Quality of Life through Quality of Information
J. Mantas et al. (Eds.)
IOS Press, 2012

doi:10.3233/978-1-61499-101-4-756

Towards Human-Centric Visual Access Control for Clinical Data Management

Sascha FAHL[1a], Marian HARBACH[a] and Matthew SMITH[a]
[a]*Leibniz University Hannover, Distributed Computing & Security Group, Germany*

Abstract. We propose a novel human-centric, visual, and context-aware access control (AC) system for distributed clinical data management and health information systems. Human-centricity in this context means that medical staff should be able to configure AC rules, both in a timesaving and reliable manner. Since medical data often includes (meta-) information about a patient, it is essential that an AC system includes the patient into the AC process. To cater for the strong security needs in the medical domain, both the AC policy creation by medical staff as well as the patient-interaction feature need to be taken into account. While traditional AC systems offer sufficient security in theory, they lack in comfort and flexibility and as a result find no widespread acceptance with non tech-savvy users. Distributed medical institutions could enormously benefit from the opportunity of dynamic AC configuration at an end-user level while adhering to legal, ethical or other privacy requirements. Hence, this paper presents a human-centric visual AC model for medical data, addressing usability, information security and patient interaction.

Keywords. Health Information Systems, Clinical Data and Object Management, Visual Access Control, Usable Security

Introduction

With the integration of IT systems in healthcare, medical data is stored in picture archiving and communication systems (PACS). Those systems store medically relevant data as well as corresponding meta-data and provide an interface to access the information. This patient-related data needs to be protected from unauthorised disclosure and is protected by national legislation in many countries (e.g. HIPAA). Therefore, the available solutions use AC mechanisms to appropriately regulate access to medical data. Usually RBAC [1] or other MAC [2] based systems are applied. While both paradigms provide sufficient security in theory, they do lack good usability. Every access privilege configuration requires a security administrator to intervene and can hardly be configured by non-tech-savvy medical staff. This introduces delays, which clearly interfere with the often time-critical work in the medical environment. The DAC [3] concept, allows the configuration of access privileges at the end-user level on the one hand, but on the other hand can hardly enforce organisational or legal policies.

In addition to strict legal and ethical frameworks, medical information has another important security requirement. Since patient information is included in medical data, AC configuration should not be solely put at the physician's discretion. Instead, the

[1] Corresponding Author: Sascha Fahl, Leibniz University Hannover, Schlosswender Str. 5, 30159 Hannover, Germany; Email: fahl@dcsec.uni-hannover.de.

patient should be involved in and interact with the AC process to have the final say on who should be granted access to the patient's data. Hence, we propose a combination of MAC and DAC features to provide flexibility as effectively as possible and finally integrate the patient to respect his privacy needs whenever feasible.

Independent of the infrastructure – centrally in one or distributed between multiple medical institutions – AC configurations in medical scenarios might become very complex and confusing [4].

Hence, to meet the requirements of a usable AC framework as described previously, we think the following features should be provided:

- Guarantee the compliance with legal, ethical or institution wide data and meta-data access policies;
- Enable medical staff to configure access privileges;
- Integrate patients into the access control process of their data and meta-data;
- Comfortably support the configuration of access control in a multi-domain environment;
- Enable medical staff to request access to data and meta-data.

A usable AC system that respects the just mentioned requirements would enormously simplify the secure deployment of clinical information management. Medical staff would benefit from timesaving workflows while strict privacy policies for medical data could be automatically adhered to. In [5], we introduced a new visual AC concept for research ecosystems, called MindMesh. It proposes to model access privileges visually and uses context information for AC configurations. Since this concept supports distributed and dynamic environments, it is suitable for improving collaboration and data sharing in medical systems. Semantic Web-based inference mechanisms can be applied to implicitly configure AC policies from the context available in the system. While the MindMesh approach offers a high level of usability and flexibility, all AC modelling competencies of a single user are strictly framed by institution-wide (global) policies. Hence, MindMesh concept combines the flexibility of DAC with the security of MAC systems while focusing on usability by design.

In this paper we describe an extension of the MindMesh concept for medical applications. Furthermore we implemented a prototype for the DCM4CHE [6] open source system.

The rest of this paper is organised as follows: The next Section outlines a sample scenario of the MindMesh access control framework in medical scenarios. Section 2 introduces the MindMesh concept and the extension for the medical domain. The last Section concludes the paper.

1. Scenario

One scenario of main interest is the configuration of ad-hoc and short-lived collaborations between multiple distributed medical centres (MCs). For example, X-ray images in form of DICOM files are used for diagnostic purposes. After they are stored in a PACS system, the data is locally available at the MC where the images were captured. During a diagnostic process, a physician in MC A might need to consult with a specialist for clarification of an uncertainty. Since this specialist might work in a different MC B, granting him access to the relevant data can be rather laborious. Currently, a patient often needs to physically take the pictures to the specialist. Yet, an

IT-based solution would currently have the need of an administrator to manually configure the AC system regarding the demands. The case of consulting with a specialist is a temporally limited occasion and hence access to the corresponding data should only be granted for as little time as possible. After the consultation is finished, access for the external physician should be denied. Traditionally, the removal of that access privilege once more requires the intervention of an administrator. Since there is little motivation for the removal of access privileges – because this does not help medical staff to get their job done – access to sensitive data is often granted for a longer period of time than strictly necessary. Security holes and the violation of privacy policies are the result. Having an AC system similar to the MindMesh at hand, a physician at MC A could drag and drop a physician of MC B onto the required patient data in order to give him access for a joint diagnosis. Using that new policy, the patient-interaction procedure as described in the second scenario would be triggered. In case of a positive patient response, both physicians can collaboratively examine the medical data. After a certain timespan, the temporal access privilege automatically expires and access for the external physician is denied for future requests.

2. MindMesh in the Medical Domain

In allusion to Mind Maps, the MindMesh approach focuses on the intuitive visualisation of organisational structures, the interconnection of different organisations and a visual representation of AC concepts. In this paper we adapt the original MindMesh idea to the needs of clinical data and object management in a distributed and collaborative environment.

The MindMesh extends the Mind Map concept and models information in a graph structure and allows arbitrary relationships between any two entities, while preserving the usage and interaction patterns of the Mind Map paradigm. Adding explicit semantics and concept definitions in ontologies, the MindMesh effectively is a semantic network. Obviously, such a structure is suitable to capture information concerning the medical landscape, such as medical centres, wards, physicians, nurses and relationships between the different entities.

However, using a graph clearly poses a challenge for visualisation, especially for non-ICT natives such as medical staff members. Any visualisation layout has to capture the essence of the contextual situation. Figure 1 shows an exemplary MindMesh graph for a medical infrastructure. Even with the non-optimised graph layout, one can already gain an understanding of the medical centres' organisation and which links exist. However more importantly, the software allows the user to explore the structures by zooming in on certain parts as well as adaptively hiding and highlighting certain properties. This gives the opportunity to zoom in from a coarse-grained outline of the complete infrastructure to a detailed view of the physicians and nurses of a single ward in a medical centre. In addition to exploring the infrastructure and certain EHRs, a search interface enables an alternative way of access to information of interest.

To increase the intuition of the visualisation layout, semantic information from the underlying ontology is used to create supporting layout substructures. For example in a medical centre context, we can assume that there is some sort of hierarchy in organisational structures. Hence, certain links representing these hierarchical structures can be sublayouted as a tree. Additionally, the granularity of the view can be adapted to the context of the task.

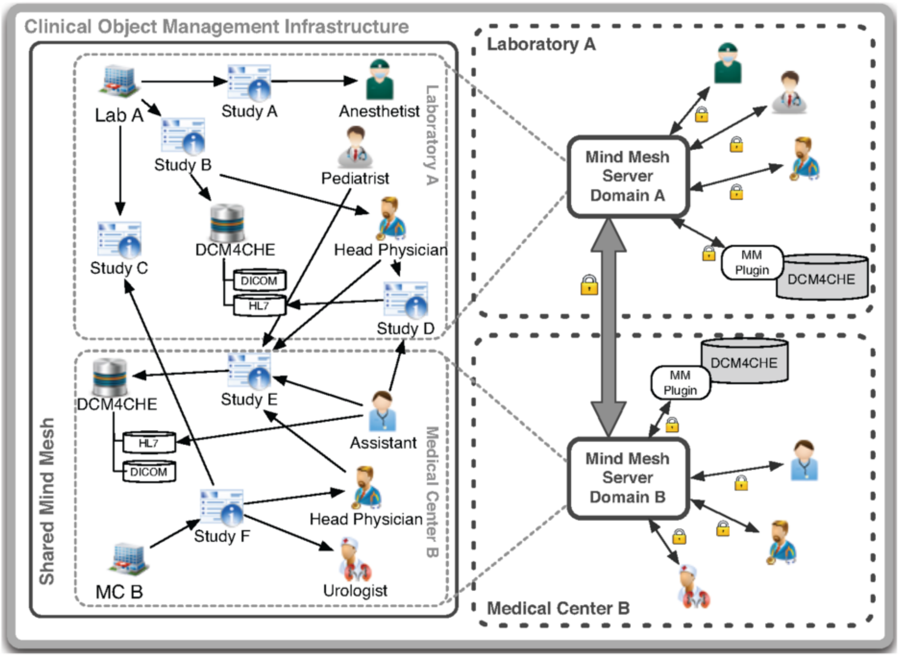

Figure 1. The proposed architecture, exemplarily shown for a laboratory and a medical centre sharing a MindMesh graph. Each domain maintains its own PACS and a local MindMesh server. The left hand side illustrates the structural organisation of each domain and interconnections between studies and physicians.

For instance, if the user wants to gain an overview, similar nodes such as all medical staff of an institution can be clustered and only displayed abstractly. Another example would be the exploration of EHRs that can be mapped to a single patient. Anything except the patient and his EHRs can be faded out. The patient is located in the centre of the screen and all his EHRs are arranged in a star like layout.

The applicability of multiple context-aware instead of a single generic graph layout algorithm for complex networks has been demonstrated in the area of Semantic Web.

To facilitate the integration of legacy systems, MindMesh plugins link resources with the MindMesh Plugins for DCM4CHE can provide information on for instance the available DICOM images stored on this server. The MindMesh user that primarily is medical staff in this scenario can then see how resources are organised in the context of the participating medical institutions.

2.1. Policy Governance

To increase security of the highly sensitive medical data, medical staff should not be allowed to arbitrarily create AC policies. Rather, the policy creation process needs to be controlled by higher instances. An example of such a governing catalogue of policies is the HIPAA.

Instead of applying known delegation mechanisms such as attribute-based AC that allow for the delegation of one's privileges to a third party, our solution works with meta AC policies instead. Our meta AC approach controls the user-driven creation of resource AC policies. In case a physician intends to add a new policy concerning some medical information (e.g. giving a colleague access for a collaborative diagnosis), the system's meta AC policies first check if the intended policy is allowed to be created.

2.2. User Interaction

In addition to policy governance, a second extension to the MindMesh concept is a patient interaction feature within the policy creation process. Each time a new medical data item is added to a PACS the patient should be asked what interaction procedure he wishes to apply for the certain medical data item. A patient may choose between the procedures **Local**, **Permissive**, **Permissive-Informed** and **Control** as described in the second scenario. While the Local and Permissive procedures result in no further patient interactions for future AC configurations, the Permissive-Informed and Control procedures require patient-interaction for every new AC configuration. To increase usability, the policy creation request should to be explained to the patient in an intuitive way.

The patient should be able to verify who sent the policy creation request and which users will have access to the given EHR if the request is approved. In case a single user is granted access, his name and the institute he works for can be displayed. In case the policy specifies multiple users, a coarse grained overview is given by extrapolating the most characteristic attributes (e.g. a policy says that all heart specialists from a particular medical centre are granted access).

3. Conclusion

In this paper we presented a novel visual and context-aware user-centric access control concept for medical data and object management databases. Several key contributions were made: We identified why traditional central data and object management approaches fall short of fulfilling the requirements of short-lived collaborative access control configuration in the medical landscape. Our approach integrates the DCM4CHE system into the MindMesh to demonstrate how the daily workflow of medical staff can benefit from an intuitive AC system allowing the creation of short-lived collaborations between users of different organisations. To respect a patient's privacy needs, we proposed a patient-interaction framework that allows patients to choose different levels of data privacy for their medical data. Patients can choose from very restrictive to very permissive to controlling policies and have the security of their medical data in the hands.

References

[1] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based Access Control Models. Computer 1996; 29: 38-47.

[2] Sandhu RS. Latice-based Access Control Models. Computer; 1993; 26: 9-19.

[3] Loscocco PA, Smalley SD, Muckelbauerand PA, Taylor RC, Turner SJ, Farrell JF. The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments. Proceedings of the 21st National Information Systems Security Conference; 1998; 303-314

[4] Yuqing S, Wang Q, Ninghui L, Elisa B, Mikhail A. On the Complexity of Authorization in RBAC under Qualification and Security Constraints. IEEE Transactions on Dependable and Secure Computing; 2011; 8 (6): 883-897

[5] Harbach M, Smith M. Visual Access Control for Research Ecosystems. 5th IEEE International Conference on Digital Ecosystems and Technologies. 2011.

[6] www.dcm4che.org (Last Accessed 23.01.2011)