Chapter 6.2
Location–Aware Access Control for Mobile Workflow Systems

Michael Decker
University of Karlsruhe, Germany

ABSTRACT

Workflow management systems (WfMS) are a special class of information systems (IS) which support the automated enactment of business processes. Meanwhile there are WfMS which allow the execution of tasks using mobile computers like PDA with the ability of wireless data transmission. However, the employment of workflow systems as well as mobile technologies comes along with special security challenges. One way to tackle these challenges is the employment of location-aware access control to enforce rules that describe from which locations a user is allowed to perform which activities. The data model behind access control in termed Access Control Model (ACM). There are special ACM for mobile information systems as well as for WfMS, but no one that addresses mobile as well as workflow specific aspects. In the article we therefore discuss the specific constraints such a model should be able to express and introduce an appropriate ACM. A special focus is on location constraints for individual workflow instances.

INTRODUCTION

Mobile technologies subsume portable computers like notebooks, PDA, smartphones and wireless data transmission based on standards like GPRS, EDGE, WiFi or UMTS. Such technologies pro-

vide the potential for many hitherto unthinkable applications since they enable access to computer technology almost anywhere and anytime. However, the development of mobile information systems (MIS) entails some specific challenges such as limited accumulator lifetime, unreliable data transmission, small displays and limited means for data input. A further challenge considered as

a very serious one by many experts are security-related issues (e.g., Ernest-Jones (2006)): Security concerns arise because due to their portability mobile computers often get lost or stolen so unauthorized people can gain access to confidential data or even services. Mobile computers are often used in environments like public and highly frequented places where unauthorized people could take a look over the user's shoulder to learn about confidential data (so called "shoulder surfing" or "shoulder sniffing"). Also, since users consider mobile computers as personal device they often use their business devices (provided by their employer) also for private matters and are following the company's security policy (e.g., prohibition to install software) to a lower degree than this would be the case for a stationary computer.

There are various approaches to tackle the specific security challenges that come along with mobile computing:

- Wireless data communication can be encrypted to thwart eavesdropping and manipulation of transmitted data
- Sensitive data can be stored in encrypted form on the mobile device
- There are even devices that have a built-in finger print reader because prompting for passwords as means for authentication is not appropriate for all mobile scenarios.

And besides these preventive measures there are even some approaches that can be taken after a mobile device got lost:

- The so called "kill pill" is an special command message which is sent to a mobile device to triggers the deletion of sensible data that might be stored on that device
- The "Equipment Identity Register" (EIR) in GSM-networks is a database that stores a list of devices reported as stolen or lost so the network access can be denied for those devices.

In the paper at hand we focus on the employment of so called *Access Control Models (ACM)* as further preventive approach to tackle specific security problems of MIS. ACM are special models to formulate which users of an information system are allowed to perform particular operations (e.g., read, write, append, delete, execute) on particular resources under the protection of an information system (e.g., data objects, services). For example, an instance of such a model could state that user Alice is allowed to perform the operation "read" on the resource "address database". Meanwhile there are ACM that were developed to express location-related access restrictions. Using such models policies like the following can be formulated: "An employee is only allowed to access a particular resource while staying at the premises of his company". Beside location-aware ACM there are also ACM to express workflow-specific rules. However, as far as we know there are no ACM that are location-aware as well as process-aware. There are several mobile workflow systems but they don't have a special ACM. Our work therefore concentrates on the development of an ACM that is able to express specific constraints for mobile workflow systems.

At the end of the paper we will also explain how ACM can address another mobile-specific problem, namely usability issues due to the constrained user interface for data output (tiny display of poor quality) and input (often no fully-fledged keyboard but just a few buttons, no pointer device like a "mouse").

The remainder of this article is structured as follows: in the next section we cover workflow systems and approaches how to adapt them to support mobile users. The section after this is devoted to an overview about ACM in general and location-aware respective workflow-aware ACM in particular. Following this we give a short introduction to the relevant aspects of location determination and the location model. In the subsequent section we first describe an example workflow process before we introduce our ACM;

Related Content

Recursive Spatial Multiplexing with Adaptive Interference Whitening

Usama Y. Mohamad, Ibrahim A. Shah, Thomas Hunzikerand Dirk H. Dahlhaus (2017). *International Journal of Wireless Networks and Broadband Technologies (pp. 43-59).*

www.irma-international.org/article/recursive-spatial-multiplexing-with-adaptive-interference-whitening/201850

Survey and Evaluation of Advanced Mobility Management Schemes in the Host Identity Layer

László Bokor, Zoltán Faigland Sándor Imre (2014). *International Journal of Wireless Networks and Broadband Technologies (pp. 34-59).*

www.irma-international.org/article/survey-and-evaluation-of-advanced-mobility-management-schemes-in-the-host-identity-layer/104629

Trends in Managing Multimedia Semantics

Roberto Poli, Achilles Kameasand Lambrini Seremeti (2014). *International Journal of Wireless Networks and Broadband Technologies (pp. 40-55).*

www.irma-international.org/article/trends-in-managing-multimedia-semantics/115589

Factors Affecting WiFi Use Intention: The Context of Cyprus

Despo Ktoridou, Hans-Ruediger Kaufmannand Christos Liassides (2012). *Wireless Technologies: Concepts, Methodologies, Tools and Applications (pp. 1760-1781).*

www.irma-international.org/chapter/factors-affecting-wifi-use-intention/58867

Machine Learning in Radio Resource Scheduling

Ioan-Sorin Coma, Sijing Zhang, Mehmet Emin Aydin, Pierre Kuonen, Ramona Trestianand Gheorghi Ghinea (2019). *Next-Generation Wireless Networks Meet Advanced Machine Learning Applications (pp. 24-56).*

www.irma-international.org/chapter/machine-learning-in-radio-resource-scheduling/221425