Emerging Trends in Health Care Delivery: Towards Collaborative Security for NIST RBAC

Solomon Berhe[1], Steven Demurjian[1], and Thomas Agresta[2]

[1] Department of Computer Science & Engineering, University of Connecticut, U-2155, 371 Fairfield Road, Storrs, CT, USA
steve@engr.uconn.edu, solomon.berhe@engr.uconn.edu
[2] Department of Family Medicine, University of Connecticut Health Center, 263 Farmington Avenue, Farmington, CT, USA
Agresta@nso1.uchc.edu

Abstract. In the next 10 years there will be rapid adoption of health information technology - electronic medical records by providers and personal health records by patients - linked via health information exchange. There is an emergent need to provide secure access to information spread across multiple repositories for health care providers (e.g., physicians, nurses, home health aides, etc.) who collaborate with one another across cyberspace to deliver patient care. Are available security models capable of supporting collaborative access where providers are simultaneously modifying a patient's medical record? To address this question, this paper details collaborative security extensions to NIST RBAC.

1 Introduction

In 1990, two seminal articles were published related to health care security [7,20]. In [7], privacy and confidentiality in medical information systems was explored. In [20], a detailed case study of mental health delivery from information and semantic perspectives was presented. In the nearly 20 years since their publication, has security kept up with the current and emergent needs of health care delivery in 2010 and beyond? Today, health information technology (HIT) systems are widespread, including: electronic medial record (EMR) to manage all of the health-related information for each patient; electronic prescribing (eRx) to write and transmit prescriptions to pharmacies, personal health records (PHR) that place health-related information directly into the hands of patients. All of these systems must adhere to stringent HIPAA regulations (Health Insurance Portability and Accountability Act of 1996) [16] in regards to the security, availability, transmission, and release of a patient's medical information. In the US, the approved stimulus bill (H.R.1) contains significant funding for HIT adoption including EMRs, PHRs, and health information exchange (HIE).

The movement to a massively linked health information network will be accompanied by dramatic changes in health care delivery, particularly in regards to the way that health care providers collaborative communicate and interact

E. Gudes, J. Vaidya (Eds.): Data and Applications Security 2009, LNCS 5645, pp. 283–290, 2009.

with one another (and patients and their families) [1,2]. Patients with chronic conditions move from provider to provider (e.g., from an internist to a cardiologist) and from location to location (from their home to a hospital to a rehab center and back home again). A patient's medical record differs from data stored in a database in that no data is ever deleted; the record continues to grow over time and can be distributed across multiple EMRs and PHRs. The key is to maintain a complete medical record, and to provide models of collaboration for providers as a patient moves among providers or locations [21].

For collaborative health care, patient privacy and confidentiality must be protected while promoting shared access of information by providers; role-based access control (RBAC) [10,17,19] is a starting point. However, is NIST RBAC [13] well suited to address emergent HIT and HIE needs? Historically, in NIST $RBAC_2$, constraints for separation of duty (SOD), mutual exclusion, and cardinality [3,8] focus on prevention of actions by restricting behavior. For health care, with an "ever-increasing" patient record composed of multiple connected objects in different locations, we are concerned with limiting access while promoting effective and timely treatment. For collaborative care on a single patient, each provider could simultaneously add notes, treatment recommendations, prescriptions, etc. In this context, providers are required to *collaborate on duty* rather than separate their actions. In the remainder of this paper: Section 2 details background and related work; Section 3 proposes extensions to NIST $RBAC_2$ for *collaboration of duty (COD)*; and, Section 4, offers concluding remarks.

2 Background and Related Work

In this section, we present a scenario of patient care based on current and emerging technologies that involves a *virtual chart* [11] which collects a patient's medical history from multiple sources using HIE for unified access against a combined view. Mr. J Smith is a 78 year old patient with known diabetes and a long history of smoking who presents to the emergency room (ER) with shortness of breath and wheezing for the first time. The ER staff initiates a request for his current health records via a secure messaging portal. It is noted that the patient also has a G6 PD deficiency and an allergy to Penicillin. On exam, the patient has findings consistent with emphysema and the possibility of a newly evolving cardiac condition, so a chest X-Ray, an EKG, and some laboratory studies are ordered. The chest X-Ray demonstrates some findings consistent with emphysema and a minimal amount of fluid at the lung bases. The ER physician and ER nurse immediately contact a cardiologist and a radiologist (in another building) to collaboratively review the X-Ray and EKG; based on this collaboration and other test results, the decision to admit the patient is made.

The patient is seen by a hospitalist physician who orders the antibiotic Bactrim and is contacted by the pharmacist prior to dispensation of the medication to discuss how that can cause hemolysis when used in patients with G6 PD deficiency so an alternate is chosen. The patient continues to get better. The hospitalist communicates directly with the primary care physician via a web-based technology on the

day of discharge to discuss follow-up and medication use. They agree that the patient would benefit from a visiting nurse twice weekly over the next 3 weeks. The discharge summary is sent automatically to the patient's primary care physician and the patient's medications on discharge are sent via a E-Prescribing portal that also updates the EMR in the primary care office as well as the patient's PHR. The patient monitors his vital signs and weight daily, recording these into his PHR, which sends a flag automatically to his primary care physician's office if he falls outside of the agreed upon parameters. The patient follows up with his primary care physician 2 weeks after discharge and is doing markedly better. While this scenario is futuristic, all of the indicated systems are available, often in isolation and with limited HIE. The example demonstrates the collaborations that optimally would take place among health care providers to view and modify a patient's medical record.

As to related work, there are many areas that have influenced our work. First, there have been research efforts addressing RBAC [3,8,10,17,19], collaboration models [1], and health care [11]. We have examined these efforts to insure that we can define a collaborative security model based on NIST RBAC and applicable to the health care and other domains. [14] presented the impact of legal patients' rights and their security requirements. Our work shares the common goal of protecting patients' medical records with the help of RBAC. In terms of access control and collaboration [21], a set of eight criteria critical in an collaborative environment are presented. We have begun to evaluate the degree that our COD extensions address these criteria. Another related effort includes a general design for secure collaboration [12], which will be examined more closely against our model since their effort impacts on both the security design process and enforcement. In [4], a model for dynamic trust negotiation for health care collaborations is presented, necessary for emergency situations where collaboration and the associated sharing of patients' medical records is paramount. We will need to consider dynamic collaborations as we expand our COD to include workflow. Lastly, in [9], a list of inter-professional and inter-organizational collaboration challenges in the health care domain are reviewed, along with a validation model. Generalizing and applying such a validation to our work on COD will be an important step in assessing our work.

3 Collaboration on Duty via Extended NIST $RBAC_2$

For our purposes, the general act of collaboration can be defined as: "Two or more users (each with their own role) each with their own set of allowable actions who are accessing (read and/or write) one or more objects for the same entity with the possibility that their access is constrained by time (when an action can occur) or order (defined sequence of the order of actions)." This section explores collaboration by: reviewing the NIST RBAC model and its limitations for health care; and, extending NIST $RBAC_2$ with *collaboration of duty (COD)* constraints illustrated using an example collaboration from Section 2.

The NIST reference models, $RBAC_0$ to $RBAC_3$[17] are an ideal starting point for security as related to the scenario in Section 2. $RBAC_0$ links the concepts of

roles and permissions (permission assignment) and users and roles (user assignment). $RBAC_1$ allows the definition of role hierarchies where privileges assigned to one role are available to other roles depending on the defined relationship. For example, an ER physician would be a a child of a physician role. $RBAC_2$ extends $RBAC_1$ with constraints [3], namely, *separation of duty (SOD)* and *mutual exclusion* [8]. For example, in the early stages of training, an intern may wish to write a prescription for a narcotic (e.g., oxycontin) but may require a resident physician to approve and write the prescription; this illustrates static SOD. While NIST RBAC can handle typical requirements, there are changes emerging. There is a movement towards the *medical home* where care is coordinated by one physician who reaches out and collaborates with a myriad of health care providers [5,6]; Section 2 illustrated such a scenario. As a result, NIST RBAC is limited in support of collaboration by: no direct support for the idea of collaborative access of multiple (user, role) pairs on one or more (objects, action) pairs; overlapping roles in health care made it difficult to establish a clear cut boundary between responsibilities and tasks; and, the assignment of permissions based only on role is not sufficient to clearly take into consideration contextual concerns such as an individual's schedule, the collaboration team, availability of collaborators, sequence of collaborators, etc.. One premise of our work is that these actions are part of an enhanced security model that considers collaboration and workflow as integral to achieving secure information usage.

Given these limitations, we introduce notation consistent with NIST RBAC [13] to serve as a basis for its extension with COD. To begin, we define: $\mathcal{U}$,$\mathcal{R}$, and $\mathcal{P}$ as sets of users, roles, and permissions, respectively; $\mathcal{O}$ and $\mathcal{A}$ as sets of all *objects* and *actions*, respectively, on which permissions are defined for roles and then assigned to users; and, for *assignment*, we define three sets:

- $\mathcal{P} \subseteq \mathcal{O} \times \mathcal{A}$ be a many-to-many *object-action assignment*,
- $\mathcal{PA} \subseteq \mathcal{R} \times \mathcal{P}$ be a many-to-many *role-permission assignment*, and
- $\mathcal{UA} \subseteq \mathcal{R} \times \mathcal{U}$ be a many-to-many *role-user assignment.*

Note that SOD, cardinality, and mutual exclusion constraints determine whether or not values in $\mathcal{PA}$ and $\mathcal{UA}$ are permitted. For the exmaple from Section 2, we use Mr. Smith's initial assessments and laboratory tests (X-Ray and EKG) by defining the sets $\mathcal{U}$,$\mathcal{R}$, $\mathcal{UA}$, $\mathcal{O}$, $\mathcal{A}$, and $\mathcal{P}$:

- $\mathcal{U}$ = {ERPhysician1, ERNurse1, Cardiologist1, Cardiologist2, Radiologist1, Radiologist2, Patient1}
- $\mathcal{R}$ = {Physician, Nurse, PhysicianSpecialist, Patient}
- $\mathcal{UA}$ = {(ERPhysician1, Physician), (ERNurse1, Nurse), (Patient1, Patient) (Cardiologist1, PhysicianSpecialist), (Cardiologist2, PhysicianSpecialist), (Radiologist1, PhysicianSpecialist), (Radiologist2, PhysicianSpecialist)}
- $\mathcal{O} = \{o^{VC}_{J.Smith}, o^{X-Ray}_{J.Smith}, o^{EKG}_{J.Smith}\}$
- $\mathcal{A}$ = {read, write}
- $\mathcal{P} = \{P_1 = (\text{read}, o^{VC}_{J.Smith}), P_2 = (\text{write}, o^{VC}_{J.Smith}), P_3 = (\text{read}, o^{X-Ray}_{J.Smith}), P_4 = (\text{write}, o^{X-Ray}_{J.Smith}), P_5 = (\text{read}, o^{EKG}_{J.Smith}), P_6 = (\text{write}, o^{EKG}_{J.Smith})\}$

Instead of names, we use a job title and a number to signify a person. We assume PhysicianSpecialist is a child of Phyician. Note VC stands for virtual chart.

Given these definitions, we propose *collaboration on duty (COD)* extensions to NIST RBAC. As shown in the lower right of Figure 3, these constraints impact the COD Teams (User/Role combinations) and define the allowable actions on objects with respect to defined permissions. There are four different *COD Constraints (CODC)*: lifetime (LT) which indicates the range (time period) for when a collaboration team is active; time-to-complete (TTC) the collaboration which represents the maximum duration of the collaboration; cardinality (CARD) which denotes a range (minimum, maximum) of individuals (each with a user/role combination) who must participate in the collaboration; and, attendance (ATT) which captures the participation of the team members for the collaboration. When establishing a collaboration, the collaboration must specifically select one user/role combination to constrain the actions and affected objects of that user to that role in a collaboration:

Definition 1. A *Collaboration Team*, $\mathcal{CT} \subseteq \mathcal{UA}$, is defined as a set of user/role combinations to indicate the user and his/her role for that particular collaboration.

Definition 2. The *Collaboration Permissions*, $\mathcal{CP} \subseteq \mathcal{PA}$, represent the involved permissions of the $\mathcal{CT}$ for the collaboration.

Note that Collaboration Permissions are a subset of the defined permissions ($\mathcal{PA}$) for all of the user/role combinations on the Collaboration Team. Each member of the Collaboration Team is constrained to a subset of those objects, actions, and permissions that are defined for his/her role.

In terms of time, two optional constraints control when a collaboration occurs, lifetime (LT) and time-to-complete (TTC). LT indicates the time range (start and end time) when the team $\mathcal{CT}$ is operational for a collaboration. TTC represents the duration of the collaboration once it begins. Note that if LT is defined, a collaboration cannot start before the start time or complete after the end time. If a TTC is also defined, the collaboration must start to allow the duration to finish prior to the end time as defined by LT.

Definition 3. A *CODC for Lifetime*, $CODC_{LT} = [Start-Time, End-Time]$.

Definition 4. A *CODC for Time-to-Complete*, $CODC_{TTC} = [Duration]$.

Note that the Duration must occur within the LT (if defined); otherwise, it represents the duration of the collaboration once it begins.

Cardinality (CARD) is an aggregation constraint for the definition of the minimum and maximum number of participants. When minimum equals maximum equals the size of the team, then all team members must participate. Note that it does not denote which members must participate.

Definition 5. A *CODC for Cardinality*, $CODC_{CARD} = [min, max]$, where min $\leq$ max and max $\leq \mid \mathcal{CT} \mid$.

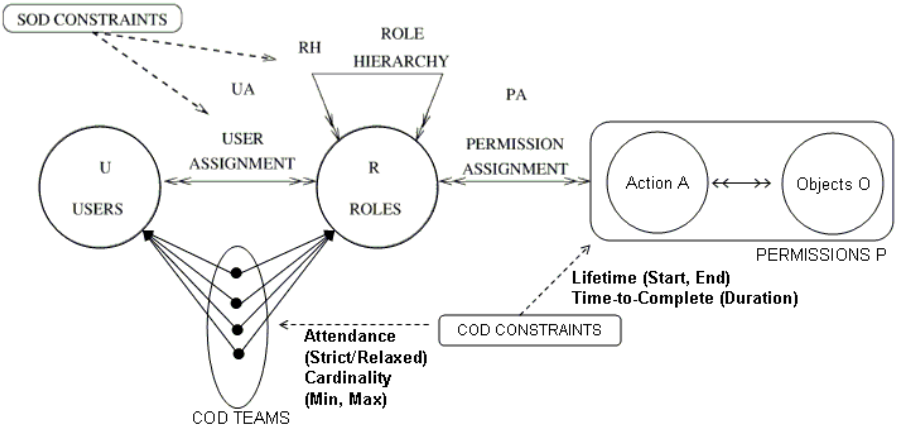

Fig. 1. COD Capable NIST $RBAC_2$

$CODC_{CARD}$ is not sufficient to dictate who must participate in a collaboration; we differentiate between the users in $\mathcal{CT}$ who must participate in the collaboration vs. those who may participate. When defining COCD attendance (ATT), we specify two sets of users: C_{strict} is a set of users who must participate in the collaboration, while $C_{relaxed}$ is a set of sets of users, where for each set of users, at least one must participate.

Definition 6. A *CODC for Attendance*, $CODC_{ATT} = \{C_{relaxed}, C_{strict}\}$ where:

- $C_{strict} \subseteq \mathcal{U}$ are the set of users who must participate in the collaboration,
- $C_{relaxed} = \{\{ua_1\}, \{ua_2\},...,\{ua_n\}\}$, where each ua_i ($\mid ua_i \mid \geq 2$), i ∈ 1..n, is a set of users, and for each set there exists at least one $u_j \in \mathcal{U}$ who participates in the collaboration, and
- $\forall_{i=1}^{n} ua_i (\in C_{relaxed}) : C_{strict} \cap ua_i = \emptyset$

Notationally, we collect all of the COD Constraints for a collaboration as:

Definition 7. The COD Constraints for a collaboration is:
$\mathcal{CODC} = [CODC_{LT}, CODC_{TTC}, CODC_{CARD}, CODC_{ATT}]$.

In this notation, any of the constraints may be null. Next, an individual collaboration brings together the collaboration team, permissions (a subset of the overall permissions $\mathcal{PA}$), and the constraints for that team as:

Definition 8. A Collaboration $\mathbb{C}$ is a three tuple defined as: $\mathbb{C} = (\mathcal{CT}, \mathcal{CP}, \mathcal{CODC})$.

For the example: $\mathbb{C}_1 = (\mathcal{CT}, \mathcal{CP}, \mathcal{CODC})$ where

- $\mathcal{CT}$ = {ERPhysician1, ERNurse1, Cardiologist1, Cardiologist2, Radiologist1, Radiologist2}

- $\mathcal{CP}$ = { (ERPhysician1,P_2, P_3, P_5), (ERNurse1,P_2, P_3, P_5), (Radiologist1,P_2, P_4), (Radiologist2,P_2, P_4), (Cardiologist1,P_2, P_3, P_6), (Cardiologist2,P_2, P_3, P_6) }
- $\mathcal{CODC}$ = $[CODC_{LT}, CODC_{TTC}, CODC_{CARD}, CODC_{ATT}]$ with
  - $CODC_{LT} = (\emptyset, \emptyset)$
  - $CODC_{TTC}$ = 1 hour
  - $CODC_{CARD} = (3, 4)$
  - $CODC_{ATT} = \{C_{relaxed}, C_{strict}\}$ where $C_{relaxed}$={{Radiologist1, Radiologist2}, {Cardiologist1, Cardiologist2}} and C_{strict}={ERPhysician1, ERNurse1}

$\mathbb{C}_1$ is a four-way collaboration between ERPhysician1, ERNurse1, a radiologist, and a cardiologist, with their permissions to read and write the patient's VC, X-Ray, and EKG as indicated by $\mathcal{CP}$. For COD constraints there is: a one hour time-to-complete ($CODC_{TTC}$); a requirement that at least one radiologist and at least one cardiologist join the collaboration ($C_{relaxed}$); and, a requirement that ERPhysician1 and ERNurse1 must attend (C_{strict}). Note that we have slightly eased the cardinality of the collaboration since according to busy schedules or other emergencies, we only require that 3 out of 4 individuals be present, but all four must participate at some point in the time limit.

Finally, a given application consists of multiple collaborations:

Definition 9. An Applications (APP) Collaborations $\mathcal{APP}_{\mathbb{C}} = \{\mathbb{C}_j\}$ for j=1..m collaborations.

This definition captures collaborations for the entire application, to be complemented with roles, users, permissions, SOD, mutual exclusion, etc.

4 Conclusion

In this paper, we have revisited two classic articles [7,20], and used them as rationale to look forward to understand the rapidly changing and evolving role of information technology in health care. Electronic medical records, personal health records, electronic prescribing systems, with health information exchange to tie them all together will offer new opportunities for health care professionals and providers to collaborate with one another towards improved patient care. This paper has focused on the extension of NIST RBAC to support collaboration of duty (COD) by: presenting a futuristic health care scenario collaboration in Section 2; and, COD extensions to $RBAC_2$ to capture collaborations and constraints with respect to time, access, and attendance in Section 3, supplemented with an illustrative example from the futuristic scenario. We believe that the work presented herein is an important step in introducing collaboration into the security and NIST RBAC.

References

1. Abraham, J., Reddy, M.: Moving Patients Around: A Field Study of Coord. Between Clinical and Non-Clinical Staff in Hospitals. In: Proc. of ACM 2008 Conf. on Computer Supported Cooperative Work (2008)
2. Agrawal, R., et al.: Enabling the 21st Century Health Care Information Technology Revolution. Comm. of the ACM
3. Ahn, G.-J., Sandhu, R.: Role-Based Authorization Constraints Specification. ACM Trans. Inf. Syst. Secur. 3(4) (2000)
4. Ajayi, O., et al.: Dynamic Trust Negotiation for Flexible E-Health Collaborations. In: Proc. of 15th ACM Mardi Gras Conf. (2008)
5. American Academy of Pediatrics Web Page and Discussion on Medical Home, `http://www.medicalhomeinfo.org/`
6. American College of Physicians Web Page and Discussion on Medical Home, `http://www.acponline.org/advocacy/where_we_stand/medical_home/`
7. Biskup, J.: Protection of Privacy and Confidentiality in Medical Information Systems: Problems and Guidelines. In: Spooner, D., Landwehr, C. (eds.) Database Security, III: Status and Prospects. North-Holland, Amsterdam (1990)
8. Chen, H., Li, N.: Constraint Generation for Separation of Duty. In: Proc. of 11th ACM Symp. on Access Control Models and Technologies (2006)
9. D'Amour, D., et al.: A Model and Typology of Collaboration Between Professionals in Healthcare Organizations. BMC Health Services Research (2008)
10. Ferraiolo, D., et al.: Proposed NIST Standard for Role-Based Access Control. ACM Trans. on Information and Sys. Sec. 4(3) (2001)
11. Kenny, P., et al.: Virtual Humans for Assisted Health Care. In: Proc. of 1st Intl. Conf. on PErvasive Technologies Related to Assistive Environments (2008)
12. Nakae, M., et al.: A General Design Towards Secure Ad-hoc Collaboration. In: Proc. of 2006 Symp. on Information, Computer and Communications Security (2006)
13. NIST RBAC Standard, `http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf`
14. Ali Pabrai, U.O.: Getting Started with HIPAA. Course Technology Press (2003)
15. Park, J., et al.: A Secure Workflow System for Dynamic Collaboration. In: Sec 2001: Proc. of 16th Intl. Conf. on Information Security: Trusted Information (2001)
16. Rindfleisch, T.: Privacy, Information Technology, and Health Care. J. of the ACM 40(8) (1997)
17. Sandhu, R., et al.: Role-Based Access Control Models. IEEE Computer 29(2) (1996)
18. Sims, S., et al.: Surveillance of Methadone-Related Adverse Drug Events Using Multiple Public Health Data Sources. J. of Biomedical Informatics 40(4) (2007)
19. Ting, T.C.: A User-Role Based Data Security Approach. In: Landwehr, C. (ed.) Database Security: Status and Prospects. North-Holland, Amsterdam (1988)
20. Ting, T.C.: Application Information Security Semantics: A Case of Mental Health Delivery. In: Spooner, D., Landwehr, C. (eds.) Database Security, III: Status and Prospects. North-Holland, Amsterdam (1990)
21. Tolone, W., et al.: Access Control in Collaborative Systems. ACM Computing Surveys 37(1) (2005)
22. Xiao, Y.: Artifacts and Collaborative Work in Healthcare: Methodological, Theoretical, and Technological Implications of the Tangible. J. of Biomedical Informatics 38(1) (2004)