NETWORK SECURITY SYSTEM AND METHOD FOR RIBF CONTROL SYSTEM

A. Uchiyama#, R. Koyama, SHI Accelerator Service Ltd., Shinagawa, Tokyo, Japan
M. Komiyama, M. Fujimaki, N. Fukunishi, RIKEN Nishina Center, Wako, Saitama, Japan

Abstract

A closed network is more reliable for accelerator control from the viewpoint of information security. The control system of RIKEN RI Beam Factory (RIBF) based on EPICS is also constructed on a closed network that is completely disconnected from all the other networks including laboratory intranets used for daily research activities. However, there are several inconveniences in exchanging information between the network of RIBF control and others. To solve the conflicts, we designed and implemented the network security system. This proceeding describes the design policy of the system and the method used for the exchange information between the intranet in RIKEN and the closed network used for RIBF control system.

INTRODUCTION

The control system of RIKEN RIBF adopted the EPICS (Experimental Physics and Industrial Control System) that used LAN-based protocols [1] and was constructed on its own network (ACC-LAN). E-mail services and Internet accesses unrelated to accelerator operations utilize the RIKEN virtual LAN (RIKEN-VLAN) which is a major network system in RIKEN Wako campus. In the RIKEN-VLAN, Wireless Fidelity (Wi-Fi) routers have been installed in all of the buildings, and all visitors including beam users can access the Internet using the Wi-Fi with DHCP services in RIKEN.

ACC-LAN, however, should not be connected directly to the RIKEN-VLAN because there are possibilities of illegal accesses of intruders to ACC-LAN via Wi-Fi services of the RIKEN-VLAN, even if illegal accesses from wide area network (WAN) is denied with a firewall.

Although the use of the network disconnected from RIKEN-VLAN and WAN is effective for network security of RIBF control system, there were several inconveniences. In this network system, it is difficult for members of the accelerator group to monitor the status of accelerator operation in real time from their offices because access ports of ACC-LAN are not prepared for the offices of the members. The members were hence required to use a storage device, such as USB flash memory, to extract logged data of accelerator operation from ACC-LAN. It was also impossible to transfer E-mail alerts, which are widely used for server management. In addition, RIBF beam users frequently request wide varieties of information, such as accelerator operation status. For these reasons, we decided to improve the inconvenient situation without risking information security.

NETWORK ARCHITECTURE

The ACC-LAN consists of Ethernet switches, optical fibres and metal cables, which are all commercially available. The control system comprises two different systems: an accelerator control system based on EPICS and the other is a system for non-EPICS-based utility control (see Fig. 1). The controllers, servers, and client PCs are installed on the EPICS-based network system. On the other hand, some digital measurement instruments, video servers, and network cameras are connected to the network for non-EPICS-based utility control.

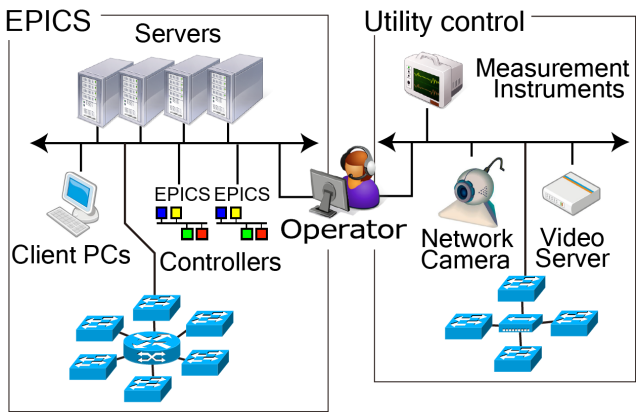

Figure 1: Outline of the ACC-LAN.

PROTECTION AGAINST MALWARE

Nowadays, spread of malware, such as warm, becomes one of the serious issues on the Internet. For example, according to Adobe.com report, systems using Microsoft Windows, Macintosh, Linux and Solaris are possibly infected by malware due to critical vulnerability in old versions of Adobe Flash Player, Reader and Acrobat [2]. Usually the accelerator operation does not require Internet connections and E-mail services. Since major parts of malware infections are caused by Web browsers and E-mails, communications to the Internet or RIKEN-VLAN from client PCs used in accelerator operation are strictly prohibited.

#a-uchi@riken.jp

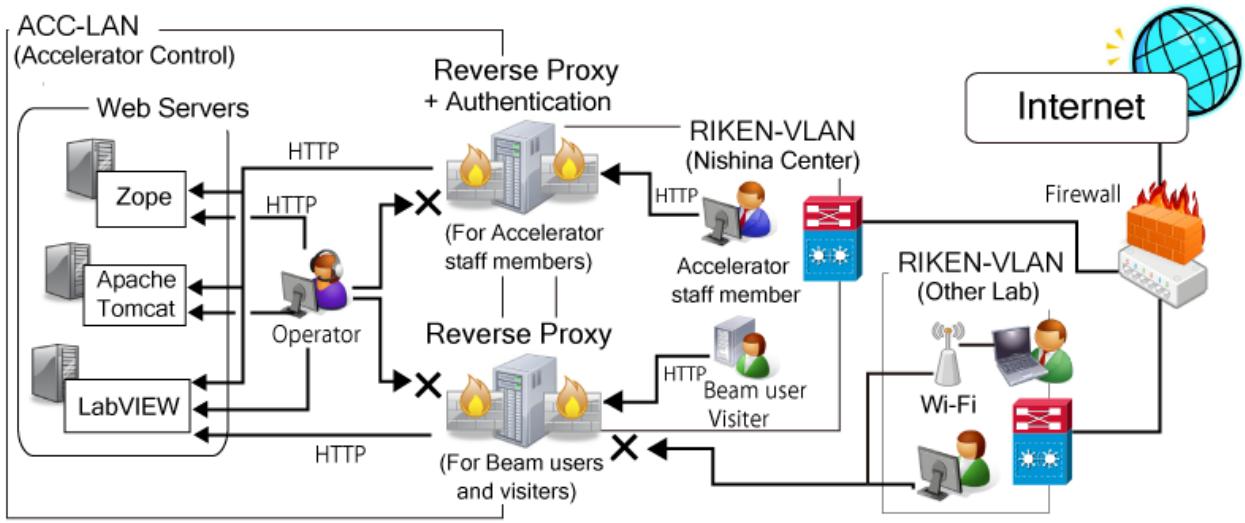

Figure 2: Network diagram in the web communication using reverse proxy servers between ACC-LAN used for RIBF control system and RIKEN-VLAN for office network.

WEB COMMUNICATION USING REVERSE PROXY

System Construction

From the view points of the system management and easiness of system construction, web communication is a suitable to provide information stored in ACC-LAN to many people. To meet the requirements, a combined system with reverse proxy servers for web communication and a firewall has been constructed for providing accelerator information to RIKEN-VLAN with ensuring secured access. Installation of reverse proxy servers, in front of real web servers, is widely used prescription for security and caching.

In order to implement the system, the standard package of CentOS 5.5 has been used as the operating system. Further, Iptables [3] for the firewall and Squid [4] for the reverse proxy server are installed. The system chart and basic concepts are shown in Fig. 2. The significant feature of our system is that accesses from RIKEN-VLAN are masked by the web servers behind the reverse proxy servers. As a result, our system is protected from attacks.

Access Control of Information

In order to restrict unnecessary accesses from beam users and visitors to critical information of accelerator control, such as operation log and raw data, we have adopted an authentication system. In order to control the access of users by authentication, our system consists of two reverse proxy servers. To manage the username/password and denial or allowance to hosts from each user easily, accelerator staff members and beam users/visitors use different reverse proxy server. Therefore, the environments that allow users to access web sites are different for accelerator staff members and beam users/visitors, because the content of information is different. Beam users/visitors are permitted to access only some specific website without the authentication, while accelerator staff members can access all the registered web servers in ACC-LAN with authentication. Consequently, single sign-on (SSO) authentication has been achieved by choosing the accessible reverse proxy server for the accelerator staff members, because SSO has a mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems.

Protection against Illegal Access

In order to prevent illegal accesses using SSH and other protocols, the revers proxy system opens only a minimum number of ports to the reverse proxy servers by installing firewall. Additionally, access control based on network addresses was implemented, that is accesses using HTTP protocol required from the PCs having Nishina Center's network addresses in RIKEN-VLAN. Furthermore, the authentication system is used not only for the access control but also play an essential role for the protection against illegal access. Actually, it is difficult to test vulnerabilities against all the type of attacks, for example cross site scripting, for all of the web sites inside ACC-LAN. However in this case, the administrator needs to test only a small number of web sites which visitors can access without authentication.

Result of Access Test

The following software and devices, which support a web interface or the HTTP protocol, have been used inside ACC-LAN.

- Zlog (Zope based Operational Log System) [5]
- MyDAQ2 (MySQL based Archive system) [6]

- Wiki-based log system for 28GHz Ion Source [7]
- Wiki-based documents for RIBF control system
- RIBFCAS (RIBF control data archive system) [8]
- Video server (produced by AXIS using ActiveX)
- Network camera (produced by Sony using ActiveX)
- Digital oscilloscope (produced by Agilent)
- Digital measurement instrument (MW100 produced by Yokogawa Electric Corporation)

We executed access tests to check if the ones listed above in ACC-LAN can be accessed from RIKEN-VLAN via the reverse proxy servers. As a result, it was confirmed that all of them except the digital oscilloscopes and MW100, which have web interface using Java applet, can be accessed successfully.

Other Web Services

The present method enables us to develop a new type of software of RIBF control system with HTTP protocol because process variables (PVs) of EPICS can be accessed from RIKEN-VLAN via reverse proxy server. PVs are converted into XML and JSON formats by our frame-work, which run on the apache and is written in PHP by using PHP EPICS module developed by PSI [9]. Since many application programming interfaces, such as web application have been adopted XML and JSON format recently, it has scalability for the system development. For this reason, using PVs converted XML and JSON formats, we can develop EPICS clients running on RIKEN-VLAN without the use of EPICS channel access protocol.

Additionally, some applications have been provided by using LabVIEW's HTTP service after construction of this revers proxy system. One example of these applications is "Beam Transport Map" developed by R. Koyama et al. [10]. This web application provides real-time operation status of RIBF accelerators with members, users of RIKEN Nishina Center via this reverse proxy. Consequently, various types of monitoring data and status in ACC-LAN become commonly communicated in RIKEN-VLAN by using HTTP protocol (See Fig. 3).

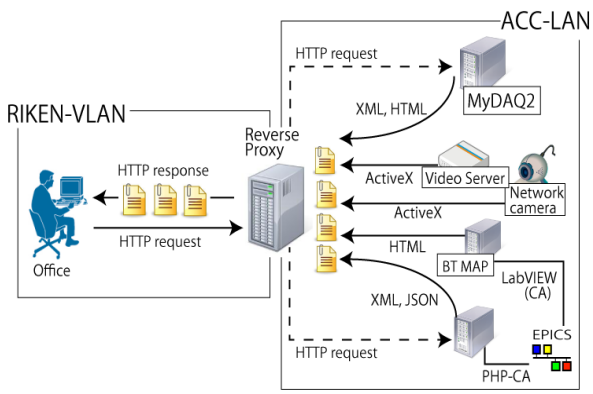

Figure 3: Integrated communication with HTTP protocol.

SOFTWARE UPDATE

Generally, almost all Linux distributions are updated by using YUM and APT. However, it is not easy to update software in a closed network, when it is required to fix security bugs. In the RIBF control system, almost all servers and clients have adopted CentOS and Scientific Linux based on Redhat Enterprise Linux. Therefore, we constructed our own YUM server inside the ACC-LAN. When a serious security hole will be reported, we will install an updated package in our YUM server as soon as possible.

E-MAIL ALERT

Although, it was successfully proceeding to implement the reverse proxy system in RIBF control system. The present work is not completed and the introduced system is not a perfect risk-free system from the view point of information security. As an example of perfect risk-free system in sending information from a completely closed network system, we introduced a new E-mail alert system. It is also important to notify administrators via E-mail automatically on serious failures for management of servers and systems. Since RIBF control system did not have this feature, we designed and implemented a system to send E-mail alerts from EPICS. The present alert system sends E-mail by using on-off control action of EPICS-based mechanical switches without a connection between the networks.

The system consists of an E-mail auto-sender embedded board (mailer board, See Fig. 4) manufactured by TriState ltd. [11], Yokogawa FA-M3 as Programmable Logic Controller (PLC) and Linux Input/Output Controller (IOC). The system chart is shown in Fig. 5. The main characteristic of the mailer board is sending E-mail to a specified mail address that is determined by 16 DIs. The mailer board is installed as a standalone E-mail client in the RIKEN-VLAN. The PLC is installed as one of EPICS control devices within ACC-LAN. As a result, the E-mail alert from EPICS IOC installed in ACC-LAN was sent to RIKEN-VLAN with secured access, though the each network is separated completely. In RIBF control system, it has been used as E-mail alert to administrators in case of system troubles, such as interruption of important services, and reboot of EPICS IOCs.

We have succeeded in sending information using hardware signal in a perfectly closed network. Currently, the reverse proxy system and E-mail alert system are being weighed from the view point of ensuring security.

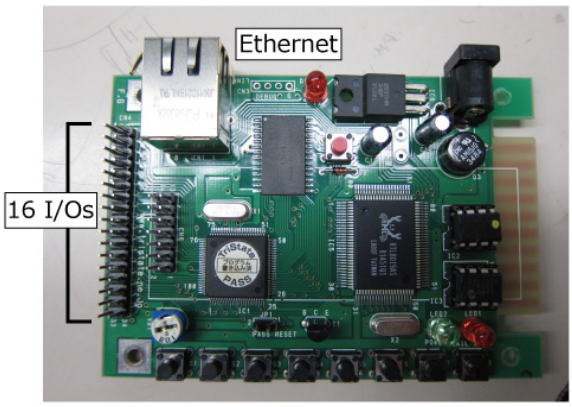

Figure 4: Photograph of the E-mail auto-sender embedded board manufactured by TriState Ltd.

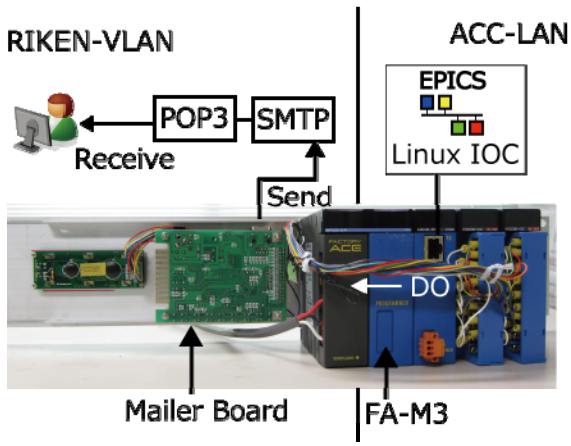

Figure 5: The system chart of E-mail alert.

SUMMARY

Reverse proxy servers, which interconnect the RIBF control network and the RIKEN-VLAN for providing various types of services in the RIKEN Wako campus, were designed and constructed. The HTTP protocol was adopted for the reverse proxy servers to allow accelerator staff members, beam users and other staff members to access the real-time information on operational status of accelerators with ensuring security against possible attacks via the RIKEN-VLAN. In addition, an E-mail alert system has been constructed by using an E-mail auto-sender board on the RIKEN-VLAN and a PLC-based IOC, prepared in ACC-LAN. The E-mail alert system helps the administrators to notice quickly when serious problems occur. It was confirmed that reverse proxy system is an effective method to provide information ensuring secured access in RIKEN RIBF. The usefulness of E-mail alert system without network connection was also proved by operational experience.

ACKNOWLEDGEMENT

One of the authors (A.U) would thank to Prof. K. Furukawa of KEK for useful discussion and valuable comments.

REFERENCES

[1] M. Komiyama et al., "Status of Control System for RIKEN RI-Beam Factory" Proc. ICALEPCS07, Knoxville, Tennessee, USA, 2007, p.334
[2] http://adobe.com
[3] http://www.netfilter.org/projects/iptables/
[4] http://www.squid-cache.org/
[5] K. Yoshii et al., "Web-Based Electronic Operation Log System – Zlog System" Proc. ICALEPCS07, Knoxville, Tennessee, USA, (2007), p.299.
[6] T. Hirono et al., "Development of Data Logging and Display System, MyDAQ2" Proc. PCaPAC08, Ljubljana, Slovenia, (2008), p. 55.
[7] A. Uchiyama et al., "Construction of Client System for 28GHz SC-ECRIS" RIKEN Accel. Prog. Rep. 43, p. 133, 2009.
[8] M. Komiyama et al., in these proceedings.
[9] A. Bertrand et al., "EPICS on the WEB" Proc. 10th ICALEPCS, Geneva, Swiss, (2005), P3_087.
[10] R. Koyama et al., "Development of "BTmap": Online visualization of beam-transport status" RIKEN Accel. Prog. Rep. 44 (Accepted).
[11] http://www.tristate.ne.jp/mailer02.htm