Chapter 3
A Context-Aware Authorization Model for Process-Oriented Personal Health Record Systems

Eleni Mytilinaiou
University of Piraeus, Greece

Vassiliki Koufi
University of Piraeus, Greece

Flora Malamateniou
University of Piraeus, Greece

George Vassilacopoulos
University of Piraeus, Greece

ABSTRACT

Healthcare delivery is a highly complex process involving a broad range of healthcare services, typically performed by a number of geographically distributed and organizationally disparate healthcare providers requiring increased collaboration and coordination of their activities in order to provide shared and integrated care. Under an IT-enabled, patient-centric model, health systems can integrate care delivery across the continuum of services, from prevention to follow-up, and also coordinate care across all settings. In particular, much potential can be realized if cooperation among disparate healthcare organizations is expressed in terms of cross-organizational healthcare processes, where information support is provided by means of Personal Health Record (PHR) systems. This chapter assumes a process-oriented PHR system and presents a security framework that addresses the authorization and access control issues arisen in these systems. The proposed framework ensures provision of tight, just-in-time permissions so that authorized users get access to specific objects according to the current context. These permissions are subject to continuous adjustments triggered by the changing context. Thus, the risk of compromising information integrity during task executions is reduced.

DOI: 10.4018/978-1-61692-895-7.ch003

INTRODUCTION

Healthcare delivery is a highly complex process involving a broad range of healthcare services (e.g. in-patient, out-patient, emergency), typically performed by a number of geographically distributed and organizationally disparate healthcare providers requiring increased collaboration and coordination of their activities in order to provide shared and integrated care (Koufi & Vassilacopoulos, 2008). As healthcare providers are mostly hosting diverse and disparate information systems, it is difficult to obtain a complete picture of a person's healthcare record at the point of care when needed.

Recently, there has been a remarkable upsurge in activity surrounding the adoption of Personal Health Record (PHR) systems (Tang et al., 2006). A PHR is a consumer-centric approach to making comprehensive electronic health records (EHRs) available at the point of care while protecting patient privacy (Lauer, 2009). Unlike traditional EHRs which are based on the 'fetch and show' model, PHRs' architectures are based on the fundamental assumptions that the complete records are held on a central repository and that each patient retains authority over access to any portion of his/her record (Lauer, 2009; Wiljer et al., 2008). Thus, there is no need for interoperable virtual patient record architectures since storing and retrieving essential patient data is no longer fragmented. Hence, quality and safety of patient care is enhanced by providing patients and health professionals with relevant and timely information when and where needed, while ensuring protection and confidentiality of personal data.

Providing patients with access to their electronic health records offers great promise not only to improve patient health and satisfaction with their care but also to enhance professional and organizational approaches to health care (Wiljer et al., 2008). In particular, much potential can be realized if cooperation among disparate healthcare organizations is expressed in terms of cross-organizational healthcare processes, where information support is provided by means of PHR systems.

Healthcare processes are fundamentally different from those of other domains for a number of reasons including: (a) patient care requires availability of an extensive amount of medical data (medical images and free texts, XML documents, medical charts, etc), (b) ad hoc collaborative work and high degree of communication between healthcare professionals is an integral part of activities surrounding patient care, (c) each healthcare professional is involved in the care of several patients in parallel and (d) healthcare professionals are working in a mobile environment where their availability status is subject to rapid change due to the constant interruptions anytime, anywhere. Moreover, the computing environment in healthcare organizations is becoming increasingly complex as multiple heterogeneous technologies are employed and highly interactive user applications are supported. In such an environment, privacy and security of personal health information are considered critical factors in advancing the interests of both healthcare providers and consumers (Atluri & Huang, 1996; Wu, Sheth, Miller & Luo, 2002). Thus, one important consideration in the development of process-oriented PHR systems is to secure personal information against unauthorized access, collection, use, disclosure or disposal by ensuring a tight matching of permissions to actual usage and need. To this end, the least privilege principle should be enforced which, in turn, requires continuous adjustments of the sets of user permissions to ensure that, at any time, users (e.g. healthcare professionals) assume the minimum set of permissions required for the execution of each task of a healthcare process.

In healthcare processes, however, certain user permissions depend on the process execution context. That is, contextual information available at access time, such as user-to-patient proximity, location of attempted access and time of attempted access, can influence the authorization decision