MEDINFO 2007
HISA Ltd Australia
© 2007 The authors. All rights reserved.

The iAccess Handbook: A Methodology for Access Control Integration

Per Håkon Meland[a], Lillian Røstad[b], Inger Anne Tøndel[a], Øystein Nytrø[b]

[a] *SINTEF, Software Engineering, Safety and Security, Norway*
[b] *Department of Computer and Information Science, NTNU, Norway*

Abstract

Health care information about a patient is usually scattered among several clinical systems - potentially more than a hundred separate systems just within one hospital. System integration and interoperability is difficult to achieve, and various strategies for integration exist. However, one topic that has not received much attention is how to integrate system specific security mechanisms such as access control. This paper presents the iAccess handbook, which is a tool to aid this process. It consists of a repository of reference information and a set of methods for collecting information and presenting results, and concerns the legal, organizational and technological aspects of integrated access control for health information systems. The methods have been applied on two separate integration efforts in Norway.

Keywords:

access to information, information protection, computer security, medical records

Introduction

In this paper we present the iAccess (*Integrated Access Control for Health Care Information Systems*) handbook which is a tool to be used during planning, designing and describing access control for integrated health care solutions. The handbook consists of a repository of reference information and a set of methods for collecting information and presenting results.

The methods have been applied on two separate integration efforts in Norway.

Methods and results

The iAccess handbook

The purpose of the iAccess handbook is to serve as a collection of information and methods that are useful and appropriate when integrating the access control of heterogeneous health care information systems. The handbook itself is web-based, and both readable and editable for registered users, such as people from health care organizations, researchers and students (doctoral fellows primarily). The handbook has been created using the free MediaWiki software package[1], which allows easy publication and development of content in a collaborative setting. The following sections will briefly explain the main contents from each of the three parts of the handbook.

Handbook part 1: Reference information

For the reference part of the iAccess handbook, we have borrowed the concept of viewpoints from the software architecture field - specifically from *IEEE 1471-2000 Recommended Practice for Architectural Description of Software-Intensive Systems* [1]. We have defined three viewpoints; *legal, organizational and technical*. These viewpoints were selected in recognition of the fact that access control is not merely a technical issue. Organizational measures are important in enforcing access control and ensuring patient privacy. The legislation defines *if*, *how* and *when* sharing of sensitive health information can take place.

Handbook part 2: Survey methods

This part of the handbook defines a set of survey methods, and we will here briefly present the main ones and discuss our experiences with them.

Study of documentation

From studying documentation you can learn a lot about an organization and/or a system that will be useful when working with access control integration, and also for planning workshops and interviews (see the following sections). There are certain kinds of documentation with relevance for access control, which should be present in a health care organization, and we recommend focusing on the following: organizational information security policies, organizational structure - including roles and responsibilities for information security, organization-level access control policy, strategies - for instance integration strategy, high-level system documentation, description of implementation and use of access control mechanisms, requirements with respect to identification, authentication and authorization, risk analysis based on system security and patient safety.

Different organizations have different types of documentation. The results from a documentation study greatly depend on the organizations studied. It can be just as interesting to see what kind of documentation exists, as to study

1 MediaWiki is a free software wiki package originally written for Wikipedia, see http://www.mediawiki.org.

the actual content. If the anticipated documentation does not exist, asking for it still serves a purpose by making the organization aware of what information could be expected to be present.

Process workshops

Our process workshop is based on the methodology defined by Dingsøyr et al in [2]. The purpose of the process workshop is to get input from a heterogeneous group of people that are involved in a given process. In other words: While documentation can provide information about how something is supposed to be done - the process workshop conveys information about how it is actually done.

During a process workshop, the participants are presented a scenario, and then each one writes down keywords related to activities, participating roles, documentation and tools that are used to solve the scenario. This is done in the same way as a traditional brainstorming session. After this, the workshop participants gather around a process map and eliminate/add/reorganize the notes on the map until they have reached a version of the process description that they can all agree upon, as shown in Figure 1.

Semi-structured interviews

Semi-structured interviews [3] are used to gather detailed information to complement and elaborate the process descriptions obtained in the workshops. This is be done by using a set of pre-defined questions (an interview guide), but allowing the interviewees to answer freely - there are no categories to select from and the interviewees are allowed to ask questions. An interview guide should start by explaining the interview motivation, and briefly explain the relevant terms. The interview guide should be based on the process maps.

Handbook part 3: Combining and presenting results

This part of the handbook describes how to combine and present the results from the survey methods. The most promising technique is the use of an extended version of UML[2] activity diagrams for modeling the process descriptions and information related to processes. An UML activity diagrams is well suited for describing processes and activities, both related to human and system behavior, because of a visual organization that is easily understandable by most people.

Discussion

The original reason for creating the iAccess handbook was to have an instrument for surveying and documenting real-life access control integration efforts of health care systems in Norway.

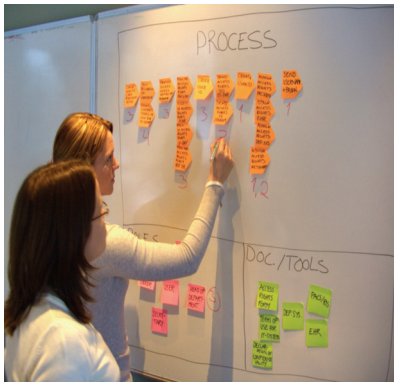

Figure 1 - Creating the process map by using sticky notes and active discussions

The results so far have mainly been used by the health care organizations themselves and by doctoral fellows researching how technical, legal and organization challenges should be solved. A survey gives a snapshot of today's situation, what has improved from the past and what is planned in the near and distant future. Just as interesting, some improvements may be negative for the majority of the users, and it is important to share that kind of information with the rest of the community in order to avoid reoccurrence.

Conclusion

We have presented the iAccess handbook, which consists of three parts relevant for analyzing planned or existing efforts for access control integration for health care systems. Representing multiple views from various stakeholders in unified diagrams eases the understanding on how things are and what should be done. The methods in this paper are first and foremost qualitative, and our future work will add methods that provide more quantitative results.

References

[1] IEEE Std 1471-2000 IEEE Recommended Practice for Architectural Description of Software-Intensive Systems: IEEE; 2000.

[2] Dingsøyr T, Moe NB. The Process Workshop: A Tool to Define Electronic Process Guides in Small Software Companies. In: The Australian Software Engineering Conference; 2004 13-16 April; Melbourne, Australia: IEEE Computer Society Press; 2004. p. 350-357.

[3] Fontana A, Frey JH. Interviewing: The Art of Science. In: Norman K. Denzin YSL, editor. Handbook of Qualitative Research. 2nd edition ed: SAGE Publications; 2000. p. 361-376.

2 The Unified Modeling Language, see http://www.uml.org