XML DOCUMENTS AND ACCESS CONTROL MANAGEMENT

LiLi Sun

BSc(Sci), MSc(Sci)

A Dissertation submitted for the degree of Doctor of Philosophy

The Department of Mathematics and Computing

The University of Southern Queensland

January 2010

Statement

I hereby declare that the work presented in this dissertation is my own and is, to the best of my knowledge and belief, original except as acknowledged in the text. It has not previously been submitted either in whole or in part for a degree at this or any other university.

Lili Sun

Signature of Candidate Date

ENDORSEMENT

Signature of Supervisor Date

Acknowledgement

I express my sincere gratitude and appreciation to many people who made this PhD thesis possible. I would like to thank my PhD supervisor Dr Yan Li of the University of Southern Queensland (USQ) for her general view on research, invaluable advice and encouragements during the realization of this research.

I sincerely thank the Department of Mathematics and Computing, Faculty of Sciences and Research and Higher Degrees office of USQ for providing the excellent study environment and the financial support. It is a great pleasure to study at the Department of Mathematics and Computing.

I also acknowledge all the help from those who carefully read the dissertation and made the English corrections.

Finally, my appreciation goes to my parents Lianshu Sun, Yuntao Cai, my husband Hua and daughter Nana for their love and affection. I could not be able to complete my PhD study without their encouragement and support.

Abstract

Security requirements of confidentiality, integrity and availability are essential for business online. With the growing acceptance of Extensible Markup Language (*XML*) technologies for documents and protocols, it is necessary that security should be integrated with *XML* solutions. *XML* was designed to transport and store data, especially over the Internet. Information exchanges on the Internet should meet precise protection requirements: fine-grained authenticity, secrecy, non-repudiation and access control. The requirements have to address for *XML* documents and *XML* applications [15]. *XML* has become an important universal language for the Internet-based business world [24]. An *XML* document can be generated from various resources with varying security requirements, such as Authentication, Authorization, Integrity, Signature, Confidentiality, Privacy and Digital Rights Management. According to these requirements, the main relevant developments of *XML* Security standards are [12, 15, 37]:

- *XML* Digital Signature,
- *XML* Encryption,
- *XML* Key Management,
- Security Assertion Markup Language (SAML),
- *XML* Access Control Markup Language (XACL).

XML is a fundamental component in many *XML* web services and it is used to store and exchange data in the Internet environment that may include private messages. It overcomes the complexity of Standard Generalized Markup Language (*SGML*) and the user can define document structures, removing the limit of the fixed tags in Hypertext Markup Language (*HTML*) [26]. *XML* Security therefore must be integrated with *XML* in such a way as to maintain the advantages and capabilities of *XML* while adding necessary security capabilities.

Traditional access control models for *XML* primarily consider static authorization decisions based on the subjects' permissions on target objects [91]. The models have been used only on the control of access to server-side objects and static authorization decisions are not assessed once an access permission is granted. Static authorizations for *XML* documents are performed without ongoing evaluating of query expressions against an actual database application. For example, a prepaid mobile needs ongoing checking to determine whether or not a call can continue or will be denied. To cope with these problems, recently proposed usage access control is a new access control model, which extended traditional access control models in multiple aspects: dynamic authentication, pre-authorization, ongoing-authorization, obligation and conditions [27].

In this dissertation, we aim to provide a bridge between the existing security technologies and the secure methods for *XML* documents. We extend existing web security technologies for *XML* documents. Usage access control models are analysed for *XML* schema and Document Type Definition (*DTD*) level authorizations. As validation of *XML* documents, technologies for *XML* databases have been enhanced and improved through usage access management. The theory developed in this dissertation can be applied in electronic services, such as E-learning. Role-based access

control (*RBAC*) is an access approach and permission-role assignments are main parts in *RBAC*. The new authorization algorithms for permission-role assignments in *RBAC* have been developed.

Publications Based on this Thesis

1. L. Sun and Y. Li, Using Usage control to access *XML* Databases, International Journal of Information Systems in the Service Sector, Vol. 1, No. 3, pages 32-44, July-September 2009.

2. L. Sun and Y. Li, *XML* and Web Service Security, The 12th International Conference on Computer Supported Cooperative Work in Design, Vol. 4823/2008, pages 765-770, IEEE, April 2008.

3. L. Sun and Y. Li, *XML* Schema in *XML* Documents with Usage control, International Journal of Science & Network Security, Vol. 6, pages 170-177, December 2007.

4. L. Sun, H. Wang and Y. Li, Protecting disseminative information in E-Learning, Advances in Web Based Learning -ICWL 2007, Vol. 4823/2008, pages 554-564, Springer, August 2007.

5. L. Sun and Y. Li, DTD Level Authorization in *XML* Documents with Usage control, International Journal of Science & Network Security, Vol. 6, pages 244-250, November 2006.

Contents

List of Figures

List of Tables