Remote support of hospital equipment – how does it work and what are the data security issues?

April 2003

Klaus Kjøller
Radiometer Medical A/S
Åkandevej 21 DK-2700
Brønshøj, Denmark

It is more and more common that computer-based systems in hospitals are serviced or "looked after" by service engineers dialing in from remote locations.

The combination of highly computerized laboratory equipment and the emerging network technologies makes remote support a very attractive possibility. In many cases, simple problems can be solved or questions be answered if a service engineer is able to "take a look" at the equipment.

Technologies supporting remote support have moved all the way into standard operating systems; one example is Windows XP from Microsoft, which includes Remote Desktop. With Remote Desktop it is possible to let another computer in the network take control of the XP computer for e.g. troubleshooting an application problem.

Applying technologies like these to the healthcare environment raises security concerns - if remote users are granted access to my systems does that mean that sensitive patient information can fall into the wrong hands?

This article describes some of the security issues and how they are dealt with when remote support systems are implemented.

Introduction

Remote support can be implemented as an integrated part of a computer-based system in which dedicated software is written as part of the system application. Such solutions will often be used for very sophisticated devices offering e.g. constant monitoring of the system.

Alternatively, remote support is implemented with third-party software solutions such as NetOp from Danware or pcAnywhere from Symantec. This article focuses on the latter type of remote support implementations.

Both NetOp and pcAnywhere consist of two applications - a host application and a guest application. The host

application is installed on the computer system, which should be accessed remotely, and the guest application is the program used to access the host.

The host application runs as a background application on the computer and "wakes up" when a remote user accesses the host system.

The guest application allows a remote user to use her screen, keyboard, and mouse exactly as if she were sitting in front of the host computer. The screen signal from the host computer is transmitted to the guest and any keystrokes or mouse clicks made by the remote user are sent back to the host system.

The communication between the host and the guest can be either point-to-point communication using a modem connection between the two stations (**Fig. 1**) or a network connection using the Internet (**Fig. 2**).

FIG. 1

FIG. 2

Security issues

The following sections deal with security-related issues. These can be divided into two categories:

- Access security
- Communication security

Access security is related to controlling access to a computer system, and assigning user privileges to users working on the system are, in general terms, a question of how to keep intruders from entering the system and how to control what different users are allowed to do.

Communication security is related to the techniques used to keep information sent between the two stations secret, or, in general terms, how to prevent unauthorized persons from monitoring or listening to the data transmission.

Access security is independent of the transmission method used between the two stations, whereas communication security is related to which data transmission method is used.

Access Security

Remote support systems such as NetOp and pcAnywhere come with a number of built-in access security features:

1. Access to the guest software package - access to a host running the remote support software is only possible with the right guest software; it is not possible to get access from e.g. a standard Internet browser like Internet Explorer.
2. Closed user group - guest and host software need to be members of the same closed user group. This means that the remote support host distributed by e.g. Radiometer only allows access to a remote support guest from Radiometer. The guest software cannot be purchased from any third-party software distributor.
3. Logon authentication - in order to log on to the system the user must be configured on the host system with a user id. and a password.
4. Access profiles - users are allocated a specific user role (a user profile) on the host system. The user profile describes which parts of the computer system the remote operator can access; for example, it is possible to define a setup in which a service engineer working from remote does not have access to patient-related information but can work with all service programs and analyzer-related data.
5. Connection notification - the host system can be configured to notify local users when a remote operator is accessing the system. The notification displays the name of the user wanting access and prompts the local user to confirm the remote session.

Communication security

The communication in remote support systems can be established in such a way as to have the same security level as online Internet-based home-banking systems:

1. The type of data sent between the host and the guest. Products like NetOp and pcAnywhere do not transmit "raw" data; the information exchanged between the host and the guest is so to speak a picture of the screen. If somebody looks at the data stream, the only information they can see is information to the guest about how to build the screen image and not information about the content of the screen image. The data sent back to the host are keystrokes and mouse movements - again, this is not readable text but information to the host software about where to position the cursor and which characters to enter.
2. Communication protocol - the communication protocol used between the host and the guest is not a standard communication protocol but a proprietary protocol developed and optimized for the specific product.
3. Optional encryption of the data stream - encryption is a mathematical way of coding the information. The host and guest modules include a number of different encryption algorithms, which can be used to code the data sent between the two stations. Encryption techniques are widely used when transmitting data on the Internet; one of the best known protocols for data encryption is the SSL (Secure Socket Layer) used on most web pages for entering e.g. credit card information.

Data encryption is based on mathematics and requires computer resources in both host and guest, and the user will often feel that a system is running more slowly when encryption of the data transfer is enabled.

Systems like NetOp offer different levels of encryption in order to provide the right level of security and performance - the term "level of encryption" refers to how difficult it is for an unauthorized "listener" to break the coding and retrieve the original content of the transmission.

The host and the guest can communicate either by modem (**Fig. 1**) or by using the Internet as a transport media (**Fig. 2**). The two communication methods offer different security features.

Communication methods and security aspect

Remote support systems are communicating via the telephone network or by the Internet.

Modem-based communication

Communication based on modems is point-to-point communication. The guest dials the phone number of the host system; when a telephone connection is established the authentication procedure is initiated and the guest can log on to the host system. A very commonly used security feature when dealing with modem-based communication is dial-back.

Dial-back means: When a guest is accessing the host by establishing a modem connection, the host will disconnect the phone connection immediately and return the call to a predefined phone number of the guest. This means that only a predefined phone number can get access to the system - this could e.g. be the phone number of the service office. Dial-back prevents unauthorized persons from accessing the system.

Internet-based communication

A commonly used way to use the Internet for remote support communication is to establish a VPN (Virtual Private Network) tunnel from the guest PC to the network of the host system.

VPN is a private connection over an open network. VPN connections manage authentication between the host network and the guest PC and provides data encryption for the connection.

Only authorized users can access the network, and the data exchange cannot be intercepted. VPN connections are often offered by central hospital IT departments

for remote access to hospital systems and require a special VPN client software package at the guest end; this software must be supplied by the hospital network responsible and is closely related to the way the hospital is connected to the Internet.

Using remote support via a VPN connection is very secure, and with the very high bandwidth on the Internet it is a very attractive and easy way to establish a remote support system.

Logging of sessions

Systems such as NetOp and pcAnywhere can be configured to keep a log of all remote users and their activities when they access the host. This feature does not provide direct data security but allows a supervisor to review which remote operator has been working on the host system and when.

Conclusion

Remote support products such as NetOp and pcAnywhere come with a wide range of built-in security features, which configured and used in the right way provide a very secure system with limited risk of compromising data integrity.

The technologies used are the same as those used for transmitting critical data in Internet environments where most people accept to send e.g. their credit card information to servers on the other side of the world.

This kind of application is used in many application areas such as banking and finance institutions and there is no reason not to benefit from this new technological possibility in the healthcare area.