MEDINFO 2007
HISA Ltd Australia
© 2007 The authors. All rights reserved.

Secure Remote Access for Web Based Clinical Information System Using Policy Control of PCs and Healthcare PKI Authentication

Katsuya Tanaka[a], Mayumi Yoshida[b], Ryuichi Yamamoto[b]

[a] *Department of Planning, Information and Management, The University of Tokyo Hospital*
[b] *Interfaculty Initiative in Information Studies, Graduate School of The University of Tokyo*

Abstract and objective

This paper describes a robust method of secure remote access for Web based clinical information system using Healthcare PKI authentication. It enables medical staffs to refer the medical data using his own PCs from their home or their mobile phones over the Internet. This system contributes to reduce strain of medical staffs especially in such institutes where intensive care is carried ***uninterruptedly.*** *For this purpose, it must permit the remote access to the hospital information system from PCs in various conditions, it is necessary to establish a secure connection using VPN or SSL, and control the policy of client PCs for the prevention of computer virus effect etc., and at the last, confirm user authentication with strict identification using Healthcare PKI (HPKI).*

Keywords:

Healthcare PKI, Clinical Information System, Secure Remote Access Control, VPN

Introduction

In Japan, healthcare ICT is promoted by Japanese government and in 2006, the government made "New IT Reform Strategy" and "The Action Plan 2006". It emphasizes the reengineering in the healthcare field using ICT. It includes some actual plan such as constructing secure and reliable network for regional and inter-regional cooperation and development of Healthcare PKI (HPKI) which is based on ISO 17090. Actually we started to use HPKI in 2004, as a demonstration experimental system in the University of Tokyo Hospital for secure remote access to the medical data. HPKI was used in this system for authentication purpose, with verification the attributes of the national licenses of healthcare professionals, such as medical doctors, registered nurse, etc. By using this system, a physician can access the medical data of his patients with his own PCs even in his home or his mobile phones.

Methods

In our hospital, medical staffs are able to access to medical records using web based system in addition to special client PCs. The overview of the developed system is shown in Fig.1. Mainly based on the web interface, the following parts were developed.

1. Certification Authority (CA)
For the convenience of user registration operation, All CA function was implemented in a note PC. It is also used for registering HPKI certificate to USB token. The CA function was implemented on a virtual Linux machine in that note PC using OpenSSL library, and the host OS of the PC was Microsoft Windows 2000 with a capability of handling HPKI certificates (i.e. getting a certificate via web interface of the virtual machine, and storing it to the USB token).

2. VPN gateway
The connection between the hospital network and a client PC is established using IPSec. We picked a VPN gateway, Cisco Systems/VPN 3005.

3. Policy Control System
At the establishment of VPN connection, the server side policy is downloaded to the client PC, and during the connection, client PC is under the predefined policy which force PC to evoke only modules essential to brows our server and stop working other unnecessary modules. We picked Check Point (Zone lab)/Integrity.

4. USB Token for HPKI
At the insertion of this USB token, HPKI certificate is copied to the certain repository in Windows, and on the removable of token, the repository is cleared.

5. Reverse Proxy Server
For the verification of the HPKI certificate, especially hcRole attribute, user access is only allowed via this SSL reverse proxy server. At the connection to an internal web server in hospital, the user certificate in client PC is pushed and verified. This proxy server was developed by adding a capability of handling HPKI certificates to Fujitsu Co. Ltd./Interstage Security Director

6. Mobile Access System
For the mobile access over the Internet not using HPKI, we developed CHTML converter gateway. The identification number of each mobile phone is stored at the registration in server side, and the access of unknown device is prohibited. The overview of the system is shown in Fig. 2.

In each case, the user needs to access the SSL gateway first of all, and then log onto the web-based hospital information system using his account (id/password), choose a patient, refer to the patient information.

Results

In this experiment, 30 doctors for the PC client access system and 20 doctors for the mobile phone access system participated and the developed systems are now in use. This system is effective to check the results of emergency laboratory tests, or radiological images on PACS system from remote place.

We also carried out a questionnaire for the participants, and the following points were pointed out.

1. Identity Verification

At the registration, the hospital ID card and the driver's license card with a picture were checked. The participants say it is reasonable enough for the user verification.

2. Client Software

This system requires various client software modules, such as IPSec client software, USB token driver and policy control client, so it is difficult to manage for the user to install or operation.

The software environment of PC clients quite differs from one to another depending on the user's usual system usage or his work. It sometimes caused troubles at the installation or the operation. We had some difficult problems to support users against these various PCs.

3. Connection Environment

For the access from the user's home, the client PC is not always directly connected to the Internet. Especially when the access needs to be established through a NAT router, some users had a difficulty to realize an IPsec VPN connection.

For the mobile-phone access system, no claims were pointed out.

Discussion

Our developed system aims to realize a secure access over the Internet to the web-based clinical information systems in the hospital. Main issues are,

1. Secure Connection

SSL connection over IPsec VPN was used. It is safe enough to protect the clinical information from snooping or other risks for the access over the Internet.

2. Policy Control of client PCs

For the restriction of running dangerous .exe/.dll programs, we need to gather the environment information of various client PCs. It is easy to restrict the access depending on browser type or its version, but it is very difficult to judge whether other installed programs or libraries are safe or not. Our policy control method which allows only essential modules to work is an effective solution in such situation.

3. Authentication using HPKI certificate

In this experimental system, we restricted access to the user whose certificate includes an hcRole attribute of "Medical Doctor". The account itself has the attribute information of the user's job title. The requirement of this feature has lower priority.

We are now discussing for the improvement of this system, taking in recently available technologies such as smart card for the HPKI token, SSL-VPN technology for an easy management of client PCs. Concerning secure data access, it is better to use virtual machine environment on the client PC side working with a SSL-VPN gateway.

Conclusion

Our developed secure remote access system is described. It was implemented based on proxy gateway adding no special reconstruction to our hospital information system. In the experimental results, several improvement factors for the software installation or operation issue were pointed out. For the achievement of higher user-friendliness, it is necessary to apply other easy-to-use methods, such as SSL-VPN with virtual client environment.

References

[1] ISO TS 17090 Part 1 – Part 3, "Health Informatics - Public key infrastructure –", ISO, Geneva, 2002

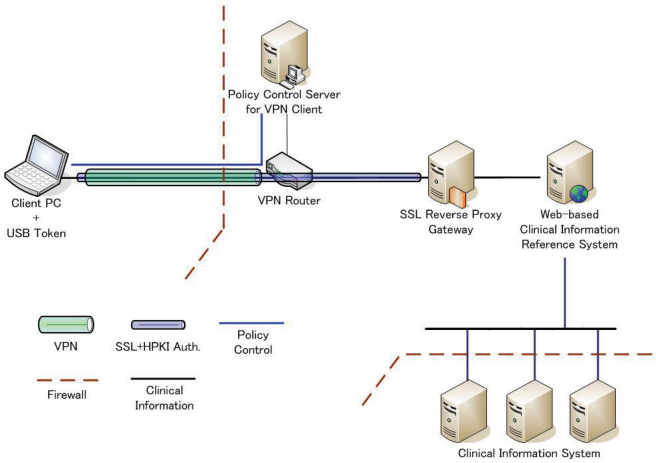

Figure 1 - Overview of developed secure remote access system for PC client

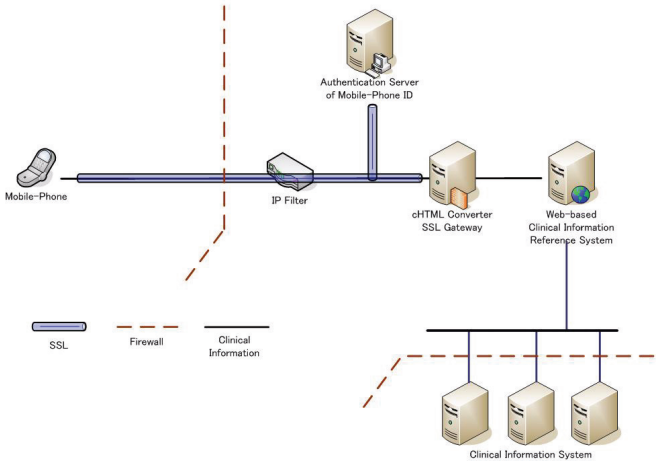

Figure 2 – Overview of developed secure remote access system for mobile phone