Vital Signs Services for Secure Telemedicine Applications
Chaoxin Sima, Ravi Raman, Ramana Reddy,
William Hunt and Sumitra Reddy
Concurrent Engineering Research Center
West Virginia University
Morgantown WV 26506-6506

Telemedicine using teleconference provides only a part of the picture. The remote patient’s electronic medical record and vital signs may often be essential for proper diagnosis and treatment. While there are commercial solutions for telemonitoring, they do not address issues such as security and interoperability leveraging the growing public communications infrastructure. On the other hand there are performance considerations due to the quality of service over available communications media that can hinder real-time operation. The objective of this research effort is to develop secure tele-monitoring facilities that enable healthcare providers to collaborate over public communication networks; to securely convey their patient’s vital signs to a remote specialist; and to enable “near real-time” examination of those vital sign data. It is our belief that such applications can help overcome barriers to quality healthcare in the scattered populations of rural areas enabling telemedicine to be a part of the practice of medicine. The authors, who are developing secure telemedicine applications, describe their approach in developing secure vital signs services.

INTRODUCTION

Since 1993 the Concurrent Engineering Research Center (CERC) at West Virginia University has been developing computer-supported collaboration technologies and applications for clinical healthcare providers. One system, called ARTEMIS (Advanced Research Testbed for Medical Informatics)[1,2], funded jointly by the US Defense Advanced Research Projects Agency (DARPA) and the US National Library of Medicine (NLM), was among the first to enable healthcare providers to access distributed clinical patient records utilizing the World Wide Web. In October 1996, sponsored by the National Library of Medicine, CERC began developing the enabling technologies for Secure Collaborative Telemedicine applications to be used in three telemedicine scenarios: at rural hospitals, clinics, and homecare sites:

1. Secure telemedicine for intensive care providers enabling remote access of Intensive Care Unit electronic patient data.
2. Secure telemedicine for mid-level providers (such as physician assistants and nurse practitioners) providing computer-aided diagnosis and collaboration with remote supervising physicians.
3. Secure telemedicine for homecare patients through patient counseling information resources and support for near-time monitoring of patients with chronic ailments.

Crucial elements in these applications are the means to ensure the authenticity of users, to encrypt the information communicated between users and information resources, to enable remote “near real-time” viewing of patient vital signs, and to enable healthcare providers to collaborate synchronously and asynchronously with their peers. Our emphasis on security measures for safeguarding electronic health information is in accordance with the recommended practices of the National Research Council’s Computer Science and Telecommunications Board [3]. An earlier paper at AMIA 1997 provided an overview of our approach to develop the technologies and services for the secure telemedicine applications [4]. We have, since, developed a number of facilities to enable secure communications. Companion papers being submitted to this conference discuss our experience in developing smart card applications as well as details on the assessment methodologies for evaluations at our pilot rural telemedicine sites.

There are vendor solutions that enable remote monitoring, which are generally closed, proprietary solutions. Moreover, many are meant for large hospital systems and do not easily scale, cost effectively, to clinical telemedicine use. Facilities such as Microsoft’s Dialup Networking 1.2 with support for virtual private networks via PPTP (Point-to-Point Tunneling Protocol) and multi-link modems may allow some vendor solutions to be transparently overlayed. Multi-link modems allow the PC to leverage the availability of multiple phone lines to route data over them and thereby have a higher bandwidth. Such multilink modems are becoming available, even for cellular phones. A similar technique was employed in Maryland where a bank of cellular phones provided the bandwidth to transmit vital signs in (video format) from an ambulance [5].
SECURE VITAL SIGNS SERVICES

The Secure Collaborative Telemedicine Architecture (SCTA) employs an open systems approach, utilizing vendor-supported, standards-compliant components and technologies. To ensure scalability and broad usage, we are using CORBA (Common Object Request Broker Architecture). Where essential, we are employing vendor-supplied bridge facilities to accommodate other standards, such as Microsoft’s Distributed Component Object Model (DCOM) for integration and site-specific customization with essential applications and systems on client and server systems.

The Vital Signs Services was developed on the basis of an early version of CORBAMed’s IDL (Interface Definition Language) specifications. CORBAMed’s objective is to define consensus-driven specifications that facilitate integration of components from multiple vendors. CERC’s Vital Signs Services consist of four components:

1. A communications interface to the patient monitor, implemented as a dynamic link library, it implements the monitor specific communications protocol that controls and passes along the measurements and any alarms;
2. An on-site application program which interfaces with the patient monitor and communicates through a Vital Signs Server to remote viewers. This application program enables the local healthcare to identify the patient and control the vital signs to be measured and transmitted.
3. A Vital Signs Server, which is able to push the patient monitor data to one or more, authenticated remote healthcare providers.
4. A remote viewer program which enables the healthcare provider to authenticate themselves and to specify the category of vital signs that they wish to receive and view (from among those measured and available for transmission).

The patient monitor communications interface was implemented as a dynamic link library in the C++
programming language. The remaining three components were implemented in the platform-independent programming language Java. These three distributed components are integrated via CORBA, with the Vital Signs Server being a CORBA service. We developed CORBA transformers to provide secure communications between client applications and server/middleware services. The transformer employs key-exchange protocols and RSA (Rivest-Shamir-Adleman) encryption algorithms to ensure secure communications. This configuration enables one or more remote viewers to connect, authenticate and then receive near real-time vital signs.

The monitor that we employed was a Propaq 106-EL from Protocol Systems, Inc. It is a portable, rugged unit having an LCD panel and an RS-423 connector. It measures 3-lead ECG, non-invasive blood pressure, two channels of invasive blood pressure, temperature, saturation oxygen, end tidal carbon dioxide. Either of the client applications can run on a current day Pentium notebook PC. Though the monitor is capable of being used in an ICU, we are targeting its use in the mid-level and home care scenarios, because our pilot site hospital ICUs employ HP equipment. The Propaq monitor in conjunction with a notebook PC is, together, small enough to be carried easily to a patient’s home by a homecare nurse or into an examining room by a mid-level provider if either wished to communicate, synchronously, with a remote supervisor.

We tested the system over modems connected at 28.8kbps over the Internet and noticed that the typical delay was around 5 to 8 seconds when transmitting EKG waveforms along with the numerical data. For performance reasons, we chose to allow one waveform to be displayed at a time, but enabled the remote viewer to switch, at will, between the waveforms being measured. The buffered display at the remote viewer enables it to overcome small delays due to intermittent degradation of the quality of service over the Internet. The remote viewer application can print the current measurements so that they may be incorporated into a paper-based patient chart.

![Vital Signs Provider System](image)

**Figure 2. On-site Healthcare Provider Interface**
We are using PIN protected smart cards in our telemedicine applications for the identification and authentication of providers, and the storage of limited patient medical information [6]. The SCTA’s secure middleware components utilize authentication services that restrict access to authenticated and authorized personnel. We have developed healthcare professional and patient cards. Based on the G-7 healthcard interoperability specification [7,8], the patient cards contain emergency medical information including the patient’s demographics, insurance information as well as clinical information. Role-based access restricts the information viewed or modified by the patient and the different categories of health professionals (healthcare business staff, physicians and nurses).

We will shortly be integrating the smart card modules with the vital signs client applications enabling smart card based authentication of healthcare professionals. In case the patient were to have a patient card, then the application would be able transmit the information (restricted by the role of the remote healthcare professional) to enable it to be viewed in the context of the patient’s vital signs.

CONCLUSIONS

Public key cryptography technologies can enable secure communications over public networks. In combination with scalable, distributed object integration technologies such as CORBA, it can enable the development of near real-time vital signs monitoring systems which empower healthcare providers with the critical information necessary for the timely diagnosis and treatment of their patients. With Internet service providers being a mere phone call away CERC’s vital signs monitoring applications demonstrate that, through telemedicine, access to care need not be a barrier anymore.

Acknowledgments

This work has been sponsored by the U.S. National Library of Medicine under Contract No. N01-LM-6-3549. We would like to acknowledge the singular contributions to this research of Rahul Singhal and Dharmesh Mistry while they were graduate students at CERC. Rahul developed one of the early prototypes of the Vital Signs Service, while Dharmesh implemented the Protocol monitor interface. Thanks also to Yiming Hu, a graduate student at CERC, for his help during the testing and debugging of some modules of this system.
Figure 4. Printout of Patient Vital Signs

References


