Ain Shams University Information Network
جامعة عين شمس
شبكة المعلومات الجامعية
@ ASUNET
شبكة المعلومات الجامعية

بسم اللّه الرحمن الرحيم

Ain Shams University Information Network

جامعة عين شمس

شبكة المعلومات الجامعية

@ ASUNET

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

Ain Shams University
Faculty of Computer & Information Sciences
Computer Science Department

A Multi-Agent Based Framework for Managing Security Policies

Thesis submitted as a partial fulfillment of the requirements for the degree of Master of Science in Computer and Information Science.

By

Mohamed Al-Morsy Abd Al-Razek
B.Sc. in Computer Science.
Demonstrator in Computer Science Department,
Faculty of Computer and Information Sciences,
Ain Shams University.

Under Supervision of

Prof. Dr. Taha El-Aref
Professor of Computer Science
Faculty of Computer and Information Sciences,
Ain Shams University.

Dr. Hossam M. Faheem
Associate Professor of Computer Systems
Faculty of Computer and Information Sciences,
Ain Shams University.

Cairo 2009

ABSTRACT

The revolution of new technologies and internet has motivated organizations expanding their networks to provide more services to customers and employees. Although the benefits gained, organizational assets become more vulnerable. Security become an important concern in today networked environments. As the underlying environments are complicated and dynamic, Security solutions should be flexible, scalable, and can integrate to achieve organizational security needs.

Policy-based management, as one of the latest approaches for network, distributed systems, and security management, ia promising solution for the security management problem. It introduces security policies as abstraction of the business needs away from security solutions that implement the business needs. Security policy specification, security policy configuration, security policies conflicts detection, policy enforcement, and deployment are critical issues that need to be clearly defined any policy-based management. With the increase of the organization scale, security officers exert more efforts to cover the organizational security needs and impact of changes in business objectives, hence come the need to automated security policy management system.

The Proposed framework is a new idea in automating the security policy management process. The framework is based on mobile agents. It provides an XML/Ontology-based standard security policy language (SSPL), architecture for deploying policies based on SSPL, security solutions integration interface, and a set of helping tools for specifying

and managing policies. The SSPL is aimed to be a standard, formal and readable security policy specification language. It helps in eliminating problems of writing security policies in natural languages or the developed security policy specification languages. The XML technology gives SSPL the formalization (in syntax) while ontology adds the semantics and analyzing capabilities to SSPL.

The proposed architecture simplifies/automates the mapping phase among security policies and security solutions by introducing abstraction tier between policy development tier and security solutions tier and using mobile agents for communication among them.

The proposed security solutions integration interface is a software driver that defines and manages how security solutions integrate with the proposed framework. It acts as a communication channel between the framework and the security solutions deployed.

The framework eliminates ambiguities of using natural languages in specifying security policies, eliminates the needs to learn many of the existing security policy specification languages to be able to specify the whole organizational security policies, eliminates difficulties associated with configuring heterogeneous security solutions, and automates the impact of the changes in security policies configurations. The framework is designed to be as flexible and extensible to cover new policies, new policy domains, and capable to integrate with new security solutions seamlessly.

ACKNOWLEDGMENT

I would like to express my gratitude to my supervisor Dr. Hossam M. Faheem whose expertise, understanding, and patience, added considerably to my experience and finishing this work. Also, my most profound gratitude goes to my family who has been the timeless source of inspiration for me; especially my great wife, to whom this thesis is dedicated.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES