A Risk-Based Evaluation of Group Access Control Approaches in a Healthcare Setting

Maria Line, Inger Tøndel, Erlend Gjære

To cite this version:

Maria Line, Inger Tøndel, Erlend Gjære. A Risk-Based Evaluation of Group Access Control Approaches in a Healthcare Setting. 1st Availability, Reliability and Security (CD-ARES), Aug 2011, Vienna, Austria. pp.26-37, 10.1007/978-3-642-23300-5_3 . hal-01590398

HAL Id: hal-01590398
https://hal.inria.fr/hal-01590398

Submitted on 19 Sep 2017

A Risk-based Evaluation of Group Access Control Approaches in a Healthcare Setting

Maria B. Line, Inger Anne Tøndel, Erlend Andreas Gjære

SINTEF ICT, Trondheim, Norway
{maria.b.line, inger.a.tondel, erlend.andreas.gjare}@sintef.no

Abstract. This paper focuses on access control approaches usable for information sharing through large screens where several individuals are present at the same time. Access control in this setting is quite different from traditional systems where a user logs on to the system. The paper outlines a number of possible approaches to access control, and evaluates them based on criteria derived from risk analyses of a planned coordination system for the perioperative hospital environment. It concludes that future work should focus on extending the location-based approach with situation awareness, and add support for using pop-ups or handheld devices for sharing of the most sensitive information.

Keywords: Access control, privacy, health care, information security

1 Introduction

There are a number of systems available whose main purpose is to inform the public about status and status changes. Examples are screens showing incoming flights at airports, or overviews of meeting room occupancy at hotels. In these example systems the information on the screen is unlikely to be sensitive, and thus there is no need to control information visualization. But imagine such information displays being used in healthcare or in other businesses where some status information should be considered internal.

In this paper we focus on access control solutions for wall-mounted screens that show status information in a perioperative hospital environment (before, during and after surgery). This environment is characterized by multidisciplinary teams, the need to react to unanticipated events, and utilization of expensive resources. Planning and coordination are difficult but important in such a setting [1]. To improve coordination, wall-mounted screens visualizing progress and current status can be placed at waiting rooms, wards, operating rooms, recovery rooms etc. where health care personnel is likely to see them. As a result it becomes easier to understand how the patient care is progressing and adapt own behaviour.

Access control in systems communicating via large public wall-mounted displays is quite different from traditional access control where a single user logs on to a system. First, it is difficult to know at a given point of time who is able to view the information on screen. In the perioperative environment, there can be a number of health care personnel having access to the location of a screen, in addition to patients, their next-of-kin, and other types of personnel such as cleaners or technicians. Still, if we were able to know who were present, it is not a straight-forward task to determine how this knowledge should affect what information to display. Access policies are normally defined on a single-user level, while the coordination system may just as well have none or several users to consider in its decisions on what to display. Second, the information - though it may be sensitive - is displayed because it is needed for a purpose. What to display in a given situation must be based on proper trade-off decisions between privacy on one hand and efficiency and patient safety on the other. This calls for access control solutions that are dynamic and context-aware, and that fit the way of work in the perioperative domain. To further complicate matters, there is in general no time for users to login to the system, as information should be available by just by taking a quick look at the screen.

In our previous work [1] we have decided on a strategy in order to overcome these challenges, termed flexible de-identification. With *flexible* we mean that decisions on what to display should not be static but adapted to the situation and current context. *De-identification* leads to solutions that go beyond the more traditional consideration of whether to display identifying information or not. Instead we assume that information needs not be at the highest level of granularity to be useful for coordination purposes.

In this paper we focus on providing flexible access control, while de-identification is left out[1]. We do not consider access to information by single users, but instead how to determine access rights for a dynamically changing group of individuals. This group is likely to consist of personnel with different professions and different needs and rights for information, who - though they work together - will have different opinions as to what information gives meaning and is useful. We present several approaches to access control in this setting. Our main contribution is a preliminary evaluation of these approaches based on criteria derived from a risk analysis of a the COSTT system[2] - a planned coordination system for the perioperative hospital environment.

The paper is organized as follows: Section 2 outlines relevant approaches for access control. Section 3 explains the method used to perform the risk analyses and to deduce evaluation criteria. Section 4 gives the results of the risk analyses, explains the evaluation criteria and applies them in order to evaluate the different access control approaches. Section 5 discusses the validity of the evaluation result, and suggests directions for future research, before section 6 presents our concluding remarks.

[1] See Gjære et al. [2] for more information on de-identification solutions for this kind of systems.

[2] Developed by the Co-operation Support Through Transparency (COSTT) research project. http://www.costt.no

2 Relevant Approaches to Access Control

Access control related to shared disiplays have been given some attention from researchers, and proposed solutions include using special types of glasses to allow different people to see different types of information [3] and using visualizations (e.g. colors) instead of text to present the most sensitive information [4] (similar to our de-identification approach). Available research on how to determine access rights of dynamically changing groups of users is however sparse. We are only aware of one publication [5] that addresses this issue to some extent. This publication lists three different approaches that can be used in combination. The first approach is *aggregation* where the access rights of a group correspond to the sum of the access rights of the individuals in the group. As a result, larger groups are likely to get access to more resources than smaller groups. The second approach is *maximum/minimum* where the individual with the highest/lowest access rights determines access rights for the whole group. Third, the *group structure* approach computes access rights based on the structure of the group, e.g. ensures that at least two users with a certain access level are needed in order to gain access to a specific resource.

Current access control solutions developed for healthcare are mainly based on Role Based Access Control [6] where users are granted access based on their profession [7][8]. A study of an up-and-running Electronic Patient Record system at a Norwegian hospital [9] identified the need for access control solutions more tailored to the needs of health care personnel. Solutions should be better able to handle dynamic events, workflow and collaboration.

Dynamic context-aware access control solutions have been suggested in various forms, some also specifically addressing health care (e.g. Hu et al. [10]). We will not go into specifics on the different models, but rather point to parameters that can be used when creating more dynamic access control solutions in a health care setting. Hu et al. mention time, location, trust-level of authentication, relationship to patient, and specialist area. Most of these are also mentioned by Alam et al. [11], who add device type, duration, purpose, number of accesses, user consent, presence of the patient, delegation and emergency situations to the list. Risk and benefit are also factors that can be taken into account in access control decisions. Examples of access control solutions that include the concept of risk is the work of Cheng et al. [12], Dimmock et al. [13] and Diep et al. [14].

Below we present the main access control approaches considered in this paper. It is assumed that we have technology available for authenticating and locating users[3].

Location-based: Only the screen's location applies, which means that all screens have a given default view that can not be affected by persons being present. Access control to the screen is managed through physical access control; people being allowed to be at a certain location are also allowed to see all information displayed on the screen at the given location.

[3] The purpose of locating users will NOT be surveillance of all their movements and actions.

Minimum [5]: A group's access rights will correspond to the lowest level of access rights present in the group. This will clearly ensure patients' privacy, as nobody in the group will see more information than they are allowed to. However, the usefulness may be low, as the persons with higher levels of access rights will not always see all information meant for them.

Maximum [5]: A group's access rights will correspond to the highest level of access rights present in the group. This will ensure usefulness, as all health care workers will see all the information meant for them. However, the patient's privacy may be compromised.

Group structure [5]: The access level is decided by computations on the group structure. An average value is calculated based on who is present, including weighting of who is closest to the screen and considerations of how many is present with limited access rights vs. wide access rights.

Facilitator: One of the users in the group acts as a facilitator. The facilitator is authenticated, and makes decisions as to whether to include new users into the group and which information is needed/appropriate based on the users present.

Situation aware: The system is aware of the situation in which it operates, e.g. it combines information on type of patient and diagnosis with time of day and an understanding of whether this is an emergency or normal operation. Situational awareness is then used to decide access rights of the group.

Possible extensions: Pop-up window and handheld devices: All the suggested approaches can be extended with solutions that grant individual users access to more information. This can be done by utilizing small pop-up windows where e.g. surgeons can authenticate themselves and get access to more details shown in a limited part of the screen, or get the information sent to a handheld device. Getting access to information in a pop-up window limits the reading access for other people being within proximity, information is only readable for the one/those standing really close to the screen. Sending information to a handheld device further reduces the risk of confidentiality breaches.

3 Method

In this work, we use the results of two risk analyses of the planned COSTT system to identify criteria that the access control solution need to fulfil, and use these criteria to evaluate and compare the alternative access control approaches. The main motivation for using risk analysis in this respect is twofold. First, the results of the risk analyses are already available and provide valuable insight into the environment in which the access control solution will be put to use. Second, access control aims to protect (some of) the system assets by reducing risks, but may also introduce new risks. Performing a risk analysis is a good way to identify both the assets and the risks towards these assets. We recognise that using risk analysis of systems to evaluate access control policies is uncommon. Still, we uphold that the results of a risk analysis are useful for performing a preliminary evaluation of alternatives in order to decide which should be further investigated and evaluated.

Two risk analyses have been performed, and both were carried out in two stages: 1) Asset identification[4]: “What are the most valuable assets in the COSTT system? What do you want to protect?”, and 2) Risk identification and ranking: “What are the most important risks for COSTT? What are you most afraid of happening?”. In each stage the participants were given five minutes to write down their answers to the questions posed. Both stages were summarized by organizing the brainstorming results into groups that the participants agreed upon. The risk identification stage also included ranking of the risks. Each participant was given three votes they could use to prioritize risks. The risks were then ranked according to votes in total.

The COSTT project group was used as participants. Together they represent a broad spectrum of specialist areas; IT, sociology, medicine, and technology management. The first risk analysis was performed at the stage where the system itself existed only as a concept and many decisions that would affect the outcome had not been made yet. The purpose of this preliminary analysis was to get an initial sense of what are the key risks as perceived by the project team. The second risk analysis of the future COSTT system was performed 10 months after the first one. The system itself still existed only as a concept but some research, including literature studies and empirical studies, had been performed. The purpose this time was to see if the results would differ a lot from earlier, and to identify the major changes, if any.

4 Results

In this section we present the results of the risk analyses, and use these results as a basis for identifying evaluation criteria. Then we show to what extent the identified access control approaches are able to meet the criteria.

4.1 Results of the risk analyses

The findings from the first risk analysis represent a starting point and a snapshot of the project status at that point of time. The second risk analysis revealed the same results, but both broader and in more depth. One of the main differences, was the ranking of the risks related to sensitive information and access control; as the participants increased their understanding of what the COSTT system will be, they also increased their worries of sensitive information leakage, while they decreased their worry of the access control mechanisms not being strong enough. We choose to present the results from the latter only, because that is sufficient in order to cover all identified issues.

Table 1 presents all assets and risks identified. Note that the categories of assets and risks are not considered to be mutually exclusive. The participants themselves sorted the input from their brainstorming process and gave names to the categories of information. The assets mainly include types of information available in the system; both to be displayed on the screen and underlying

[4] Inspired by the asset identification method described by Jaatun and Tøndel [15].

Table 1. Identified assets and risks

Category	**Assets**
Patient information	Identification, medical data, secret relations, irrelevant health history
Employee information	Name, role, actions, personal data
Location data	Position for all tagged persons, info about rooms, movements
Aggregated/reasoned data	Efficiency of employees, process statistics, surveillance of procedures
Deviations	Unwanted incidents, info on operations, system errors in hospital
Usefulness	Utility value by using the COSTT system
Category	**Risks**
Poor quality of data (9)	Drawing wrong conclusions on what info means, inaccurate catching of events, misinterpretation of events, coordination trouble due to erroneous data, patient injury
Surveillance of employees (6)	Management monitoring efficiency of employees, wrong/incomplete statistics on employees, employees feel they are being monitored, public negative exposure of some employees
Sensitive personal information (6)	Info displayed to persons not concerned, deduction of patient having a sensitive diagnosis, unintended access to sensitive info, hacking/data theft, info is taken out from the hospital
Unintended/erroneous use (5)	Location tag theft, active bypassing of access control lists in other systems, bypassing physical access control, unhealthy changes in work processes, employees working against the system or refusing to use it, conflicts due to low efficiency
Patient (2)	Patients choosing a different hospital, theft of patient data, patient info known to public press
Access control (1)	Limitations hide important data when it should be available, bugs giving illegitimate access
Wrong focus (1)	Fussbudget, loss of efficiency, debates on prioritizing, critical questions due to insignificant errors
Relatives (0)	Creating unnecessary feelings, unhappy relatives calling frequently on health personnel
Public (0)	Negative newspaper headlines

information needed to make the system work properly. Also, parameters that can be deduced from information in the system are considered valuable assets. The risks span from concerns of the underlying sensors not being able to catch events to breaches of both patients' and employees' privacy. The numbers listed in parenthesis in the column of categories indicate the prioritizing done by the process participants. In the table, the risks are presented in prioritized order.

4.2 Identification of Evaluation Criteria

In the process of identifying evaluation criteria, we focused on the highest ranked risks. The criteria are referred to as C1, C2 etc., which constitutes a mapping to table 2 where they all are summed up.

Poor quality of data: The main risk was considered to be poor quality of data. As shown in table 1, this is mainly a concern about the underlying system not being able to catch and/or interpret events correctly. In the COSTT project, the coordination information that is to be displayed on the screens are built by capturing events in other information systems [16]. Simple events (e.g. access to the medical record of patient A by a given health care personnel) are combined into composite events (e.g. cardiology assesment of patient A has been performed), and it is these composite events that will be displayed on the screens. It is however important to be aware of the uncertainty involved in the event enrichment process. As an example, access to medical record of patient A can indicate that the health care personnel that accessed the record is performing an examination of the patient, but it can also be that the health care personnel is preparing for the examination. Thus, events in the COSTT system will be associated with a quality attribute that is a measure of the validity of the event [16]. This quality attribute should ideally influence the access control decision, as presenting information that is correct is an important part of the information security of any system (integrity). This is reflected by the data quality awareness criteria (C1).

Surveillance of employees: The next highest ranked risk was that of surveillance of employees. This covers the employees' fear of being monitored and the possibility for management to misuse registered data about their employees to measure efficiency or other statistics. Data registered for the purpose of COSTT may not give the complete and correct picture of employees' actions, which means that it should be used with high caution, if at all, for management purposes. Thus it is relevant to consider whether the solutions increase the need for surveillance, e.g. by requiring location information (C2). Employee surveillance is also related to what information is published on the screens (further addressed for the risk of sensitive personal information).

Sensitive personal information: The third highest ranked risk is that of displaying sensitive personal information in ways that makes the information available to unauthorised persons. It is important that solutions are able to maintain privacy of both patients and employees, and strive towards the ideal solution where everybody gets access to what they need - and no more. This is reflected by the privacy preserving criteria (C3).

Unintended/erroneous use: The risk related to sensitive personal information should also be considered together with the risk of unintended/erroneous use (rated fourth) and also the much lower prioritized risk related to access control. The concern that access control does not support the work flow is reflected in all these three risks. Failure in this respect can lead to active bypassing of access control due to important information not being available (C4). To meet this challenge it is important to consider dynamic and/or user controlled access control solutions that is able to fit into the way people work. It is also important to consider the effort required from users in order to use the systems in a secure manner (C5), as expectations on user involvement may require changes in work processes in itself in addition to requiring time and effort from the users. This

Table 2. Identified criteria based on risk analysis

Nr	**Criteria**	**Explanation**
C1	Data quality awareness	The ability of the solution to take the data quality into account in the access control decisions.
C2	Minimisation of employee surveillance	The need for use of employee surveillance techniques, e.g. for monitoring the location of employees.
C3	Privacy preservation	The ability to restrict sensitive/private information to those that are authorized for access.
C4	Availability ensurance	The ability to ensure that information important for safe and efficient treatment of patients are available when needed. This can e.g. be ensured by using dynamic approaches able to adapt to the situation , or to ensure that users can override the access control decision.
C5	Workload reduction	The ease of use for users. Solutions that rely on user cooperation will require some time and effort on behalf of the users.
C6	Complexity	The more complex the access control mechanism is the higher risk of mistakes that may render the access control solution vulnerable.

Table 3. Evaluation of access control approaches with respect to the selected criteria

Approach	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**
	qual.	surv.	priv.	avail.	workl.	compl.
Location-based	-	+	?	?	+	+
Minimum	-	-	+	-	+*	+
Maximum	-	-	- -	+	+*	+
Group structure	-	-	?	?	+*	-
Facilitator	-	+	-/+	+	-	+
Situation aware	?	+	?	?	+	-
Extension: Pop-up/handheld	-	-/+	+	+	-	+

influences the perceived system efficiency and is likely to have an impact on the employees' attitudes towards the system; employees working against the system or refusing to use it. Risks related to access control can also increase with complexity (C6). With complex access control solutions it is easier to make mistakes e.g. during implementation or during policy specification.

4.3 Evaluation of access control approaches

Table 3 summarises the evaluation of the suggested access control approaches with respect to the evaluation criteria. A '+' indicates a positive score while a '-' indicate a negative score. A score of '-/+' indicates that the approach is able to meet the criteria to some extent, but not fully. A '?' is used in situations where the evaluation result will depend on trade-offs made when defining access control policies. A '*' is used to illustrate that the score depends on the mechanism used to determine who is present.

The *location-based* approach is in many ways the most simple approach. Its ability to meet the needs of COSTT is however dependent on how easy it is to determine beforehand which information should be available in given locations. As several of the envisioned locations (e.g. corridors and examination rooms) are likely to be accessed by a number of different groups of users, we envision that it will be difficult to make such pre-set trade-offs that are able to meet the criteria for both privacy and availability.

The *minimum* approach is unlikely to meet the availability requirements of the users in need for most information. The same way, the *maximum* approach will probably result in too many privacy breaches, as everybody will get access to whatever information should be available to the one present with the highest access rights. Considering group structure is likely to perform better than using the minimum/maximum access rights, but is complex and its success depends on the ability to make proper trade-offs between the access rights of the highest and lowest ranked users present.

Relying on a *facilitator* seems to be a solution that could fit COSTT well, as it is able to meet the majority of criteria to some extent. The privacy achieved will be dependent on whether we can trust the facilitator to make good decisions as to what information to display in given situations. In a study of clinicians' experiences related to privacy and security of health information systems [17] Fernando and Dawson noticed that most clinicians used measures such as lowering their voices and omitting to ask relevant questions in order to protect privacy and security when residing in a shared workplace. At the same time they found that privacy and security implementations on electronic health information systems often took time from patient care, and were therefore considered to hamper patient care. Sharing of passwords was mentioned in this study, as well as in a study by Vaast [18]. In his study he also found that physicians were concerned that employees on wards were overwhelmed with work and therefore were likely to forget to close programs or patient charts. To be able to reach a conclusion as to whether the facilitator approach is adequate in the COSTT setting, more research is needed on the situation in which the COSTT system will operate when it comes to the work process and the general attitude of the employees.

Making the access control solution more *situation aware* is also likely to improve the trade-off between privacy and availability, but at the cost of complexity. This is the only approach that has the potential to meet the data quality awareness criterium.

The *pop-up/handheld extension* also seems promising, and is able to meet the majority of criteria. By implementing this extension one is able to introduce more flexibility and user involvement without sacrificing privacy. It should however not be used as the only approach.

To sum up, none of the access control approaches studied is able to meet all evaluation criteria. However, the ones that seem most promising are either using the facilitator role or using an access control solution that is situation aware. Alternatively, one of the more simple automatic approaches, e.g. the location-based approach, can be combined with the pop-up/handheld extension.

5 Discussion

The preliminary evaluation performed is based on a risk analysis of the COSTT system at an early stage and with participants from the project group. At this stage the project participants are the ones most likely to have the best understanding of how the COSTT system will work and what are the main challenges and risks. The results of the risk analysis would however be more reliable if it had included project-external representatives as well.

Basing the preliminary evaluation on the results of a risk analysis is useful in that the evaluation criteria will be risk-based and likely to reflect the top issues. The criteria derived are however high level and have not been evaluated by the intended users of the system. It is also not possible from this initial evaluation to state how the different access control approaches will perform in real life. User evaluations are needed in order to assess how the alternative approaches are able to fit the work processes of the perioperative domain. In particular we suspect that the facilitator-based approach, though getting good scores in the evaluation, will fail in this respect.

In the evaluation of the alternative access control approaches, we have studied the approaches individually and evaluated how they perform related to the identified criteria. It is however possible to combine several of the approaches into a final solution and in this way achieve a solution that better fits the needs of COSTT. To illustrate, screens in waiting rooms may have a preset access level (location-based approach) while screens at other locations may have a maximum access level that is determined by their location but where the group structure, the general situation or a facilitator determines the access level at a given point of time. It is also possible to use the extension suggested where individual employees can get access to more information by utilizing pop-up windows or handheld devices. The preliminary evaluation of the approaches suggests that future work looks into combinations of the location-based approach, the facilitator approach, the situation aware approach and the pop-up/handheld extension approach. The location-based approach is a simple one with the possibility of offering good baseline security. The facilitator approach is able to meet the majority of the criteria. The situation aware approach is the only one able to meet the data quality criterium, and has the potential to also perform well on most of the other criteria. The pop-up/handheld extension approach has good scores on both the privacy and availability criteria.

As the location-based approach is in many ways the most feasible solution, we plan to use this solution as a starting point and look into how it can be combined with risk-based access control approaches in order to add situation awareness. Making proper trade-offs between the risk of privacy breaches and the risk that information is not available is central to the success of the COSTT solution. Risk-based access control solutions can utilise knowledge of the screens' location in order to determine the probability of privacy breaches, as well as the availability requirements for an information item. Other context information, like the time of day and who is likely to be present, can influence the risk evaluation as well. This way, the combined solution will likely perform better on the criteria related to privacy (C3) and availability (C4). In addition, the quality of the information can be taken into account (criterion C1). Though the facilitator approach gets quite high scores on the criteria used in our evaluation, we believe that this solution will not be usable for this type of systems, as it requires quite a lot of interaction with the users. Instead we recommend using handheld devices in combination with large wall-mounted screens in cases where highly sensitive information is needed (to better meet criteria C3 and C4).

6 Conclusion

The main contribution of this paper is a preliminary evaluation of several approaches to access control for public screens used in a perioperative setting. The evaluation criteria used are derived from a risk analysis of the COSTT system. In the evaluation, the facilitator based and the situation aware approaches received high scores, and so did the possible extension of using pop-up windows or handheld devices to get access to additional information. Of the simpler and most feasible approaches, the location-based approach turned out to be the best candidate. As none of the approaches were able to perform well on all evaluation criteria, the results motivate to look further into combining access control approaches. As there are major usability concerns with the facilitator approach in this setting, we recommend focusing on extending the location-based approach with situation awareness, and add support for pop-ups or handheld devices.

Acknowledgments

Thanks to the COSTT project group for participating in the risk analyses. Thanks also to Torstein Nicolaysen for his work in a related MSc thesis, and to Åsmund A. Nyre, Arild Faxvaag, Andreas Seim and Warren Sandberg for reading and commenting on this paper during the writing process. This work has been performed as part of the COSTT project that is supported by the Norwegian Research Council's VERDIKT program (grant no. 187854/S10).

References

1. A. Faxvaag, L. Røstad, I. A. Tøndel, A. R. Seim, and P. J. Toussaint, "Visualizing patient trajectories on wall-mounted boards - information security challenges," in *MIE*, ser. Studies in Health Technology and Informatics, K.-P. Adlassnig, B. Blobel, J. Mantas, and I. Masic, Eds., vol. 150. IOS Press, 2009, pp. 715–719.
2. E. A. Gjære, I. A. Tøndel, M. B. Line, H. Andresen, and P. Toussaint, "Personal health information on display: Balancing needs, usability and legislative requirements," in *MIE , ser. Studies in Health Technology and Informatics (to be published)*, 2011.
3. G. B. D. Shoemaker and K. M. Inkpen, "Single display privacyware: augmenting public displays with private information," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, ser. CHI '01, 2001, pp. 522–529.

4. P. Tarasewich and C. Campbell, "What are you looking at," in *The first Symposium on Usable Privacy and Security (SOUPS 2005)*, 2005.
5. A. Bullock and S. Benford, "An access control framework for multi-user collaborative environments," in *GROUP '99: Proceedings of the international ACM SIGGROUP conference on Supporting group work*, 1999, pp. 140–149.
6. ANSI, "American National Standard for Information Technology - Role Based Access Control," 2004, ANSI INCITS 359-2004.
7. A. Appari and M. E. Johnson, "Information security and privacy in healthcare: Current state of research," *Forthcoming: International J. Internet and Enterprise Management*, 2009.
8. A. Ferreira, R. Cruz-Correira, L. Antunes, and D. Chadwick, "Access control: how can it improve patients' healthcare?" *Studies in Health Technology and Informatics*, vol. 127, pp. 65–76, 2007.
9. L. Røstad and O. Edsberg, "A study of access control requirements for healthcare systems based on audit trails from access logs," in *ACSAC '06: Proceedings of the 22nd Annual Computer Security Applications Conference*, 2006, pp. 175–186.
10. J. Hu and A. Weaver, "Dynamic, context-aware access control for distributed healthcare applications," in *Proceedings of the First Workshop on Pervasive Security, Privacy and Trust (PSPT)*, 2004.
11. M. Alam, M. Hafner, M. Memon, and P. Hung, "Modeling and enforcing advanced access control policies in healthcare systems with SECTET," in *1st International Workshop on Model-Based Trustworthy Health Informaton Systems (MOTHIS 07)*, 2007.
12. P.-C. Cheng, P. Fohatgi, and C. Keser, "Fuzzy mls: An experiment on quantified risk-adaptive access control," IBM Thomas J. Watson Research Center, Tech. Rep., January 2007.
13. N. Dimmock, A. Belokosztolszki, D. Eyers, J. Bacon, and K. Moody, "Using trust and risk in role-based access control policies," in *Proceedings of the ninth ACM symposium on Access control models and technologies*, ser. SACMAT '04, 2004, pp. 156–162.
14. N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y.-K. Lee, and H. Lee, "Enforcing access control using risk assessment," *European Conference on Universal Multiservice Networks*, vol. 0, pp. 419–424, 2007.
15. M. G. Jaatun and I. A. Tøndel, "Covering your assets in software engineering," in *Third International Conference on Availability, Reliability and Security*, 2008, pp. 1172–1179.
16. L. W. M. Wienhofen and A. D. Landmark, "Poster: Representing events in a clinical environment - a case study," in *The 5th ACM International Conference on Distributed Event-Based Systems (DEBS 2011) (to be published)*, 2011.
17. J. Fernando and L. Dawson, "The health information system security threat lifecycle: An informatics theory," *International Journal of Medical Informatics*, vol. 78, no. 12, pp. 815–826, 2009.
18. E. Vaast, "Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare," *The Journal of Strategic Information Systems*, vol. 16, no. 2, pp. 130–152, 2007.