Multi-Level Security in Healthcare Using a Lattice-Based Access Control Model

Steven A. Demurjian, University of Connecticut, Storrs, USA
Eugene Sanzi, University of Connecticut, Storrs, USA
Thomas P. Agresta, University of Connecticut Health Center, Farmington, USA
William A. Yasnoff, National Health Information Infrastructure Advisors, Portland, USA

ABSTRACT

Controlling access to sensitive personal information is a primary concern in healthcare. Regardless of whether access control policies are determined by patients, healthcare professionals, institutions, legal and regulatory authorities, or some combination of these, assuring the strict enforcement of policies across all systems that store personal health information is the overriding, essential goal of any healthcare security solution. While a comprehensive healthcare security architecture may need to impose specific controls on individual data items, most access control decisions will be based on sensitivity levels automatically assigned to information classes by a “sensitivity profile,” combined with the authorization level of the user. This article proposes the use of multi-level security, defined by lattice-based sensitivity profiles, to ensure compliance with data access restrictions between systems. This security approach accommodates the complexities needed for health data access and benefits from existing, proven tools that are used for defense and national security applications.

KEYWORDS
Lattice-Based Access Control, Lattice-Based Security, Multi-Level Security, Sensitivity Profile

1. INTRODUCTION

Ensuring that the correct individual receives only authorized information is one of the key security concerns in the health care domain. This requires that access to both personally identifiable information (PII) and personal health information (PHI) be precisely controlled. There are two dimensions that are relevant for securely accessing health care data. For the first dimension, access control must be realized in all of the health information technology (HIT) systems that are available to the various stakeholders (medical professionals, administrative staff, patients, family members, etc.). HIT systems include: electronic health records (EHRs), practice management systems (PMS), and personal health records (PHRs); the majority but not all of these systems must adhere to the Health Insurance Portability and Accountability Act (HIPAA) (HIPAA, 2017) for the security, availability, transmission, and release of a patient’s medical information. For the second dimension, patient-controlled access to data is a desirable and increasingly important aspect of making information accessible, and may allow patients

DOI: 10.4018/IJPHIM.2019010105

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
to define who (among the aforementioned stakeholders) can have access to what information at which times to view/modify medical/health/fitness data. While both privacy and security are of paramount concern for both these dimensions, our focus is on ensuring that the security is robust enough to operationalize a wide variety of potential privacy policies including HIPAA and patient control. Caine and Hanania (Caine & Hanania, 2013) studied the type and granularity of medical/health/fitness data for which patients wanted to control access. An earlier effort (Sujansky et al., 2010) emphasized fine grained access control by role to allow a patient to define that, for example: a family member can view a subset of my medication list, a person’s personal physician may view/modify medical/health/fitness data, and an emergency physician can see all of an individual’s medical/health data in an emergent situation, etc. Previously, Peleg et al (Peleg et al., 2008) described a method to establish privileges and access control from the perspective of the patient – called situation-based access control. More recently, it has been proposed (Kendall & Quill, 2017) that every American have a lifetime electronic health record that has complete information and is available from any location.

In order to support the security needs for the two dimensions, access control models have been historically utilized, with the most dominant being role-based access control (RBAC) (Ferraiolo, et al., 2001) and discretionary access control (DAC) (Dittrich, Hartig, & Pfiefferle, 1988). RBAC has a strong history in the health care domain, as evidenced by a recently published literature review (Fernández-Alemán, Señor, Lozoya, & Toval, 2013) that identified access control models deployed by EHRs, where out of 45 articles reviewed, 35 used access control methods, and 27 of these specifically utilized RBAC. DAC has also been studied for EHRs in conjunction with RBAC (Alhaqabani & Fidge, 2008; Khan & Sakamura, 2012) in an attempt to combine the capabilities and advantages of both approaches. Despite the attention to both RBAC and DAC, there has been limited usage of both in actual HIT systems to achieve the fine-grained control of security that is necessary for both the HIT dimension and the patient-controlled dimension. In fact, it can be argued that the complexity of allowing fine-grained permissions for medical/health/fitness data will require an approach that is able to clearly distinguish and identify different levels of security based on the confidentiality and privacy of the data itself and the way that a patient would seek to make such data available to stakeholders. The work of Caine and Hanania (Caine & Hanania, 2013) supports this argument. For our purposes, the most interesting information is their presentation in Figure 1 (replicated in our Figure 1) of their study showing the recipients (stakeholders) and information items that are involved in the process of patients managing and sharing their medical data. Protected items include contact information and demographics, information relevant to current conditions, medications (prescribed and over-the-counter), test results (blood pressure, blood tests, imaging tests, etc.), and past medical history. More sensitive items include: history of substance abuse and treatment, mental health information, sexual health information, records relating to domestic violence, reproductive health records, and genetic information.

Given the wide variety and scope of medical/health/fitness data, one security approach that may address the granularity issue for fine-grained control is multi-level security (MLS), which has its origins in the lattice-based access control model (LBAC) (Denning, 1976) and the mandatory access control model (MAC) (Bell & LaPadula, 1976). Both models rely on sensitivity levels (e.g., unclassified, confidential, secret, top secret, etc.) that are assigned to objects (termed classifications) and users (termed clearances). Access to objects depends on a comparison of a user’s clearance against an object’s classification based on the type of operation (read, write, etc.); they differ in that MAC utilizes a strict hierarchy of sensitivity levels while LBAC utilizes a lattice. As an example, consider that medications may have a different sensitivity level and need to be more secure than contact information/demographics. In fact, medications may have multiple sensitivity levels since a patient may not want to disclose all medications they are taking to a particular stakeholder, e.g., medications related to mental health, domestic violence, etc. There have been some very limited attempts to utilize MLS and MAC in the health care domain (Alhaqabani & Fidge, 2008) that also include MAC in their work; one study (Gajanayake, Iannella, & Sahama, 2014) considered the use of MAC in EHRs; and another (Hafner,
Anti-Counterfeit Technologies for Spurious Drugs in India

[www.igi-global.com/article/anti-counterfeit-technologies-spurious-drugs/61321?camid=4v1a](http://www.igi-global.com/article/anti-counterfeit-technologies-spurious-drugs/61321?camid=4v1a)