

## 2. Problems with existing security measures

Typical network security measures in use today are firewalls, patch management, and system penetration detection (**Fig. 1**).

A firewall is a type of boundary defense. It divides the network into internal and external sections on the premise that the internal network can be considered to be reliable. In recent years, however, many network applications like instant messengers have incorporated tunneling techniques for passing through firewalls. It has consequently become difficult to provide a complete defense against unauthorized access from the outside solely on the basis of a firewall. In addition, the spread of technology for constructing ubiquitous environments composed of mobile and wireless networks, virtual private networks (VPNs), and IPv6 elements has diversified and dispersed entrances to internal networks, and from the viewpoint of security, the concept of network boundary is rapidly becoming meaningless. For example, it has been reported that most of the infection paths taken by last year's Blaster worm into corporate networks originated with personal computers brought into company premises from the outside.

Security patches are issued and applied when security problems are identified or after attacks occur. However, patch management requires the testing of irregularly and frequently issued patches as well as many resources for applying them to systems. Other problems include the difficulty of determining if a patch should be applied to one's own system even if

[†] NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: watase.jumpei@lab.ntt.co.jp

information about security holes and available patches can be obtained and the inability to respond fast enough due to the division of responsibility, terms of system maintenance contracts, etc.

Technology for detecting system penetration, while being useful for detecting security incidents and accumulating evidence for after-the-fact response, does not provide functions for defending systems against malicious behavior.

These technologies and products have been useful in reducing security-related risks and maintaining system stability, but there is now a need for new security technology that can address the above problems and complement existing measures.

## 3. OS with enhanced security functions

To solve the problems involved in defending boundaries, a defense must be mounted at end points themselves such as servers, PCs, and portable terminals. Furthermore, as there are no perfect security measures, we need to minimize and confine damage caused by attacks on security holes, unlawful impersonation, and unauthorized access by insiders until patches are applied.

One technology for achieving this is an operating system (OS) with enhanced security functions (also called a “secure OS”). While there is no precise definition of a secure OS, in the Japanese IT market this term has come to refer to an operating system equipped with a number of advanced security functions for performing a variety of tasks. These include fine-grain non-discretionary access control and buffer-overrun prevention to make hacking difficult, network access control (packet filtering), detection of system penetration, robust authentication, file encryption, and encrypted communications (**Fig. 2**).

Fine-grain non-discretionary access control is the

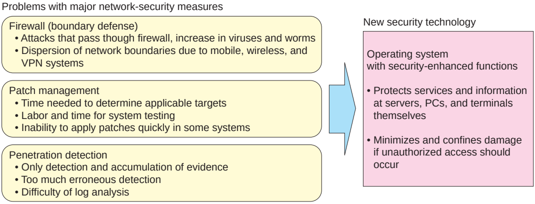
Problems with major network-security measures
Firewall (boundary defense)
• Attacks that pass though firewall, increase in viruses and worms
• Dispersion of network boundaries due to mobile, wireless, and VPN systems
Patch management
• Time needed to determine applicable targets
• Labor and time for system testing
• Inability to apply patches quickly in some systems
Penetration detection
• Only detection and accumulation of evidence
• Too much erroneous detection
• Difficulty of log analysis
New security technology
Operating system with security-enhanced functions
• Protects services and information at servers, PCs, and terminals themselves
• Minimizes and confines damage if unauthorized access should occur

Fig. 1. Existing security measures and problems and new security technology.

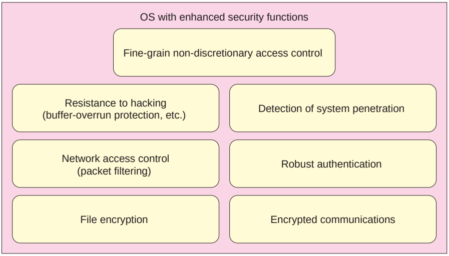
OS with enhanced security functions
Fine-grain non-discretionary access control
Resistance to hacking (buffer-overrun protection, etc.)
Detection of system penetration
Network access control (packet filtering)
Robust authentication
File encryption
Encrypted communications

Fig. 2. OS with enhanced security functions.

key technology of an OS with enhanced security functions. It can directly protect services and information that need defending and minimize and confine damage caused by unauthorized access, viruses, and worms.

## 4. What is non-discretionary access control?

Non-discretionary access control in an OS with enhanced security functions can enforce a policy established by the security manager and it provides fine-grain processing. It makes use of labels that are attached to OS resources (such as processes, files, sockets, and devices) and set beforehand by the security manager. These labels allow the OS to control access from an access subject (such as a process) to an access object (such as a file) by referring to an access control policy dictated by the labels (**Fig. 3**). Non-discretionary control is achieved by having the kernel decide whether to permit access from a subject to an object. The kernel itself is protected from user programs by processor functions.

In contrast, the access control model installed in ordinary UNIX, in Linux, and in Windows, which is based on users and groups, is discretionary access control. This allows the owner of a resource (such as a file) to set and modify access rights to that resource as desired. Moreover, "super users" such as root and Administrator, have the authority to set and modify access rights for other ordinary users.

In non-discretionary access control, however, the access control rules set forth by the system security manager are enforced for all users including super users. An OS equipped with non-discretionary access control can thoroughly deploy a security policy established by the security manager. Furthermore, in an OS with enhanced security functions, non-discretionary access control can apply detailed access control to files, devices, networks, etc. in units of individual programs and processes. Non-discretionary access control has been used in military applications since the 1980s with good results. Initially, it was implemented for controlling the flow of information based on the degree of separation between organizations and on ranks in hierarchical organizations. More recently, it has developed into a form more suitable for counteracting unauthorized access and malicious behavior on Internet servers and desktop terminals.

## 5. Strong and weak points of an OS with enhanced security functions

**Table 1** lists the strong and weak points of an OS with enhanced security functions.

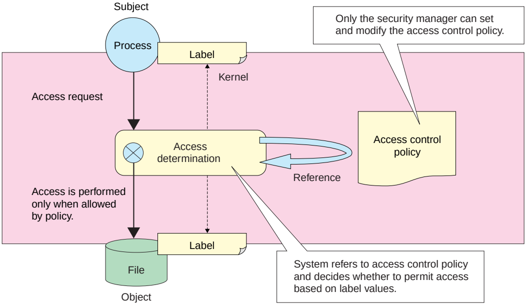
Subject
Process
Label
Kernel
Only the security manager can set and modify the access control policy.
Access request
Access determination
Access control policy
Reference
Access is performed only when allowed by policy.
Label
File
Object
System refers to access control policy and decides whether to permit access based on label values.

Fig. 3. Access control in OS with enhanced security functions.

Table 1. Strong and weak points of an OS with enhanced security functions.

| | |
|---|---|
| Strong points | 1. Makes malicious behavior difficult and minimizes damage<br>2. Improves safety and reliability of patch management<br>3. Improves reliability in outsourcing |
| Weak point | 1. Requires bothersome setting and management of access control policy |

Table 2. Limits of OS with enhanced security functions and associated countermeasures.

| Limits of current OS with enhanced security functions | Countermeasures |
|---|---|
| Cannot defend against process-contamination type of DoS attacks | Patch<br>Packet filtering |
| Cannot defend against resource-consumption type of DoS attacks | Load distribution<br>Packet filtering<br>Resource restricting |
| Malicious behavior within the rights of an application | Patch<br>Modification of settings<br>Packet filtering |
| Security hole in the kernel itself | Patch |

### 5.1 Strong point 1: makes malicious behavior difficult and minimizes damage

When fine-grain non-discretionary access control is used, users and processes can be isolated and only the minimally required rights need be assigned. This increases the difficulty of unauthorized access through a security hole in an application. If, by some chance, an unauthorized access does occur, damage can be minimized and confined. All in all, a secure OS can significantly reduce the risk of infection by viruses and worms and of unauthorized access by hacking tools that are now showing up throughout the world.

### 5.2 Strong point 2: improves safety and reliability of patch management

Even if patch-related information can be obtained, it still might take days or weeks to determine which systems need patching and then test the systems and apply the patches. An OS equipped with non-discretionary access control can prevent substantial damage caused by system penetration or by computers being used as stepping stones, even if an application does have a security hole. This improves the safety and reliability of patch management.

### 5.3 Strong point 3: improves reliability in outsourcing

An OS with enhanced security functions can clearly separate users that manage the system from those that monitor it. The net result is improved reliability in the outsourcing of system management tasks.

### 5.4 Weak point: requires bothersome setting and management of access control policy

The above strong points can only be achieved if the access control policy accurately reflects the security goals of the organizations and systems in question. However, setting a fine-grain access control policy is complicated and troublesome, and preparing and maintaining a correct access control policy requires not only system-related technical knowledge but also an understanding of organizational security policies.

## 6. Is an OS with enhanced security functions perfect?

Like other security technologies, non-discretionary access control cannot provide perfect security on its own. **Table 2** shows the limits of current OSs with enhanced security functions and countermeasures for overcoming those limits. Using an OS with enhanced security functions will not close security holes in applications. A process under attack could still come to a halt and other types of operational problems could still occur. In addition, an OS with enhanced security functions does not provide a means of coping with DoS/DDoS[*1] attacks, nor can it prevent malicious behavior performed within the rights of an application such as third-party relaying of e-mail and cross-site scripting. Finally, if there is a security hole in the kernel itself, the reliability of non-discretionary access control cannot be guaranteed.

## 7. Outlook for the future

In addition to security technology based on boundary defense, NTT Information Sharing Platform Laboratories is also working on end-point security technology. For example, in addition to accumulating techniques for making best use of an OS with

[*1] DoS/DDoS: denial of service, distributed denial of service. These are types of attack that prevent part of an information system from functioning in accordance with its intended purpose. Usually, they involve flooding a system with a huge amount of traffic to prevent it from servicing normal and legitimate requests.

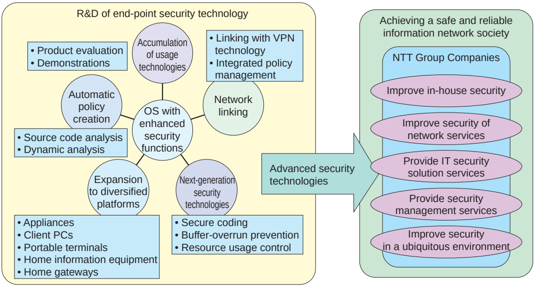
R&D of end-point security technology
• Product evaluation
• Demonstrations
Accumulation of usage technologies
• Linking with VPN technology
• Integrated policy management
Automatic policy creation
OS with enhanced security functions
Network linking
• Source code analysis
• Dynamic analysis
Expansion to diversified platforms
Next-generation security technologies
• Appliances
• Client PCs
• Portable terminals
• Home information equipment
• Home gateways
• Secure coding
• Buffer-overrun prevention
• Resource usage control
Advanced security technologies
Achieving a safe and reliable information network society
NTT Group Companies
Improve in-house security
Improve security of network services
Provide IT security solution services
Provide security management services
Improve security in a ubiquitous environment

Fig. 4. R&D areas of NTT Information Sharing Platform Laboratories.

enhanced security functions, we are also researching and developing techniques for facilitating the use of advanced security functions and techniques for linking such an OS with the network (**Fig. 4**). To make it easier to use advanced security technology, for example, we are researching and developing technology for applying an OS with enhanced security functions to a wide range of platforms and technology for automatically creating access control policies.

In addition, by linking an OS with enhanced security functions with VPN technology, we are researching and developing new access control technology for achieving secure remote-access and remote-management services that divide access authorization among individual users and service providers. This access control technology deals with packets flowing in the network and features a mechanism that assigns each packet an individual security label based on terminal and user corresponding to IPSec or other kinds of authentication. These security labels make it possible to perform non-discretionary access control at end points within the network. Past security technology enabled terminals and users that have been authenticated to use all services and information provided by servers within the network. In contrast, the new access control technology can strictly stipulate what services and information each terminal and user can access and can enforce that policy throughout the network.

The above types of usage and development technologies are expanding throughout the world. They should lead to a safer and more reliable Internet.

**Jumpei Watase**
Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in environmental engineering from Kyoto University, Kyoto in 1994 and 1996, respectively. He joined NTT in 1996. He has been engaged in R&D on IP networking and IP-VPN systems for several years. His current interest is network security and information security management. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

**Yoichi Hirose**
Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. degree in communication engineering from Tohoku University, Sendai, Miyagi in 1996. In 1996, he joined NTT Network Service Systems Laboratories, Tokyo, Japan, where he has been engaged in R&D of IP-VPN systems. He is currently engaged in research on network security. He is a member of IEICE.

**Mitsutaka Itoh**
Leader of Trusted Communication Group, Senior Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in mathematics from Waseda University, Tokyo in 1982 and 1984, respectively. In 1984, he joined NTT Laboratories and engaged in R&D of programming languages, an Ada compiler, object-oriented design, cell phone systems, online-shopping services, ITS systems, IP-VPN service systems, and the resonant communication network. His current interest is network security and trusted communications environment. He is a member of IEICE.