ELSEVIER

journal homepage: www.intl.elsevierhealth.com/journals/ijmi

Risk analysis of information security in a mobile instant messaging and presence system for healthcare

Erlend Bønes[a], *Per Hasvold*[a], *Eva Henriksen*[a,*], *Thomas Strandenæs*[b]

[a] *Norwegian Centre for Telemedicine, University Hospital of North Norway, P.O. Box 35, NO-9038 Tromsø, Norway*
[b] *Well Diagnostics AS, P.O. Box 6431, NO-9294 Tromsø, Norway*

ARTICLE INFO

Article history:
Received 9 February 2005
Received in revised form 8 June 2006
Accepted 8 June 2006

Keywords:
Instant messaging
Mobility
Healthcare
Information security
Risk analysis

ABSTRACT

Introduction: Instant messaging (IM) is suited for immediate communication because messages are delivered almost in real time. Results from studies of IM use in enterprise work settings make us believe that IM based services may prove useful also within the healthcare sector. However, today's public instant messaging services do not have the level of information security required for adoption of IM in healthcare. We proposed MedIMob, our own architecture for a secure enterprise IM service for use in healthcare. MedIMob supports IM clients on mobile devices in addition to desktop based clients.

Methods: Security threats were identified in a risk analysis of the MedIMob architecture. The risk analysis process consists of context identification, threat identification, analysis of consequences and likelihood, risk evaluation, and proposals for risk treatment.

Results: The risk analysis revealed a number of potential threats to the information security of a service like this. Many of the identified threats are general when dealing with mobile devices and sensitive data; others are threats which are more specific to our service and architecture. Individual threats identified in the risks analysis are discussed and possible counter measures presented.

Discussion: The risk analysis showed that most of the proposed risk treatment measures must be implemented to obtain an acceptable risk level; among others blocking much of the additional functionality of the smartphone. To conclude on the usefulness of this IM service, it will be evaluated in a trial study of the human–computer interaction. Further work also includes an improved design of the proposed MedIMob architecture.

1. Introduction

Use of instant messaging services is becoming increasingly popular with Internet based systems like America Online's Instant Messaging, AIM (http://www.aim.com/), Microsoft's MSN Messenger (http://messenger.msn.com/), Yahoo! Messenger (http://messenger.yahoo.com/), and ICQ (http://www.icq.com/).

However, public instant messaging systems have been criticised for having a number of security weaknesses [1–3]. These weaknesses include the facts that the IM clients are always on, that logs can contain sensitive information, and that the communication goes via an externally controlled server. Most IM services were never intended for secure communication in the first place [2]. The rapid growth in the number of public IM users has created a new security concern for IT managers.

* *Corresponding author*. Tel.: +47 95731836; fax: +47 77754098.
E-mail address: eva.henriksen@telemed.no (E. Henriksen).

1386-5056/$ – see front matter © 2006 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.ijmedinf.2006.06.002

New worms and viruses are increasingly using IM to spread, and 5–10% of the IM traffic today can be categorised as spam over IM (SPIM) [4].

Within the healthcare sector information security aspects are of vital importance, and may be of serious hindrance for the adoption of IM based services. In this paper we will examine the feasibility of using instant messaging systems in the healthcare sector from the viewpoint of information security.

Healthcare professionals are working in a mobile environment with rapid changes in their availability status, and they are exposed to interruptions at any time, anywhere. In addition to traditional desktop IM clients, IM for use in healthcare settings should therefore also offer clients on mobile devices.

In order to take care of both mobility and security aspects, we have proposed our own architecture: the MedIMob system. An overview of the MedIMob architecture is presented in this paper. Components of the MedIMob system have been further developed at the Norwegian Centre for Telemedicine (NST).

The main contribution of the paper is the results from a risk analysis of the MedIMob system, based on the architectural design of the system. The results of this risk analysis may be valid to other systems with a similar approach. In the risk analysis the assumed environment for the system was a hospital department, and communication within the department and between IM clients inside the department and IM clients outside. Information security challenges were identified as a number of security threats of different risk levels. Solutions are proposed for improvements of the unacceptable threats.

2. Background

Instant messaging (IM) is a lightweight near-synchronous communication technology. Technically it offers asynchronous communication, but it is used as synchronous communication because the messages are delivered almost in real time. Additional functionality for publishing and subscribing to presence information makes it possible for the users to see which other users and resources are available at any time. Presence information can be based on, e.g. schedules and calendar information, user settings, or keyboard activity.

2.1. *Instant messaging use in workplace and healthcare*

IM has proven its value as media for personal communication, both for peer-to-peer channels and as a conferencing platform. This adoption has mainly been seen in private social contexts. Adoption in workplace has been slower; one reason could be apprehensions that the service would be used primarily for private purposes (chatting) resulting in misuse of time and resources; another reason could be the informality of the service and the lack of security and documentation.

Based on early results from studies of IM use in enterprise work settings [5–8], we believe that IM based services may prove useful also within the healthcare sector. There are a few descriptions of IM use within healthcare. One of them is the EU-funded research project PICNIC from the fifth framework programme (FP5) of Information Society Technology (IST). The project describes IM as one of several collaboration components in a healthcare network [9]. In their system IM is used to discover the online presence of connected experts that can be invited to collaborate, e.g. to give a second-opinion on a medical case. The invited expert uses IM to confirm that a second-opinion can be given or to request additional information.

IM solutions for enterprises, including healthcare, have been developed by different companies. One of the most interesting approaches is offered by UnBound Technologies Inc. [10], where IM is part of a business process management system for hospitals. This is a presence-based enterprise messaging platform that enables wireless communication with two-way alerting and notifications. The notifications can come not only from co-workers but also from legacy systems in, e.g. laboratory and radiology.

2.2. *Characteristics of the healthcare environment*

Healthcare professionals are working in a mobile environment with rapid change in their availability status. A Danish study [11] which focuses on local mobility in a hospital department, divides the need for mobility into four categories: (1) the need for being at different physical *places*, (2) the need to access *knowledge*, (3) the need to use shared *resources*, and (4) the need to get in contact with specific *persons*. Healthcare workers are exposed to interruptions at any time, anywhere. They usually carry pagers which give them a phone number to call, but without additional information about the reason for the request. Thus, it is difficult for them to decide the importance of the interruption.

In addition to the mobility, there are also other aspects that make the healthcare domain different from other arenas. One aspect is the need for documentation and traceability of decisions and actions. Another aspect is the high need for information security mechanisms caused by the privacy requirements related to communication of sensitive patient identifiable information. Confidentiality requirements originate from the professional secrecy and non-disclosure agreement imposed to all healthcare workers. Requirements to electronic communication of patient information come from national legislation in European countries, based on EU's regulation on processing of personal data (95/46/EC) from 1995 [12], and from the American Health Insurance Portability and Accountability Act of 1996 (HIPAA) [13]. At the lowest level these requirements become apparent through the security policies of the affected organisation.

2.3. *Risk analysis of information security*

Security risk analysis is a basic requirement of ISO 17799, internationally recognized as the generic information security standard [14]. Risk analysis is also required by national legislation as a vital part of an information security management system for any organisation. Risk analysis is performed with respect to the main information security aspects confidentiality, integrity and availability. The risk acceptance criteria are defined by the information security policies of the affected organisation.