

A remote data access architecture for home-monitoring health-care applications

Chao-Hung Lin^a, Shuenn-Tsong Young^{b,*}, Te-Son Kuo^{a,c}

^a Department of Electrical Engineering, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei 106, Taiwan, ROC

^b Institute of Biomedical Engineering, National Yang-Ming University, No. 155, Sec. 2, Li-Nung St., Taipei 112, Taiwan, ROC

^c Graduate Institute of Biomedical Engineering, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei 106, Taiwan, ROC

Received 15 December 2005; received in revised form 16 February 2006; accepted 3 March 2006

Abstract

With the aging of the population and the increasing patient preference for receiving care in their own homes, remote home care is one of the fastest growing areas of health care in Taiwan and many other countries. Many remote home-monitoring applications have been developed and implemented to enable both formal and informal caregivers to have remote access to patient data so that they can respond instantly to any abnormalities of in-home patients. The aim of this technology is to give both patients and relatives better control of the health care, reduce the burden on informal caregivers and reduce visits to hospitals and thus result in a better quality of life for both the patient and his/her family. To facilitate their widespread adoption, remote home-monitoring systems take advantage of the low-cost features and popularity of the Internet and PCs, but are inherently exposed to several security risks, such as virus and denial-of-service (DoS) attacks. These security threats exist as long as the in-home PC is directly accessible by remote-monitoring users over the Internet. The purpose of the study reported in this paper was to improve the security of such systems, with the proposed architecture aimed at increasing the system availability and confidentiality of patient information. A broker server is introduced between the remote-monitoring devices and the in-home PCs. This topology removes direct access to the in-home PC, and a firewall can be configured to deny all inbound connections while the remote home-monitoring application is operating. This architecture helps to transfer the security risks from the in-home PC to the managed broker server, on which more advanced security measures can be implemented. The pros and cons of this novel architecture design are also discussed and summarized.

© 2006 IPEM. Published by Elsevier Ltd. All rights reserved.

Keywords: Home care; Remote-monitoring; Telemedicine; Patient satisfaction; Security; Availability of health services

1. Introduction

In many countries the percentage of people with chronic diseases such as diabetes, hypertension, asthma, cardiovascular diseases and motion degeneration continues to increase, in part because of the aging of the population. The appropriate management of such chronic diseases relies on self-measurements by the patient – such as glucose measurement for diabetes, blood pressure for hypertension, electrocardiogram for cardiovascular diseases, and peak flow for asthma – in order for the physicians to provide a good diagnosis and

select the correct therapy. In home care settings patients are often asked to keep a patient diary, but unfortunately many such diaries are not useful due to the patients not complying through simple forgetfulness. The continuing developments in PCs and the Internet are creating a low-cost communication infrastructure, and the residential adoption of broadband connections is steadily increasing, resulting in remote home-monitoring being considered a solution in Taiwan and many other countries [1–7].

Remote home-monitoring can provide a channel for communication and information exchange among patients, caregivers and health care institutes. The self-measurements and other patient data can be accessed by members of the patient's family away from the home to ensure that the patient diary is

* Corresponding author. Tel.: +886 2 28267022; fax: +886 2 28210847.
E-mail address: young@bme.ym.edu.tw (S.-T. Young).

kept up to date. If any readings are outside the parameters set by the physicians or relatives, the family members can take immediate action to address the patient's needs.

The application scenarios include the following:

1. The remote-monitoring users occasionally check that the patient is indeed performing self-measurements and keeping the patient diary.
2. The remote-monitoring users actively access the real-time patient information remotely (e.g. still pictures of the patient) to ensure his/her safety at home.
3. The remote-monitoring users request more patient data upon receiving an event notification indicating an abnormality of the in-home patient.

A remote home-monitoring system gives informal caregivers information on the health and well-being status of the patient without being intrusive or requiring them to call or visit to obtain such information interrogatively. It is also effective in reducing the transportation costs and hospitalization, and achieving patient satisfaction. A remote home-monitoring system, however, differs in certain aspects from other telemedicine systems. The prevalence of home care systems is dependent on the cost, ease-of-use and especially on the security and availability of the system.

In this paper we present a novel architecture design for remote home-monitoring to address the security and availability issues.

2. Security challenges for remote home-monitoring systems

2.1. Topology and application scenarios for typical remote home-monitoring systems

A typical remote home-monitoring system usually comprises the following components:

- In the home
 1. *Measurement devices.* The measurement devices are used to acquire patient data including blood pressure, blood glucose, ECG, peak flow and even images of the patient. Examples of measurement devices include a Web camera that takes images of the patient, a blood glucose meter and an ECG monitor.
 2. *PC as a home gateway (and the computer program running on the home PC).* The patient data are stored and processed on a home PC that is connected to the Internet so that remote-monitoring users have access to patient information.

The in-home connectivity can be achieved using wired or wireless technologies.

- In the remote/mobile setting
 3. *Monitoring devices with Internet connectivity.* The monitoring device provides the remote-monitoring user with access to the data of the in-home patient. This

device allows the remote-monitoring users to make requests for the patient data, and displays the returned data on a screen. The monitoring device can be a PC/notebook (NB) with a Web browser (e.g. Microsoft Internet Explorer) or a handheld device (e.g. PDA, Personal Digital Assistant) with a microbrowser that is able to connect to the Internet.

Generally speaking, there are two application scenarios for remote home-monitoring systems: (i) identifying an abnormality in the patient data and automatically notifying the remote-monitoring users, and (ii) an active remote request for information about the in-home patient from the remote-monitoring users. In the former scenario, the measurement device collects the patient data periodically or continuously and sends the measured data to the home PC for processing. The users can consult the physician and set the alarm criterion in the home PC computer program. For example, the user can set a lower threshold for the heart rate, and the computer program will detect an abnormality if the heart rate becomes lower than this threshold and then send an email or Short Message Service (SMS) message to the remote-monitoring device. In the latter scenario, the remote-monitoring users use the monitoring devices to connect to the home PC via the Internet and request patient data.

2.2. Potential risks of a remote home-monitoring system

The Internet is a useful platform for remote home-monitoring because it is inexpensive and widely adopted. However, Internet technologies were designed to optimize information sharing and interoperability rather than security, and so Internet applications are subject to several inherent risks.

In the topology of a typical remote home-monitoring system, the home PC is directly accessible by the remote-monitoring devices via the Internet. The remote-monitoring devices can connect to the home PCs, and allow the remote-monitoring users to request patient information. Since the home PC is continuously connected to the Internet to listen to the requests from the remote-monitoring users, it is threatened by potential unauthorized intrusions and possible DoS attacks, such as from computer hackers who attempt to illegally obtain private information on the Internet. The home PC, though sufficiently cheap to be widely adopted, is vulnerable to malicious programs and hackers. The risks include the remote home-monitoring service being rendered unavailable during such virus attacks or DoS attacks, and computer hackers gaining access to or even altering patient data.

Many security measures have been discussed, developed and applied to such systems, such as role-based access control, multilevel security, device and user authentication, authorization, session-specific encryption and audit trails [7–9]. These measures protect the application and patient data, and are classified as application-level or data-level measures. However, countermeasures against operating system

attacks and the protection of the home PC should also be considered. Attackers usually exploit known vulnerabilities in specific operating systems to mount DoS attacks, and the remote home-monitoring service may not be available under such attacks from the Internet. An even worse situation is a hacker being able to take control of the home PC. These security risks exist as long as the home PC provides services via the Internet. Protecting against these attacks requires performing frequent security updates of the operating system and other applications and investing in security appliances, both of which are not feasible in the home due to the cost and the patients' lack of computer experience.

3. Proposed novel topology for a remote home-monitoring system

Given the aforementioned security and access problems associated with the use of a home PC and the Internet, here we propose a novel topology for a remote home-monitoring system that introduces a 'broker server' between the remote-monitoring devices and the home PC to avoid any direct access from the Internet to the home PC, as shown in Fig. 1. The formerly-developed security measures, including data encryption, authentication, authorization and audit trails, can still be applied without question, but that falls beyond the scope of this paper.

The broker server acts as a communication channel between the monitoring devices and the in-home computer programs. It passes users' requests from the monitoring devices to the computer programs running on the home PCs on the monitored side, and passes the patient data from the monitored side back to the monitoring devices. The broker server is designed to serve multiple users by supporting multiple communication channels between both sides. As shown in Fig. 1, the solution we propose is that instead of keeping listening to the requests from the monitoring devices, the computer program running in the home PC actively polls the broker server for any incoming requests from the remote-

monitoring users. The broker server handles the communication with the browser-based monitoring devices and with the computer programs in the homes.

In this topology, the in-home computer program on one hand controls the measurement devices to collect patient data according to some preset rules or following requests from remote-monitoring users; on the other hand, it handles the communication with the introduced broker server, instead of with the remote-monitoring devices. The patient data are still stored and processed in the home PC and now direct access to the PC from the Internet is not allowed.

The measurement devices on the monitored side and the remote-monitoring devices remain the same as those described in Section 2.1, but the remote-monitoring devices now connect to the broker server, instead of the home PC to remotely retrieve the vital signs and other data from the monitored person.

3.1. Components of the broker server

The broker server is the core of the proposed remote access topology. As shown in Fig. 2, it comprises the four main components described below. The monitoring-side Web server is the service interface for the browser-based monitoring devices on the remote side. It takes a browsing command from the caregiver and waits for the computer program in the home PC to fetch the command. After the command is executed and the patient data are returned from the computer program, this component will send the data back to the monitoring users. With the launch of new monitoring devices (such as the evolving mobile devices), new service entries can easily be developed in this component. The patient-side Web server is the component that takes care of the communication with the computer program on the home side. As mentioned earlier in this section, the broker server is designed to serve multiple computer programs on the monitored side, each of which periodically polls the patient-side Web server for any incoming requests from the remote-monitoring users, according to a preset period. In our implementation, we use Microsoft

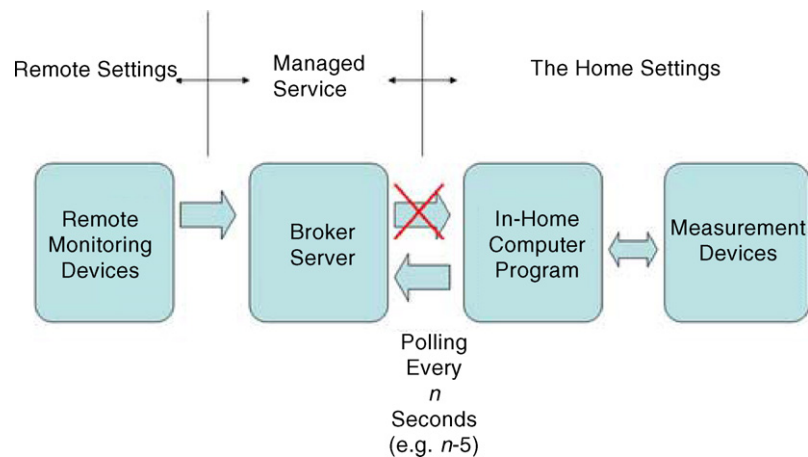


Fig. 1. The proposed system topology for the remote home-monitoring application that employs a broker server.

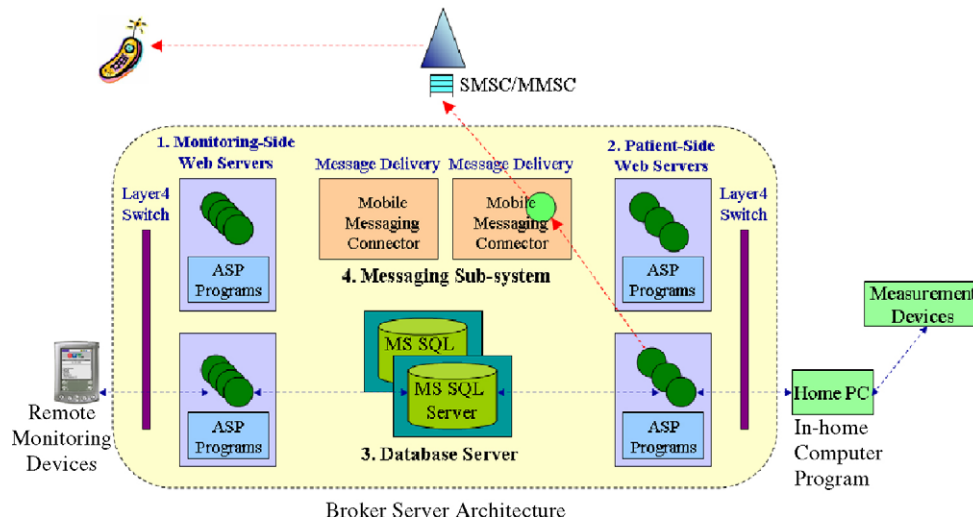


Fig. 2. The architecture of the broker server.

IIS (Internet Information Services) as the monitoring-side and patient-side Web servers, and Microsoft ASP (Active Server Pages) technology to run ASP programs on the Web servers, as shown in Fig. 2. The ASP programs on the patient- and monitoring-side Web servers handle the requests from the in-home computer programs and the remote-monitoring devices, respectively.

The information about the computer programs and the accounts of remote-monitoring users are stored in the database. In addition, the database server provides a request queue for incoming commands from the monitoring-side Web server and a response queue for responses returned to the patient-side Web server. In our implementation, we use Microsoft SQL Server 2003 as the database server, as shown in Fig. 2.

The messaging subsystem includes an SMS module and a Multimedia Message Service (MMS) module to deliver notification messages to mobile devices with diverse messaging capabilities. The messaging subsystem connects to mobile operators' SMS Center (SMSC) and MMS Center (MMSC) via the Internet. This subsystem is primarily used for the event-notification scenario and is not the focus of this paper.

3.2. Data flow with the proposed broker server

In Section 2.1 we describe two possible application scenarios of the remote home-monitoring system. Here we explore the data flow for the real-time browsing of patient data. In this scenario, the monitoring devices on the remote side and the computer programs on the home side are never directly connected together. Instead, as mentioned in Section 3.1, a request queue and a response queue are implemented so that the commands and the retrieved patient data can be exchanged at the broker server. HTTP (Hypertext Transfer Protocol) was adopted as the data communication protocol between the computer program and the patient-side Web server, and

between the remote-monitoring devices and the monitoring-side Web server. The PC-based computer program on the monitored side periodically polls the broker server for any browsing command from the remote-monitoring devices. When a remote-monitoring user wants to access in-home patient data, he/she activates the Web browser on the monitoring devices and makes a Web/HTTP connection to the monitoring-side Web server of the broker server. On the Web page returned from the monitoring-side Web server, the user can log on to the system and make a request for the in-home patient data. Upon receiving this request, the monitoring-side Web server invokes an ASP program that puts the data-request commands into the request queue in the database. The program also begins to poll the response queue, waiting for the patient data to be returned. The monitoring-side Web server will reserve the Web/HTTP connection with the remote-monitoring device until it obtains the patient data, and returns the data to the monitoring device through the same Web connection. The computer program on the home PC simultaneously keeps polling the patient-side Web server of the broker server, looking for any incoming requests from remote-monitoring users. For each round of polling requests, the patient-side Web server invokes an ASP program to look up the request queue and obtain the commands. The polling computer program will then obtain the command returned from the patient-side Web server in the next round of polling, make a request to the connected measurement device(s), perform patient-data retrieval according to the command, and return the data to the patient-side Web server. The ASP program on the patient-side Web server will then put the returned data into the response queue. The ASP program on the monitoring-side Web server obtains the returned data from the response queue, composes the data in HTML format and sends the patient data to the remote-monitoring devices through the previously reserved Web connection. Since the patient data have been composed in standard HTML format,

the remote-monitoring user can use a standard Web browser on the monitoring device to view the patient information. In this data flow there is no direct access to the home PC from the Internet, so this remote access application will not result in the home PC being attacked by hackers from the Internet. The users also can set up firewalls to deny all incoming connections without interfering with this remote access application. This topology aims to eliminate the risks of Internet intrusion but not the risks of Internet eavesdropping, so we also enable SSL (Secure Socket Layer) in our implementation so as to encrypt the data communications on the Internet. Other encryption mechanisms could be applied, but that is outside the scope of this paper.

In our implementation, we have set up two Web servers as the monitoring-side Web server and another two as the patient-side Web server. We have also deployed a Foundry ServerIron layer-4 switch, and attached the Web servers to it as shown in Fig. 2. A layer-4 switch, which is best known for its ability to balance the server load, is configured to dispatch the incoming Internet traffic to the attached Web servers to achieve load balancing and to avoid the so-called single-point failure, whereby if one Web server goes down the others will take care of the requests. The presence of the layer-4 switch slightly modifies the aforementioned data flow. On the monitoring side, the Web browser first connects to the layer-4 switch, with the requests dispatched to one of the monitoring-side Web servers. On the monitored side, the in-home computer program first connects to the layer-4 switch, with the requests dispatched to one of the patient-side Web servers. If traffic and system loading increase, more Web servers can be attached to the layer-4 switch to increase the capacity. For example, with an increasing number of in-home computer programs, we can stack more patient-side Web servers in Fig. 2.

4. Discussion

In a typical remote home-monitoring system, the home PC is usually directly accessible by the remote-monitoring devices via the Internet. This direct-access model makes the home PC (and the entire home network) vulnerable to attacks from the Internet, such as viruses or DoS attacks mounted by malicious programs. Here we propose a novel topology in which a broker server is located between the remote-monitoring devices and the home PCs. The absence of direct access to the home PC in such a topology improves the confidentiality and the availability of the remote home-monitoring system. In effect, the introduction of the broker server transfers the aforementioned security risks from the home PC to the broker server. The broker server will be managed by a service provider, and its security risks can be handled in the following ways:

1. Reported weaknesses of the system can be fixed on a regular basis since the broker server is under cen-

tralized management. Maximizing the security of the home-monitoring system requires it to be maintained and updated continuously.

2. More advanced and up-to-date security measures can be implemented on the broker server while the cost can be reduced by sharing the service between many users.
3. Other measures can be used to counter a DoS (or a distributed DoS) attack, such as remote redundancy and disaster recovery. These measures are very difficult or even impossible to apply in individual homes due to the associated cost and complexity. In contrast, the broker server can be implemented using a distributed topology, and hence such attacks would be split between multiple sites and so may overload only some of the servers, leaving the others operational. In comparison, it is not possible to deploy a distributed system in the home since this environment is essentially a single site.

A few positive and negative side effects also result from the introduction of the broker server. The positive side effects include the following:

1. No compromise in firewall configuration. Since there are only outbound connections from the home PC to the broker server, the firewall at home can be configured to deny any access from the Internet, which would eliminate the aforementioned inbound threats.
2. The home PC can have a dynamic IP address. In the previous direct-access model, the home PC must have either a registered domain name or a fixed IP address to allow a remote-monitoring user to connect to it. In our topology, as shown in Fig. 1, the remote-monitoring devices and the in-home computer programs access the broker server to exchange commands and patient data, and it is the only one that must have a fixed domain name to enable the remote-monitoring users to connect to the monitoring-side Web server and the in-home computer programs to connect to the patient-side Web server; any of the home PCs and the remote-monitoring devices can have a dynamic IP address.
3. The monitoring of system availability. Since the computer program polls the broker server periodically, the system components at home – including the home PC and the measurement devices – can regularly report their status (or presence) to the broker server. The broker server can then play the role as a centralized ‘presence server’. The implementation of presence management increases the availability of the remote home-monitoring system.
4. The integration with third-party systems or applications becomes much more flexible. For example, with the advent of more and more mobile devices, the broker server can be integrated with a Web-transcoding gateway and transform Web pages on the fly to ensure compatibility with diverse mobile devices, with the home PC remaining unchanged.
5. The complexity of the home gateway is reduced. Partial features of the home gateway can be realized in the broker

server, which helps to reduce the complexity (and hence maintenance) of the home gateway.

Some of the negative side effects of introducing the broker server include the following:

1. The latency of remote access of patient data is longer than without the broker server.
2. Since the computer programs on the monitored side poll the patient-side Web server of the broker server periodically, the loading of the patient-side Web server increases with the polling frequency and the number of in-home computer programs. In order to serve a large number of polling computer programs and to shorten the latency of remote access of patient data, it requires the deployment of more patient-side Web servers, which would be an extra capital expense for the service providers.

5. Conclusions

The continuing developments in PC technology and Internet access are creating a low-cost communication infrastructure suitable for remote home-monitoring applications. Coupled with the advances in biomedical sensors and telecommunication technologies, the Internet has the potential to dramatically improve in-home wellness management. A remote home-monitoring system aims to reduce the cost of home health care, casualty department visits and hospitalization. However, system security is a major barrier to the implementation of such systems, especially when the Internet is involved. Continuing reports of flaws in Internet and operating system security give a public impression that Internet technologies are not suitable for the exchange of sensitive information, such as patient data. Other serious concerns about privacy and security result from the typical home-monitoring usually being designed to connect the home PC to the Internet. The risks range from the home PC and network being hacked and taken control of, to confidential patient information being intercepted and revealed, to the system availability being jeopardized due to an Internet attack. All these risks would render a home-monitoring system unreliable.

In this paper we propose a novel topology that fulfils the security requirements of a remote home-monitoring system, with emphasis on system availability and robustness against DoS attacks. A broker server is introduced so as to remove the need for direct inbound access to the home PC, resulting in better confidentiality and availability of the home-monitoring system. The security risks are thereby mostly transferred to the managed broker server, on which more advanced security measures can be implemented. However, it should be remembered that perfect confidentiality and availability is impossible, even at extreme costs, and so a compromise has to be reached between perfect availability and security, and economic considerations.

Acknowledgement

The work presented in this paper has been supported by National Science Council Taiwan, R.O.C., under Grant No. NSC93-2622-E-010-004. We deeply appreciate their financial support and encouragement.

References

- [1] Chen H-S, Guo F-R, Chen C-Y, Chen J-H, Kuo T-S. Review of telemedicine projects in Taiwan. *Int J Med Inform* 2001;61:117–29.
- [2] Doolittle G. A POTS-based tele-hospice project in Missouri. *Telemed Today* 1997;5:18–9.
- [3] Doolittle GC, Yaezel A, Otto F, Clemens C. Hospice care using home-based telemedicine systems. *J Telemed Telecare* 1998;4:58–9.
- [4] Chisholm SW, Hahn MA. Emerging Veterans Health Administration geriatric and extended care initiatives. *Geriatric Nurs* 1995;16:42–4.
- [5] Lin HS, Chen HL, Liu DL, et al. NetCare City: a tele-visit system of nursing home at National Taipei College of Nursing. In: *Proceedings of the Medical Informatics Symposium*. 1999. p. 18.
- [6] Magrabi F, Lovell NH, Celler BG. A web-based approach for electrocardiogram monitoring in the home. *Int J Med Inform* 1999;54:145–53.
- [7] Lind L, Sundvall E, Karlsson D, Shahsavar N, Åhlfeldt H. Requirements and prototyping of a home health care application based on emerging JAVA technology. *Int J Med Inform* 2002;68:129–39.
- [8] Safran C, Goldberg H. Electronic patient records and the impact of the Internet. *Int J Med Inform* 2000;60:77–83.
- [9] Smith E, Eloff JHP. Security in health-care information systems—current trends. *Int J Med Inform* 1999;54:39–54.