



ELSEVIER

Data & Knowledge Engineering 43 (2002) 1–27

**DATA &
KNOWLEDGE
ENGINEERING**

www.elsevier.com/locate/datak

AutoWF—A secure Web workflow system using autonomous objects

Ehud Gudes *, Aharon Tubman

Department of Computer Science, Ben-Gurion University, Beer-Sheva, Israel

Received 10 March 2001; received in revised form 5 September 2001; accepted 29 January 2002

Abstract

Workflow management systems (WFMS) automate business processes where information flows between individuals. WFMS have two major implications for security: First, since the description of a workflow process explicitly states *when* which function is to be performed by *whom*, security specifications may be derived from such descriptions and translated into static role-based specifications. Second, since the WFMS is to be operated on the Web using web agents, dynamic and individual security rules must be enforced. AutoWF includes both types of security policies. AutoWF is implemented on top of a powerful software foundation—autonomous objects. Both general workflow management tasks and specific functional tasks are implemented as autonomous objects distributed over the Internet.

This paper surveys some of the concepts on which the system is based, it then concentrates on the design and architectural issues of the AutoWF system, and finally we present some implementation examples.

© 2002 Elsevier Science B.V. All rights reserved.

Keywords: Database security; Workflow; Cyberspace; Autonomous objects; Role-based security; Dynamic authorization

1. Introduction

Workflow management systems (WFMS) automate traditional processes where information flows between individuals. Although WFMS have been in existence for a number of years, the trend towards greater interconnection will greatly impact such systems. On the one hand, interaction will involve more and more non-human participants. On the other hand the participants in

* Corresponding author.

E-mail addresses: ehud@cs.bgu.ac.il (E. Gudes), aharontu@cs.bgu.ac.il (A. Tubman).

workflow processes will become more and more unrelated, and therefore, their security becomes a major concern.

The key to secure implementation of WFMS is proper authentication and authorization of participants in a workflow process. It is our contention that Alter-egos (see [8] and Section 2) are particularly suitable for authentication, while roles are particularly suitable for authorization. Stated differently, we will assume that a potential participant will present an Alter-ego that will serve as a proof of the participant's identity and which, along with other information, will identify the participant's role.

In earlier papers we discussed the concept of Alter-egos [15] and the derivation of security and privacy rules for a workflow system using them. In [8] we also presented an example implementation which was based on a specific prolog based object-oriented system called Mokum [13].

In [7] we generalized and formalized the above model using the *Z* formal specification language [20], and we presented a very general architecture on top of which this model can be implemented. In this paper we focus on an architecture and implementation which is based on the concept of *autonomous objects* [11]. Autonomous objects represent active database objects which can be distributed over the Internet, yet they are connected by a single name space, can communicate securely between them, and have special gates to their functional methods called *guards* which can be used to verify security before any action is performed. This makes them a very convenient tool for implementing a secure workflow system over the Internet.

The rest of this paper is structured as follows: Section 2 gives some background on Alter-egos, workflow and security, and introduces the Bank loan workflow example. This section also reviews the concept of autonomous objects and briefly describes the AutoO system. Section 3 discusses in more detail some of the security problems occurring in workflow systems, in particular the concept of dynamic authorization, and then presents our model for solving them. Section 4 presents the architecture of the AutoWF system and its mapping to autonomous objects. Section 5 presents some more details on some of the system components such as the Dynamic Authorization administrator. Section 6 presents an implemented test case, and Section 7 contains the conclusions of the paper. For reasons of space, the full specifications (in *Z*) of the AutoWF system is not given, and can be found in [18].

2. Background

2.1. Workflow in cyberspace

Workflow management models and applications were originally developed for a single organization. In that context, WFM tools are used to specify how people and information systems are cooperating within the organization. A typical workflow management application is composed of several tasks which need to be completed by one or more persons or departments. The organization business procedure usually requires that some of these tasks need to be completed before others can start, so a partial order (a directed graph) is defined on these tasks. The organization procedure may also require policies such as "separation of duties" which require specific *roles* to perform specific tasks. In addition, each such task is defined by the function it performs and the data it receives and sends. All these requirements can be specified by a *workflow model*. Currently

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات