§56. Establishment of an Environment for Remote Participation and Control on QUEST Experiments

Hasegawa, M., Nakamura, K., Higashijima, A. (RIAM, Kyushu Univ.), Takase, Y., Ono, Y. (Graduate School of Frontier Sci., Tokyo Univ.), Nishino, N. (Graduate School of Eng., Hiroshima Univ.), Nagayama, Y., Nakanishi, H., Emoto, M., Yamamoto, T., Kojima, M., Ohsuna, M.

On the recent high temperature plasma confinement experiments aiming to fusion energy, many collaborators from within and without are involved against one experimental device. Under such circumstances the requests to participate experiments from remote sites are growing rapidly. The QUEST (Q-shu University Experiment with Steady State Spherical Tokamak) planned by bidirectional collaboration between Kyushu University and NIFS (National Institute for Fusion Science) is a spherical tokamak, and these requests are also growing against the QUEST. The QUEST project is based on the cooperation of many researchers and their cooperation are indispensable to make this project successful. Because of this, the establishment of an environment for remote participation and control on QUEST experiments is an indispensable issue. To establish an environment for remote participation and control, the implementation of the sharing and manipulating of information such as numerical data and control parameters are one of the key issues. However, this means the permissions against the access from external network into the internal Local Area Network (LAN). To permit this, the establishment of the secure network such as the protection against the unauthorized access and the information leaks is indispensable. Here, we describe our approach to establish the secure network.

Network threats should assume to come from internal LAN in addition to external LAN via such as spam mail and easy use of USB memory. In general, internal LANs are constructed with more open policies. Because of this, network threats from internal LAN can sometimes be more serious than ones from external LAN. To remove these threats, anti-virus software installation and applications of new release patches to every terminal are primarily required as we all know. Besides this, internal LAN on QUEST is divided into Experimental (Exp.) LAN and Control (Ctrl.) LAN to separate security policies definitely (Fig. 1). This can also expect the advantageous effect to improve Ctrl. LAN's network quality that should make absolute communications between control terminals without inhibitions by experimental numerical data communications. The Exp. LAN is connected to the SNET which is a nationwide academic Internet backbone to provide a high-speed communication environment. The communications between Exp. LAN and SNET are restricted by Firewall administrated by LHD LABCOM group. The only communications that strictly conform to the security policy of SNET are permitted. The Exp. LAN is also connected to the external LAN (office LAN). We install the CentOS based PC rooter between these LANs to construct secure network. The CentOS is one of Linux distributions. We also install the function of Firewall on this PC rooter by configuring "iptables" to block unwanted communications from external LAN. This function is carefully configured to have operations flexibility according to group consensual security policy. (Depending on circumstances, the registration of all the terminals on Exp. LAN may be required. In that case, the communication from unregistered terminal to external LAN should be blocked at the PC rooter.) Although a Firewall block unwanted communications according to prepared rules such as privileged IP addresses and ports, this doesn't monitor whether the communications are vicious or not. (Ex. Usually, the communications with 80/tcp port are not blocked at the Firewall for http browsing. The vicious communications sometimes abuse this port.) Because of this, we install "snort" on PC rooter to complement functions of the Firewall. The "snort" is an open source network intrusion prevention and detection system (IDS/IPS) with the benefits of signature, protocol and anomaly based inspection. With this, we can detect improper attempts for intrusions from external LAN, and can also detect a terminal of Exp. LAN that transmits suspicious signals.

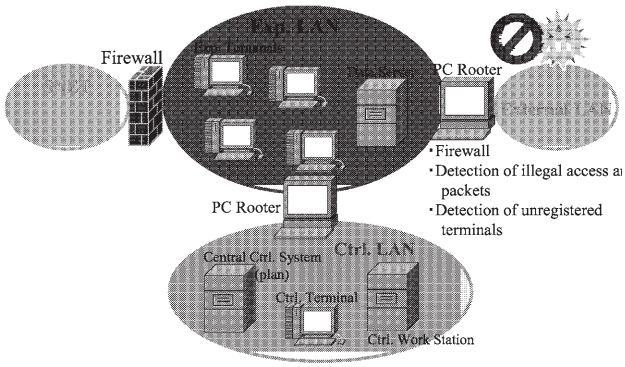

Fig. 1. Configuration of QUEST LANs

In the case that the "snort" detects some security problem at one terminal in internal network, a network administrator has to disconnect an aforementioned terminal from LAN promptly. For this reason, the network administrator is considered desirable to grasp the owners and the installation locations of all the terminals. Moreover, the mechanism that can detect an unknown terminal is also required. As a result, we installed "arpwatch" to monitor whether an unknown terminal is connected or not. This software can detect and record the combination of an IP address and a Mac address by Address Resolution Protocol (ARP), and send E-mail as an alarm to the network administrator when an unknown terminal is connected.

As mentioned above, we are trying to make our network secure by the segmentalization of internal network and the linkage of functions such as "iptables", "snort", and "arpwatch". Even though these coping processes may be insufficient, we think that the buildup of the actual performance is important at first, and we have to make continuous efforts to keep our network security. In the future, we develop remote participation and control schemes on QUEST experiment in more concrete form, based on this established secure network.