Titre du sujet de thèse Etude de la Sécurité de Documents Interactifs partagés

Titre du sujet de thèse (Anglais) Security issues in collaborative editing of XML documents.

Encadrants Clara Bertolissi, Denis Lugiez

Ecole Doctorale : ED 184

Unité de Recherche Laboratoire Informatique Fondamentale UMR 6166
39 avenue Joliot-Curie, 13453 Marseille Cedex

Localisation UFR MIM Chateau-Gombert

Directeur de Thèse Denis Lugiez, email : denis.lugiez@lif.univ-mrs.fr
Clara Bertolissi, email : clara.bertolissi@lif.univ-mrs.fr

Sujet La croissance récente de la communication numérique a augmenté la demande de sécurité pour protéger les ressources et préserver l'intégrité et la confidentialité des données. Dans des environnements distribués où on accède et échange de grands volumes de données provenant d'endroits multiples, des spécifications formelles de politiques de sécurité déclaratives (pour manipuler les complexités de la spécification), satisfaisant des propriétés de conformité (pour la vérification) sont nécessaires.

La plupart des données échangées actuellement sur internet sont sous format XML qui est devenu le langage standard pour la transmission d'informations structurées. Il est donc nécessaire que les systèmes puissent prendre en compte directement ce format. Généralement les documents XML sont traités comme des arbres non ordonnés et sont typés en utilisant des DTDs ou des schémas XML.

Il existe aujourd'hui plusieurs formats pour définir les politiques de sécurité et les systèmes de contrôle d'accès (RBAC, DEBAC, WS-SecurityPolicy,...). Récemment, une extension de XML, le langage XACML, a été proposé pour représenter des politiques de contrôle d'accès associées à un document XML.

On s'intéresse ici en particulier aux documents partagés qui peuvent être modifiés et consultés de manière interactive et distribuée. Par exemple, les agendas électroniques partagés (doodle) ou des systèmes de gestion de versions comme svn ou cvs permettent à des personnes d'effectuer un travail collaboratif à distance.

Un premier objectif de la thèse est donc de modéliser, pour des documents XML partagés, une politique de sécurité via la définition d'un système de contrôle d'accès qui doit être préservé pendant le processus d'édition et adapté à un cadre non centralisé. Plus particulièrement, le but sera d'interdire aux

utilisateurs non autorisés d'atteindre des parties confidentielles du document pendant l'édition, afin d'éviter l'extraction et la diffusion de données protégées.

Une fois la politique de sécurité définie, il s'agira de la valider en vérifiant les propriétés usuelles pour les politiques de contrôle d'accès, telles que la correction, la complétude et la consistance. Par la suite, un prototype permettant de tester la mise en place d'un tel contrôle sur des exemples réels et d'étudier les optimisations possibles sera réalisé.

English version The recent growth of digital communication has increased the demand of security for protecting resources and preserving the integrity and confidentiality of data. The specification of formal security policies that are declarative (to handle the complexities of policy specification), and satisfy important properties such as consistency (for verifiability purposes), are especially needed in distributed computing environments where we access and exchange large volumes of data from multiple locations.

The current standard for documents exchanged on the net is the XML format and applications should deal with this format directly. Usually, XML documents are seen as unordered unranked trees and are typed using DTD or XML schemas.

Several models for describing security policies in this context exist (RBAC, DEBAC, WS-SecurityPolicy,...). Recently, rule-based specifications of access control policies have gained popularity, see e.g. XACML.

In particular, we are interested here in the security of shared documents that can be read and modified in an interactive and distributed way by several users. For instance shared agenda (doodle) or shared versioning systems (svn or cvs) allow people to work remotely on the same data.

The aim of this thesis is to is to design a framework for security policies for XML documents. More specifically, we want to design a powerful rule-based access control system which is preserved during editing in a decentralised setting. A particular goal of the model is to deal with confidential data in a document : their access must be forbidden to non-authorised users during editing, in order to avoid the retrieval and diffusion of protected information.

Once the security policy is defined, we will address the relevant verification issues, e.g. testing the usual properties of access control policies, such as correctness, completeness and consistency.

Finally, the realization of a prototype will allow to test the feasability of the framework and to study possible optimisations.

Prérequis Master recherche en Informatique.

Connaissances appréciées en : XML, Xpath, sécurité informatique, politique de sécurité et controle d'accès, service Web, logiques, méthodes de résolution symbolique. Programmation Java, langages orienté XML.