Quarantine Network in the Age of Internal Governance

YASUTOME Yoshio, ADACHI Tomoo, YOSHIDA Takayuki

Abstract

The importance of the quarantine network is being acknowledged more than ever as one of the means of implementing the observance of effective security policies, which is one of the important issues of internal governance. Since multiple quarantine methods already exist, selection of an optimum method is an important factor in system introductions. This paper describes quarantine functions trends, the characteristics of various quarantine methods and issues relevant to the introduction of quarantine systems. It also introduces efforts that are being made by NEC in this field.

Keywords

quarantine network, security policy, security measure, internal governance, quarantine method, NAC, NAP, agent-less method

1. Introduction

Since the enforcement of the Japanese Personal Information Protection Law in April 2005, Japanese enterprises have developed security measures by setting the prevention of information leakage as the keyword. Subsequently the range in which security measures should be applied expanded to the field of internal governance as a result of the enforcement of the Japanese SOX Law in June 2006. Reports regarding detections of traditional viruses and worms have been decreasing, but this does not mean that the damage due to them is decreasing[1]. According to the latest trends, their atrocities, infection capabilities and abuse of security holes have been increasing, and there was even a virus that came to have more than 70 subspecies in a period of only about two months or so after its debut[2].

The traditional measure for network protection has been the installation of a firewall against external attacks. Nevertheless, it has been reported that 25% of the infection routes of the MS Blaster, which is known to have caused serious damage, were Corporate PCs taken out and returned to the office, or non-Corporate PCs carried in by contractors or business partners[3], and the firewalls were powerless against the attacks derived from such PCs. Also, the sources of many of the recent information leakage cases were PCs, and we still, even now constantly hear reports on viruses leading to disclosures of personal information such as the Antinny worm.

In the future, it is expected that protection of networks and information from the threats of viruses and worms from PCs connected via intranet will increase in importance. This paper discusses the quarantine network, which is a countermeasure taken by networks against the threats produced from PCs.

2. The Quarantine Function as a Security Measure

2.1 The Importance of PC Quarantine

(1) Previous Measures

Traditional network security measures have been centered on firewalls and IDSs (Intrusion Detection Systems) for preventing intrusions and attacks from outside networks. However, these measures cannot provide a defense against attacks produced from a PC that has been introduced by a person from inside the intranet. As a result, the countermeasures against threats that cannot be avoided from being introduced in this way remain as an issue to be solved.

(2) PC Configuration Management

The methods most often used to avoid damage caused by threats that are illegally brought into an intranet environment are the method of shutting down an unregistered PC that is detected as being connected and the method of managing the PC configuration and checking its security status. The latter method enables the application of patches to such PCs and their management in accordance with the corporate security policy.

It is very effective for the security to apply patches to all of the in-house PCs and to administer them according to a policy that is in compliance with the in-house rules[4]. At NEC, we began to apply the CAPS (Cyber Attack Protection System) to the entire corporation in order to manage all of the in-house PCs.

However, since the period from the public announcement of a patch to the production of a virus that can attack its security hole has recently been reducing, it has become even more necessary to ensure successive applications of patches.

(3) PC Quarantine

One of the solutions that can overcome the problem of time lag in the application of the latest patch and that can also reduce administration costs is to quarantine the PCs. Quarantine makes it possible to impose a unified security policy inside an organization and to apply a corporate policy, such as by means of the detection of vulnerabilities of PCs, immediate patch applications and improvements in the patch application rate. This is such a strategy that quickly implements the governance of maintaining a uniform security policy observance status throughout the entire corporation.

2.2 Quarantine Network System

The quarantine network system allows the quarantine to be applied efficiently from the network to all of the PCs operating within it.

(1) What Is a Quarantine Network System?

When the quarantine network system is introduced, only those PCs complying with the security policy are allowed to use the backbone network. The PCs that do not comply with the security policy are isolated in a quarantine network that is configured separately from the backbone network as a countermeasure in support of the security policy.

(2) The Four Elements of the Quarantine Function

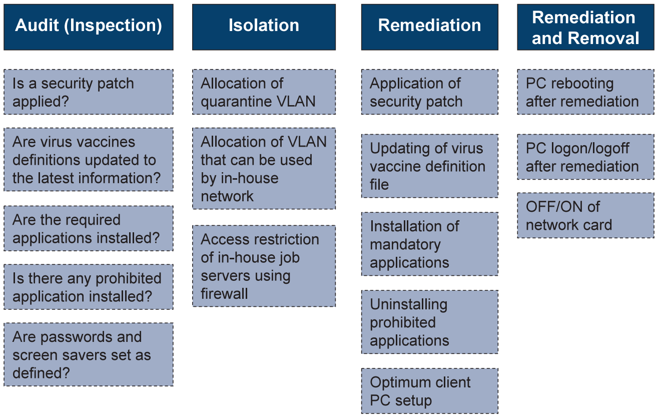
The quarantine network system is composed of the four elements of inspection (auditing), isolation, remediation and removal. **Fig. 1** summarizes each element.

1) Inspection (Auditing)

This procedure consists of checking the status of observance of the PC security policy. In general, this is done by installing agent software for the quarantine function in the PC and sending the check results to the quarantine policy server. There is also the agent-less method that does not require installation of agent software in advance and which can therefore execute quarantine on the PCs of users who cannot be forced to utilize an agent.

2) Isolation

This function consists of isolating the PCs that are judged not to comply with the security policy in the quarantine network. Isolation is available by using several quarantine methods depending on the characteristics of the devices linked with the quarantine network system.



Audit (Inspection)	Isolation	Remediation	Remediation and Removal
Is a security patch applied?	Allocation of quarantine VLAN	Application of security patch	PC rebooting after remediation
Are virus vaccines definitions updated to the latest information?	Allocation of VLAN that can be used by in-house network	Updating of virus vaccine definition file	PC logon/logoff after remediation
Are the required applications installed?	Access restriction of in-house job servers using firewall	Installation of mandatory applications	OFF/ON of network card
Is there any prohibited application installed?		Uninstalling prohibited applications	
Are passwords and screen savers set as defined?		Optimum client PC setup	

Fig. 1 Elements of the quarantine network system.

3) Remediation

This consists of enabling isolated PCs to comply with the security policy. The operations are either automated or manual and include the application of a security patch, updating of the virus vaccine definition file and uninstalling inhibited software such as Winny. To perform remediation in compliance with the security policy, the quarantine network system is linked to patch distribution and virus countermeasure utilities.

4) Remediation and Removal

This procedure consists of connecting PCs to the backbone network after the causes of their isolation have been remedied. It is sometimes included in 1) Inspection, but we would like to handle it as an independent element because the ease of removal and return to the backbone network exerts an important effect on quarantine operability.

(3) Quarantine Methods

In this section, we classified the representative quarantine methods into five different methods. **Fig. 2** shows the configuration of a quarantine network including the isolation points. The following description deals mainly with the flow of isolation and removal from the quarantine network of each method.

1) Authentication VLAN Method

This method uses a VLAN-compatible network switch and separates the quarantine network and backbone network by means of segmentation using VLAN. When a PC is identified as complying with policy auditing at IEEE802.1X authentication or DHCP authentication timing at the moment of

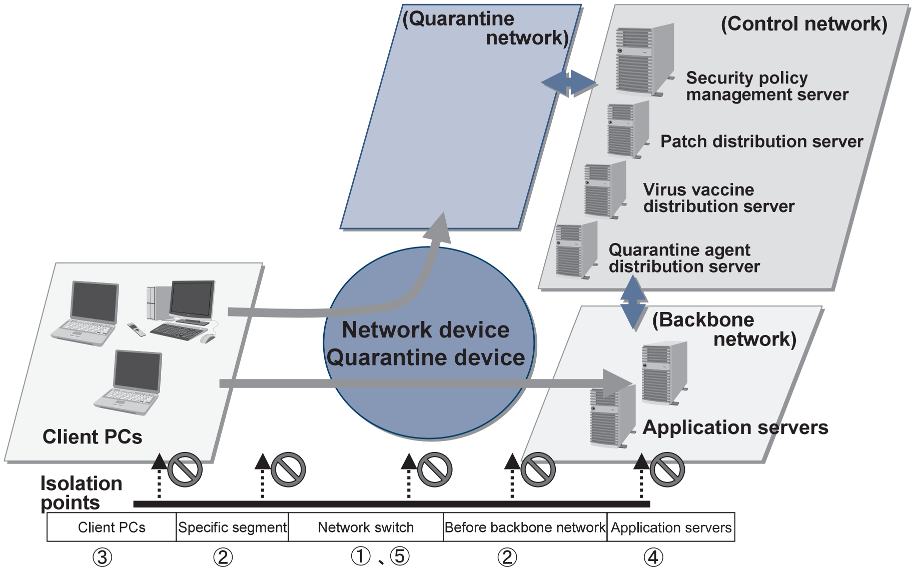


Fig. 2 Configuration of the quarantine network.

network connection, the VLAN for the backbone network is assigned to the PC. If it is found not to be compliant, the VLAN for the quarantine network is assigned to the PC. A PC that is isolated in this way is subjected to remediation and then re-audited. The compliance information obtained as a result of re-auditing is sent to the policy management server, and a VLAN of the backbone network is allocated to the PC at the time of the re-authentication. The issue in this operation is by how much the number of user operations required between re-auditing and re-authentication can be reduced.

2) Gateway (GW) Type Firewall Method

This method isolates the PC from the backbone network at the GW between them. Quarantine of a specific segment is also possible depending on the location of the GW. As the control utilizes the filtering operation of the GW including a firewall, this method is suitable for an environment based on fixed IP addresses. The PC isolated in this way is subjected to remediation and then re-audited. The isolation is canceled at the moment of re-auditing, so no user operation is required for its removal from the quarantine.

3) Client Firewall Method

This method forces the connection of the PC to the quarantine network by means of the filtering control of the client firewall installed in the PC. It does not require user operation for removal either, because it is also based on the control of the filtering operation of the firewall. However, as the method cannot control the PC unless agent software such as client software is installed, thorough management of the PC application configuration is necessary when it is used.

4) Server Firewall Method

This method introduces a dedicated firewall server on the application server so that the application server performs the filtering control. It does not require user operation for removal because it is also based on the firewall filtering control. With this method, only those PCs that are found to be compliant by auditing are permitted to connect to the application server. As this method permits the PC to access networks other than the application server, it is suitable for use in protecting specific servers.

5) Remote Access Method

Control of this method utilizes a switch that operates by remote access from outside to inside the enterprise. This method forces connection to the quarantine network by linking the remote access control with auditing. Unlike other methods, it uses different policies for access from inside to that from outside of the enterprise. As a result, it may sometimes be required to prepare different isolation locations for the two types of access. In this case, different management methods are also required for quarantine judgments.

(4) Effects of the Introduction of a Quarantine Network

The following problems may be solved by the introduction of the quarantine network system by administration departments.

• Since a newly introduced PC is isolated in the quarantine network, the spreading of a worm can be prevented even when a newly introduced PC is infected by a worm (risk reduction).

- Since a PC that does not observe the security policy is isolated, a source of disturbance of the intranet such as the infection of vulnerable PCs by worms can be prevented (risk reduction).
- Since isolation in the quarantine network is automatic and the number of PCs at risk can be counted, the labor required for management can be reduced (operation cost reduction).
- Since the isolation is compulsory, observance of security policy can be enforced throughout the entire enterprise (governance enhancement).

The effects of quarantine networks on the users are as follows.

- The risk involved in allocating responsibility for causing a problem by accidentally introducing a hazardous PC into the intranet can be reduced.
- The PC can always be connected to the intranet at the latest security level so that users can concentrate on their work without being concerned about the security.

In this way, the quarantine network can improve the security of both the administration department and the users and maintain an overall security level for the entire network.

2.3 New Trends Related to Quarantine

The quarantine network system has been attracting attention since the latter half of 2003. Major vendors including Cisco Systems and Microsoft have become active in proposals and alliances aimed at the implementation of the quarantine function and steady market growth is anticipated[5)].

2.4 Trends in Standardization

Three methods are proposed as standard specifications for the security policy management server and isolation devices (network switch, etc.) that comprise the key to the implementation of the quarantine network.

(1) NAC (Network Admission Control)

This is the concept of the self-defending network proposed by Cisco Systems. When a PC is inspected and is not found to be compliant, access to a PC is restricted by a network device. Securing the security of terminals connected to a network using existing network devices is a security solution based on an industrial alliance under the leadership of Cisco Systems. It comprises three control methods that include; a network control at layer 3 (network layer) (NAC L3-IP method), a control at layer 2 (data link layer) (NAC L2-IP method) and another control that includes the IEEE802.1X authentication (NAC L2-802.1X method). These methods have a potential for wide dissemination based on Cisco routers[6)].

(2) NAP (Network Access Protection)

This refers to the policy enforcement platform built into the Windows “Longhorn” server that is to be the OS for the next-generation servers from Microsoft. NAP is used to set the updating policies for the operating system and virus measures, and the network access of each PC is inhibited until it is certified that the PC is policy compliant. This method also has the potential of wide dissemination because it is to be used as standard in the proposed Windows server environments[7)].

(3) TNC (Trusted Network Connect)

This is an open security standard of the Trusted Computing Group (TCG), which is an industrial organization established for the development and dissemination of standards and specifications contributing to the implementation of safe computer platforms. While NAC and NAP are standards under the leadership of vendors, the strong point of the TNC standard is that it is an open standard. The specifications are open to any third parties so that they can implement quarantine mechanisms with freedom from being bound to any specified product. Therefore, this standard is expected to be support by a large number of communication device and PC security vendors[8)].

3. Issues Concerning the Introduction of the Quarantine Network

A quarantine network system with an appropriate balance between convenience and security can be built by considering relationships between the quarantine method and existing networks at the time of introduction of the quarantine network. The following sections discuss the issues concerning the introduction by also taking cost efficiency into consideration.

3.1 Protection Targets

Every quarantine method uses different means and points of isolation to other methods. This makes it necessary to clarify in advance the range that is to be protected by the quarantine network. The items to be clarified include “if it is required to protect only specific servers,” “if it is required to protect specified networks such as a data center” or “if it is required to protect the entire intranet.”

Since, unlike the backbone network the quarantine network may be exposed to intrusion by viruses and worms, an analysis of the risks and an assessment of countermeasures against intrusions is necessary. In this regard the selection of the quarantine method and utilities, it is also useful to define the range of the required protection and whether it is to be limited "only to the PCs" or "only to the segment connected by users."

3.2 Method of Isolation

After clarifying the range to be protected, start examination of the isolation target. Also examine whether the isolation method will use the authentication VLAN or access control by filtering. The next issue is the design of the quarantine network, e.g., by considering the balance between the operational cost and the safety level when choosing the patch distribution servers for use in the remedial work. Accordingly, it is necessary to select whether "a patch distribution server should be located in each segment of the policy management server" or if "separate servers should be installed in the quarantine and backbone networks."

3.3 Partial Introduction and Step-by-Step Introduction

The quarantine network can be introduced only in a specific network, such as in an office where the potential of carrying in a PC from the outside is high or for a sales department where mobile PCs are used as standard PCs. This can be a realistic solution that can reduce both the introduction cost and the risk. If such an introduction is adopted, it is important to select products that can comply with a variety of quarantine methods by considering future extensions. The operational cost can be reduced by using a quarantine method that matches each network and by applying integrated management of the quarantine methods.

In this case, matching of the existing networks needs full consideration. For example, when it is planned to link a quarantine network with network authentication based on the authentication VLAN method, the cost would be increased if VLAN compatible devices are not already in use because these will need to be purchased. However, the cost can be reduced relatively if the authentication network has already been introduced for wireless LAN, etc.

3.4 Administration

Even after the quarantine network system is introduced, it is not practical to use an operational method such as one that isolates all of the PCs simultaneously every morning. Since isolation leads to work stoppages for the user, it is necessary to design a mechanism and operational system that can optimally control; convenience, execution of jobs, methods of dealing with inquiries, concentration of server loads accompanying applications of patches and policies, and network loads. For example, in the case of the application of patches, it is required that "users who connect to the network everyday and apply patches optimally should be allowed to execute their jobs without being isolated." It is also required that periodical auditing of permanently running PCs and the isolation of PCs that have been taken outside for a long period are executed automatically. Selection of the policy management products is critical for an operational design that will not deteriorate user convenience.

4. The Quarantine Solutions of NEC

At NEC, we have been providing quarantine products (CapsSuite Quarantine Options) since August 2004. Since that time, variations in the quarantine methods have expanded so that our products now cover almost all of the major quarantine methods. We have also conducted a large-scale in-house demonstration experiment using the VLAN authentication method and have confirmed the effects of the quarantine network and the issues that are involved in its actual operation. With regard to the issues described above, we have examined them from the aspects both of function and operation and have used the feed back results of the demonstration experiments in the design of the "CapsSuite PC Quarantine System" which was released as a product to the market in September 2006.

5. Conclusion

In the above, we have described the mechanisms of the quarantine network, its technical trends and the efforts concerning it that are being applied at NEC. From fiscal 2007 we will also be studying a step-by-step introduction of an in-house quarantine network. Believing that the quarantine network is advantageous for both administrator and user and that it is capable of maintaining secure networks, we are planning to release advanced quarantine solutions in the market as some of the prominent utilities of the InfoCage Network series. These introductions will constitute an important part of the Cooperative Security system being proposed by NEC.

*The corporate and product names mentioned in this paper are trademarks or registered trademarks of their respective owners.

References

1) "KIGYO NI OKERU JOHO SEKYURITI JISHO HIGAI-GAKU CHOSA (Survey of Information Security Damages in Private Enterprises)" and "KOKUNAI NI OKERU KONPYUUTA UIRUSU HIGAI JOKYO CHOSA (Survey of Computer Virus Damages in Japan)," 2005, Information-Technology Promotion Agency, Japan (IPA).
http://www.ipa.go.jp/security/fy17/reports/virus-survey/index.html
2) "KONPYUUTA UIRUSU/FUSEI AKUSESU NO TODOKEDE JYOKYO [11-GATSU-BUN] NI TSUITE (Status of Computer Viruses and Illegal Access Reported [November 2006])," Information-Technology Promotion Agency, Japan (IPA).
http://www.ipa.go.jp/security/txt/2006/12outline.html
3) "W32/MSBlaster OYOBI W32/Welchi UIRUSU HIGAI NI KANSURU KIGYO ANKEETO CHOSA NO KEKKA NI TSUITE (Result of Enterprise Survey on Virus Damage)," IT Security Center, Information-Technology Promotion Agency, Japan (IPA/ISEC).
http://www.meti.go.jp/policy/netsecurity/Blaster_Survey.pdf
4) Okazaki, H.: "JOHO SEKYURUTI GIJUTSU TAIZEN (The Complete Information Security Technology)," 2002, Nikkei Business Publications, Inc.
5) "2006 NETTOWAAKU SEKYURITI BIJINESU CHOSA SORAN," p.214, 2006, Fuji Chimera Research Institute, Inc.
6) "Network Admission Control," Cisco Systems, Inc.
http://www.cisco.com/japanese/warp/public/3/jp/solution/netsol/security/nac/index.shtml
7) "Windows 2003 Server NETTOWAAKU AKUSESU HOGO (Windows 2003 Server Network Access Protection)"
http://www.microsoft.com/japan/windowsserver2003/technologies/networking/nap/default.mspx
8) Trusted Computing Group
https://www.trustedcomputinggroup.org/groups/network/

Authors' Profiles

YASUTOME Yoshio
Staff,
First System Software Division,
Systems Software Operations Unit,
NEC Corporation

ADACHI Tomoo
Engineering Manager,
First System Software Division,
Systems Software Operations Unit,
NEC Corporation

YOSHIDA Takayuki
Engineering Manager,
First System Software Division,
Systems Software Operations Unit,
NEC Corporation