A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems

Jason Reid\textsuperscript{1}, Ian Cheong\textsuperscript{2}, Matthew Henricksen\textsuperscript{1}, and Jason Smith\textsuperscript{1}

\textsuperscript{1} Queensland University of Technology, Information Security Research Centre, GPO Box 2434, Brisbane, Queensland 4001, Australia
\{jf.reid, m.henricksen, j4.smith\}@qut.edu.au
\textsuperscript{2} \{ian.cheong\}@acm.org

Abstract. This paper examines the access control requirements of distributed health care information networks. Since the electronic sharing of an individual’s personal health information requires their informed consent, health care information networks need an access control framework that can capture and enforce individual access policies tailored to the specific circumstances of each consumer. Role Based Access Control (RBAC) is examined as a candidate access control framework. While it is well suited to the task in many regards, we identify a number of shortcomings, particularly in the range of access policy expression types that it can support. For efficiency and comprehensibility, access policies that grant access to a broad range of entities whilst explicitly denying it to subgroups of those entities need to be supported in health information networks. We argue that RBAC does not support policies of this type with sufficient flexibility and propose a novel adaptation of RBAC principles to address this shortcoming. We also describe a prototype distributed medical information system that embodies the improved RBAC model.

1 Introduction

A fundamental concept underpinning the delivery of health care services is the notion that personal information shared with a clinician in the context of treatment is confidential. This means that the clinician must have the consent of the consumer to share information about the consumer with a third party\textsuperscript{1}. In practice, it is becoming far more challenging to ensure that all confidential health information disclosures have been consented to, particularly as health service providers adopt electronic systems based on internet technologies to facilitate

\textsuperscript{*} This research was funded and supported by the Commonwealth of Australia – Department of Health and Ageing.

\textsuperscript{1} In practice there are a number of important exceptions to the requirement for express consent, e.g., consent can be implied by circumstances or deemed unnecessary by legislation. For more information on consent requirements in health care see [4, 5].
information exchange. Electronic health information networks and electronic health records improve the ability of service providers to exchange personal health information and coordinate service delivery between clinical teams that cross organisational and geographic boundaries. As a direct consequence, an individual's personal health information is potentially available to larger numbers of people, significantly increasing the risk that the information will be accessed for purposes for which the consumer has not given their consent. A key challenge that attends the adoption of electronic health information networks is therefore to ensure that the principle of consent is meaningfully respected and enforced in electronic contexts. To achieve this a health information network needs to be capable of recording and enforcing individual access policies where the consumer defines the policy details.

1.1 Privacy in Health Care

Unauthorised disclosure of health information can have serious consequences including refusal of prospective employment, difficulties in obtaining or continuing insurance contracts and loans, ostracisation from family and community groups and personal embarrassment. Once information has been disclosed, the damage cannot be undone so, to earn consumer trust it is important that unauthorised disclosure is prevented, not merely detected after the fact through audit processes. Broad consumer support for electronic health records will be predicated on a justifiable and well founded trust that the system will protect their highly sensitive health information in accordance with the consent that they are entitled to give or withhold. This includes accommodating the needs of consumers with especially demanding privacy requirements, e.g. persons receiving treatment for sensitive conditions (HIV/AIDS, addiction, psychiatric illness etc.), health care professionals receiving treatment and celebrities. If health information networks are to be adopted and supported by consumers, their privacy concerns must be addressed.

1.2 Overview of the Paper

Section 2 examines access control requirements in distributed health care information systems, focusing on the types of access policy expression that need to be supported. Section 3 describes the basic concepts underlying Role Based Access Control (RBAC) and highlights why it is well suited for health care information systems. Section 4 reviews related work. In Section 5 a shortcoming of RBAC is presented that limits its ability to support the required types of

\footnote{An electronic health information network aims to connect a broad range of organisations involved in delivering health related services. The network is used to collect, store and exchange personal health information. Examples include the national HealthConnect network currently under development in Australia (http://www.health.gov.au/healthconnect/) and the National Health Service Network in the United Kingdom (http://www.nhsia.nhs.uk/).}