Quarantine Network with Secure Enterprise Network Access Control System

Yoshitake Tajima[†], *Shuichi Karasawa, Kenji Ota, Yutaka Watanabe, and Sotetsu Iwamura*

Abstract

We have developed a quarantine network that protects computers from viruses and worms at the network level based on our secure enterprise network access control system (SENACSY). The basic functions of SENACSY that improve the usability and security of network access by personal computers were introduced in the March issue. This article describes SENACSY's quarantine network, which is easy to introduce into the existing networks of an enterprise and easy for network users to use and for network administrators to manage.

1. Enterprise networks and network security incidents

From the viewpoint of security measures for enterprise networks, anti-virus and anti-worm methods have been becoming more and more important in recent years. One report says that more than 40% of listed companies suffered from computer viruses and worms more than three times in fiscal year 2003. In particular, the Blaster worm caused serious damage to 30% of affected networks, which were forced to stop computer system or business operations [1]. New computer viruses and worms targeting new security holes emerge every day, and they spread rapidly in enterprise networks when an infected computer is connected to them. Therefore, a computer should be updated with the latest version of anti-virus and anti-worm software *before* being connected to the network. However, it is common practice for people to update their computers over the network *after* connecting them to the network. A quarantine network may be the best solution to this problem. This article describes a quarantine network we have developed.

2. Requirements for anti-virus and anti-worm measures in an enterprise network

When personal computers (PCs) are connected to an enterprise network, the measures against viruses and worms must meet three requirements, as shown in **Fig. 1**.

1. Strict enforcement of security measures for PCs
2. Protection of enterprise network (servers and PCs)
3. Protection of vulnerable PCs

Security measures for PCs are indispensable to protect against threats from direct attacks causing file crashes and data leakage. However, in the case of PCs that are not connected to the network all the time (for example, ones used for remote access or used infrequently in the office), the basic security measures tend to be applied late. Therefore, it is important to manage those PCs efficiently and enforce the security policy of the enterprise network including the version of the virus definitions and the status of applied operating system (OS) patches.

Another requirement is to protect an enterprise network against PCs that do not comply with the policy (hereinafter called non-compliant PCs). A non-compliant PC needs to be connected to a network to get update files, but it could allow the network to be attacked before it finishes updating if it is infected with a computer virus. Moreover, because a non-

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

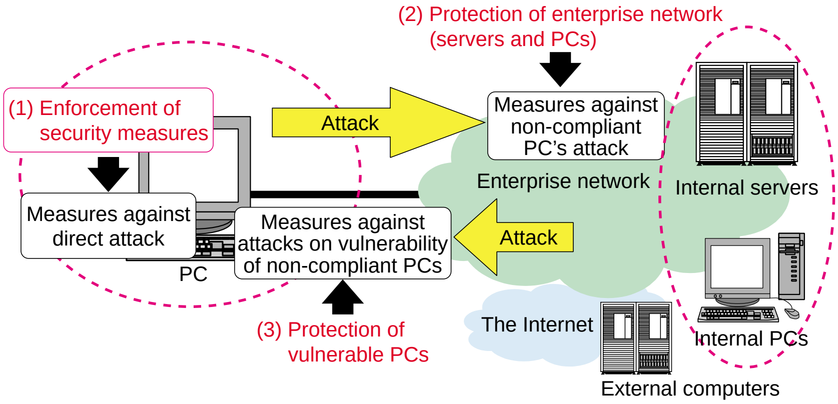


Fig. 1. Requirements for anti-virus and anti-worm measures in an enterprise network.

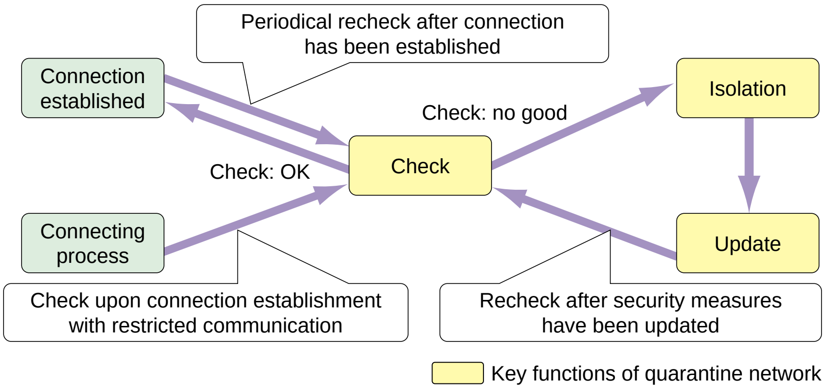

Periodical recheck after connection
has been established
Connection
established
Check: no good
Isolation
Check: OK
Check
Connecting
process
Update
Check upon connection establishment
with restricted communication
Recheck after security measures
have been updated
Key functions of quarantine network

Fig. 2. Functions of quarantine network.

compliant PC has a potential vulnerability, protection of non-compliant PCs is also required to avoid the risk of attack and infection by viruses or worms from the Internet and enterprise networks.

3. Quarantine networks

To meet the above requirements, a quarantine network has functions for checking, isolating, and updating while a PC is making a network connection, and it provides policy enforcement and protection of both enterprise network and non-compliant PCs, as shown in **Fig. 2**.

The checking function inspects the PC's security measures and compares them with the quarantine policy set in a quarantine policy server and updated frequently. In addition to a check upon connection to the network, periodical checks are performed while the PC is connected to the network. The isolation function restricts communication of a non-compliant PC to protect both the enterprise network and the non-compliant PC. The update function updates security measures to the latest version to comply with the quarantine policy and to get the isolation ended. The update files are usually provided by update servers on an enterprise network or on the Internet.

To provide those functions, network equipment makers and software makers have developed several quarantine network systems, which utilize personal firewalls, authenticating switches, or a dynamic host configuration protocol (DHCP) server. But no system has been accepted as a *de facto* standard yet [2].

4. Goal of SENACSY quarantine

NTT Information Sharing Platform Laboratories has developed a secure enterprise network access control system (SENACSY), which provides high usability and security for enterprise network access [3], [4]. As an optional function, we have developed a quarantine function. The SENACSY quarantine function based on a SENACSY tool installed on a user's PC is intended to provide total network security management. It is easy to introduce into the existing networks of an enterprise and easy for network users to use and for network administrators to manage. It checks that the following conditions of the user's PC comply with the enterprise policy and permits the PC to connect only if it complies. It checks:

- Whether particular anti-virus software is running
- The date or version of the virus definition files of the anti-virus software
- Whether particular OS patches have been applied.

5. Components and features of SENACSY quarantine function

SENACSY consists of a profile generating system, a SENACSY tool, and an authentication token for personal identification. When a user connects a PC to the network using a SENACSY tool, he/she inserts the authentication token in the PC and imports configuration data called a "profile" that is issued by a network administrator [4].

The SENACSY quarantine function comprises a quarantine policy server and a personal firewall (PFW) installed on the user's PC in addition to the basic components shown in **Fig. 3**. It is assumed that the existing anti-virus software and servers for updating virus definition files and OS patches are still used.

In the SENACSY quarantine network, the checking function is provided by the combination of the SENACSY tool, PFW, and the quarantine policy server. Isolation and updating functions are provided by the SENACSY tool, which controls the PFW and changes its filtering rules to permit communication with only specific servers.

As shown in **Fig. 4**, the SENACSY quarantine function is implemented using the information of a

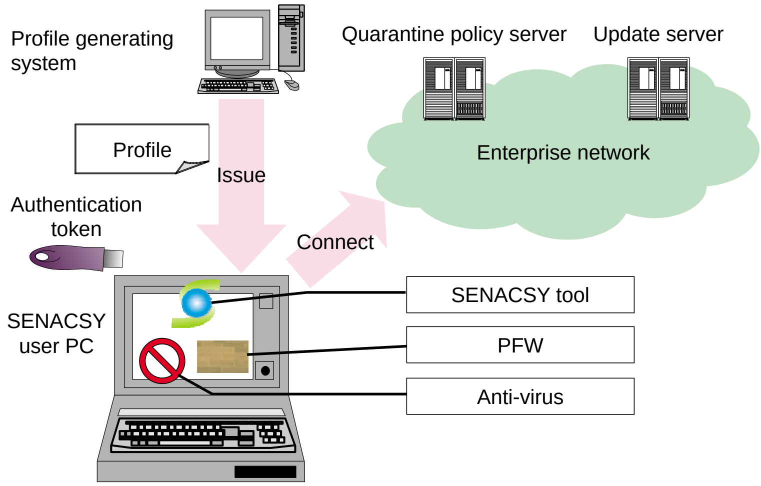


Fig. 3. SENACSY quarantine network.

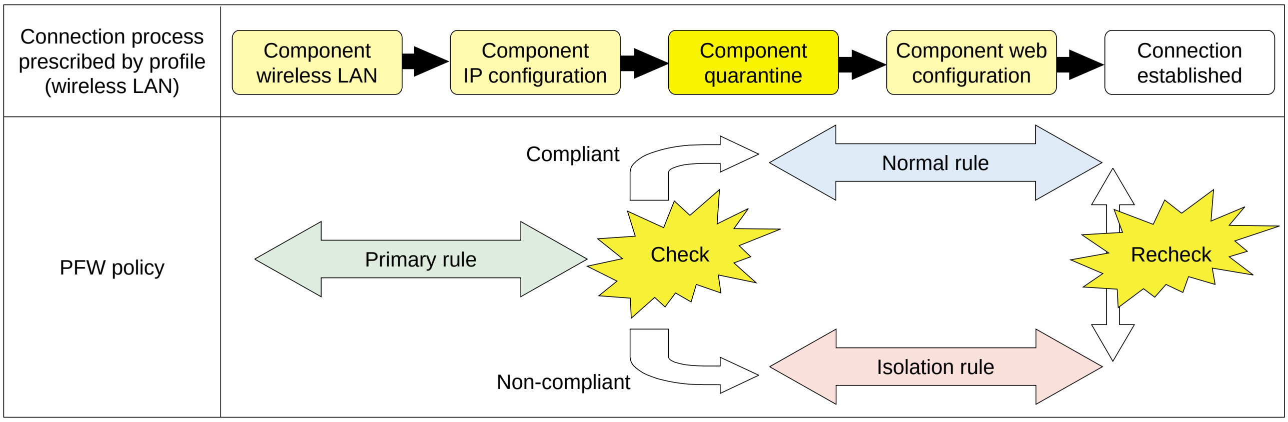


Fig. 4. Connection process of SENACSY.

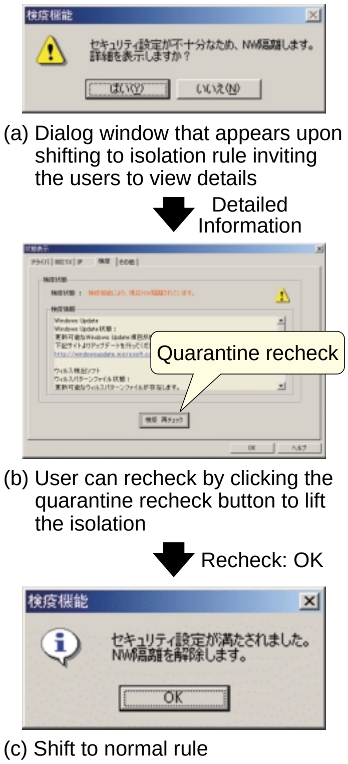
profile called the quarantine profile component that prescribes the behavior of the SENACSY tool and PFW during quarantine. It is automatically executed in the connection process sequence performed by the SENACSY tool. The quarantine profile component includes the IP (Internet protocol) address of the quarantine server and the PFW filtering rules selected according to the checking results. The PFW policy includes a primary rule, an isolation rule, and a normal rule, which are applied by the SENACSY tool.

The primary rule usually permits communication with the quarantine policy server. Though the detailed parameters of communication that should be permitted by an isolation rule depend on the network system structure and security policy, communication for the purpose of updating the security measures should be permitted. The isolation rule restricts communication with the enterprise network, but permits communication for the purpose of updating. The normal rule usually permits all communication with the network.

When a user operates the SENACSY tool to connect to an enterprise network, the user's PC is initially isolated by the PFW's primary rule, and the connection sequence is automatically executed. Then, at the stage when the PC becomes able to access the quarantine server via its IP address, the quarantine check is performed. If the PC complies with the quarantine policy, its PFW operates under the normal rule; on the other hand, if it does not, the PFW operates under an isolation rule. The PC's screen displays the popup window shown in **Fig. 5(a)**, which informs the user that the PC has been put into isolation status. In that status, the PC's communication with the network is restricted, so computers on the network are protected against possible attacks from the non-compliant PC, and at the same time the non-compliant PC is protected against possible attacks from outside and can safely update its security measures.

After the security measures have been updated, the user can confirm whether his/her PC complies with the policy by clicking the "Quarantine recheck" button shown in **Fig. 5(b)**. As it now complies, the popup shown in **Fig. 5(c)** informs the user that the isolation has been lifted and the PC may fully communicate with computers on the network under the normal rule.

As described above, the SENACSY quarantine function enables users to check the PC during the sequence of the automatic connecting process by a single click and enables the network administrator to enforce the security policy strictly. In addition, as the isolation is implemented with the PFW, the quarantine function can be introduced into the network without changing the existing network configuration, whereas the system using authenticating switches or a DHCP server requires network reconfiguration. Moreover, if application-specific access restrictions are required, the SENACSY quarantine function can configure the rules of transport layer filtering for the PFW policy for each connecting sequence and achieve fine-grained policy-based control.



セキュリティ設定が不十分なため、NW隔離します。
詳細を表示しますか？

(a) Dialog window that appears upon shifting to isolation rule inviting the users to view details

(b) User can recheck by clicking the quarantine recheck button to lift the isolation

セキュリティ設定が満たされました。
NW隔離を解除します。

(c) Shift to normal rule

Fig. 5. Dialog windows of SENACSY tool.

6. Operation of quarantine network

Though actual operation of the SENACSY quarantine will vary depending on the system and method for updating security measures, the quarantine system can be flexibly integrated into existing systems and methods. In this article, we describe the operation of a simple quarantine network in which updating is done by the internal update server, as shown in **Fig. 6**.

If the virus definition updating and OS patch deployment are done by downloading from the internal update servers, the communication identified with the servers' address and appropriate port numbers must be permitted under the isolation rule.

If the PC is non-compliant, the isolation rule will be

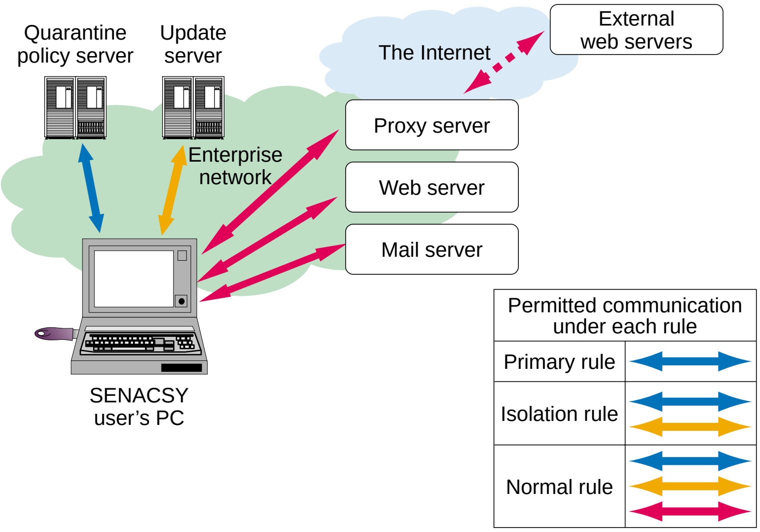


Fig. 6. Example PFW policy in operating SENACSY quarantine.

applied to the PFW, and communication with other computers except the internal update servers and the quarantine policy server will be forbidden. When the user has finished updating the PC's security measures, he/she asks the SENACSY tool to recheck access to the quarantine policy server to see whether the PC complies with the policy. If it does, the tool applies the normal rule to the PFW and lets the PC communicate with all the computers on the enterprise network. Note that the update server must always use the latest update because it is exposed to access from non-compliant PCs.

The whole quarantine system and policy are compatible with the existing system as explained above, and adaptation of the isolation rule can make it work if update servers on the Internet are used or if a proxy server is used for Internet access. Moreover, more detailed rules can be added to the communication policy. This will enable a network administrator to enforce the policy that restricts access to servers unrelated to each user's work.

7. Introduction example

We introduced a SENACSY quarantine system to the network of our laboratory, NTT Information Sharing Platform Laboratories, in August 2005 and have been managing remote-access PCs. The system contributes to network security management, which was difficult before. For example, people who took a summer vacation could safely update and connect their PCs to the network after a period of disconnection and no updating. In addition, we are ready to utilize our accumulated know-how about introducing and operating the SENACSY quarantine network to provide SENACSY quarantine to customers.

8. Future work

In future, we are planning to develop a function for interacting with integrated user management systems to improve manageability further and a management function for achieving a wider variety of security policies on the application level.

References

[1] "Survey of Information Security," Ministry of Internal Affairs and Communications, 2004 (in Japanese).

[2] M. Oonishi, "Technique of Quarantine LAN System," IEICE Technical Report, NS2005-79, Sep. 2005 (in Japanese).

[3] Y. Kagei, K. Nakagawa, T. Tachi, M. Takeda, and T. Nakagawa, "Cyber Security Project," NTT Technical Journal, Vol. 17, No. 3, pp. 14-19, 2005 (in Japanese).

[4] T. Kaji, T. Yamashita, S. Matsumoto, M. Kobayashi, and M. Nakajima, "Secure Enterprise Network Access Control System—Overview," NTT Technical Review, Vol. 4, No. 3, pp. 71-76, 2006.

Yoshitake Tajima

Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E degree in electronic engineering and the M.E. degree in information and communication engineering from the University of Tokyo, Tokyo in 1997 and 1999, respectively. He joined NTT Information Sharing Platform Laboratories in 1999. He currently engaged in R&D of network security. He is a member of IEEE, the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan, and the Information Processing Society of Japan (IPSJ).

Shuichi Karasawa

Senior Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in physics and the M.E. degree in electrical engineering from Keio University, Kanagawa in 1990 and 1992, respectively. He joined NTT Telecommunication Networks Laboratories in 1992. He is a member of IEICE and the Operations Research Society of Japan.

Kenji Ota

Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in mathematics from Keio University, Kanagawa in 1989 and 1991, respectively. In 1991, he joined NTT Software Laboratories, where he engaged in R&D related to requirement engineering. He has engaged in R&D concerning software engineering and network operations. He is a member of IPSJ.

Yutaka Watanabe

Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E. degree in electronics and the M.E. degree in electrical engineering from Ibaraki University, Ibaraki in 1988 and 1990, respectively. In 1990, he joined NTT Transmission Systems Laboratories in Yokosuka. He is a member of IEICE.

Sotetsu Iwamura

Senior Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S., M.S., and Ph.D. degrees in electronics engineering from the University of Tokyo, Tokyo in 1989, 1991, and 1994, respectively. In 1994, he joined NTT Telecommunication Networks Laboratories in Musashino. He is a member of IPSJ.