Available online at www.sciencedirect.com

SCIENCE DIRECT®

Future Generation Computer Systems 22 (2006) 547–570

FGCS
FUTURE GENERATION COMPUTER SYSTEMS

www.elsevier.com/locate/fgcs

Securing web services for deployment in health grids

D.J. Power*, E.A. Politou, M.A. Slaymaker, A.C. Simpson

Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford, Oxfordshire OX1 3QD, UK

Received 7 March 2005; received in revised form 13 September 2005; accepted 16 September 2005
Available online 25 October 2005

Abstract

In this paper we describe an approach to the facilitation of system-wide security that enables fine-grained access control within systems in which third party web services are deployed. The primary motivation for the work comes from the authors' research into the development of grid-enabled healthcare systems (or *health grids*). Indeed, we would argue that if the e-Health dream is to become reality, then there is a clear need for web services that enable remote access to medical data to be secured in an appropriate fashion. We compare our approach of wrapping web services with alternative approaches based on generic SOAP proxies. As an illustrative example we describe how the OGSA-DAI grid services have been secured via XACML-based access control policies.

Keywords: Security; Healthcare; Web services; Access control; Medical informatics

1. Introduction

Securing web services is widely acknowledged as a challenging issue, with significant research having already been undertaken. In particular, security architectures have been proposed that attempt to fill the gap, with [1,2] being pertinent examples. Of particular relevance is WS-Security [3], which is an OASIS standard that facilitates the description of security mechanisms with a view to providing, for example, integrity and confidentiality of messages used in web services. These mechanisms are not, however, the full story: they are simply the foundations that can be used – together with other technologies – to provide security.

Within the United Kingdom, the e-Science Programme has driven the adoption of web service- and grid-based technologies for the facilitation of large scale science. Within the field of e-Health the intention is that such tech-

* Corresponding author. Tel.: +44 1865283670; fax: +44 1865283531.
E-mail addresses: David.Power@comlab.ox.ac.uk (D.J. Power), Eugenia.Politou@comlab.ox.ac.uk (E.A. Politou), Mark.Slaymaker@comlab.ox.ac.uk (M.A. Slaymaker), Andrew.Simpson@comlab.ox.ac.uk (A.C. Simpson).

0167-739X/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2005.09.003

nologies will not only support medical scientists, but also, in the longer term, the provision of healthcare delivery. Digital Mammography National Database (eDiaMoND) [4] is one example of such a project: as well as being concerned with developing an archive of annotated mammograms to support researchers, the system was developed in such a way that it is sympathetic to the work practices employed within the UK's Breast Screening Programme. As such, the requirements of both healthcare researchers and practitioners have had a significant impact upon system development.

Ensuring security and confidentiality is, of course, a crucial issue within the field of e-Health, with confidentiality and data protection being fundamental requirements. Furthermore, in the United Kingdom any access to medical data must be in accordance with the Data Protection Act [5] and the Caldicott Principles [6].

The motivation for the work described in this paper comes from the authors' contribution to the eDiaMoND project. In particular, the current authors have had key responsibility for the database design [7] and security [8] aspects of that project.

The focus of this paper is the description of a generic approach to the securing of web services. Although the work was originally motivated by e-Health in general and the eDiaMoND project in particular, we would argue that the approach described is applicable to applications beyond the healthcare domain. In particular, we take into account the fact that the service that we would like to secure will often be provided by a third party vendor. As a result, a key requirement for the approach is that it should be sufficiently generic, extensible and adaptable.

An ideal architecture based on these requirements would be to create a secure access service to act as a gatekeeper for the web service that we would like to secure. This access service itself would be a web service, and a part of an overall system that has consistent mechanisms for authentication, secure message passing and access control. In this paper we outline how such a secure access service can be constructed, and show how to overcome some common problems that are encountered when constructing such a service for use in a health grid.

The structure of the remainder of this paper is as follows. In Section 2, we present the motivation for the work described in this paper. Then, in Section 3, we introduce those basic concepts of web services that are relevant to the work described in the paper. In Section 4, we describe our proposed solution. Next, in Section 5, we present an illustrative example of our approach based on the eDiaMoND project. Then, in Section 6, we discuss the relevance of XACML to our example. Next, in Section 7, we provide an example of our approach by demonstrating how it has been used to secure OGSA-DAI Grid Services. Finally, in Section 8 we discuss the contribution of this paper and outline some potential areas of future work.

2. Motivation

The fundamental goal of eDiaMoND was to develop a prototype for a national database of mammograms – together with some demonstrator applications – that is sympathetic to the work practices of the United Kingdom's NHS Breast Screening Programme (BSP).

Within the eDiaMoND architecture, data is stored at a number of different sites, all of which are legally and ethically responsible for their own data. However, in certain circumstances – with teleradiology and remote working being examples – these sites may wish to share data with particular individuals from remote institutions at particular times in a controlled fashion. Thus, the facilitation of distributed queries in a secure fashion in accordance with fine-grained, flexible access control policies is a desirable requirement of such a system. The work described in this paper represents steps towards the achievement of that goal. A more detailed discussion of these issues is provided in [9,10].

The core eDiaMoND system consists of middleware and a virtualised medical image store to support the concept of a data grid. The virtualised medical image store comprises physical databases, with each being owned and managed by a different organisation. (If we were to think of a potentially deployed system, then the term *organisation* could be replaced by *Breast Care Unit (BCU)*.) The eDiaMoND grid is formed by participating organisations coming