Analysis of Authorization Framework and its Implementation

A Project

Submitted to:
Central Department of Computer Science and Information Technology,
Tribhuvan University,
Kirtipur, Nepal

In Partial Fulfillment of the Requirements for the Degree of
Master of Science
In
Computer Science and Information Technology

Submitted by
Pushpendra Singh Bhandari
CDCSIT, TU

(December, 2011)

Analysis of Authorization Framework and its Implementation

A Project

Submitted to:

Central Department of Computer Science and Information Technology,

Tribhuvan University,

Kirtipur, Nepal

In Partial Fulfillment of the Requirements for the Degree of

Master of Science

In

Computer Science and Information Technology

Submitted by

Pushpendra Singh Bhandari

CDCSIT, TU

Supervisor: Assoc. Prof. Dr. Subarna Shakya

Tribhuvan University
Institute of Science and Technology
Central Department of Computer Science and Information Technology
Kirtipur, Kathmandu, Nepal

Date_______________

Recommendation

I hereby recommend that the project work done under my supervision by **Mr. Pushpendra Singh Bhandari** entitled "**Analysis of Authorization Framework and its Implementation**" be accepted as a partial fulfillment for the degree of Master in Computer Science and Information Technology, from Tribhuvan University, Nepal. To my best knowledge this is an original work in the computer science.

……………………………………………..…

Assoc. Prof. Dr. Subarna Shakya
Department of Electronics and Computer Engineering,
Institute of Engineering, Pulchowk, Nepal
(Supervisor)

Tribhuvan University
Institute of Science and Technology
Central Department of Computer Science and Information Technology

We certify that we have read this project work and in our opinion it is satisfactory in the scope and qualify as a project in the partial fulfillment for the requirement of Master of Science in Computer Science and Information Technology.

Evaluation Committee

____

Assoc. Prof. Dr. Tanka Nath Damala
Head, Central Department of Computer
Science and Information Technology,
Tribhuvan University, Nepal

____

Assoc. Prof. Dr. Subarna Shakya
Department of Electronics and Computer
Engineering, Institute of Engineering,
Pulchowk, Nepal
(Supervisor)

____
(External Examiner)

____
(Internal Examiner)

Acknowledgement

I deeply express my heartily acknowledgement to my respected teacher and dissertation advisor **Assoc. Prof. Dr. Subarna Shakya,** Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk, for his wholehearted cooperation, encouragement and strong guidelines throughout the preparation of this study. With this regard, I wish to express my sincere appreciation to the respected Head of the Central Department of Computer Science and Information Technology, Assoc.Prof. Dr. Tanka Nath Damala for his kind help.

I am very much grateful and thankful to all the respected teachers Prof. Dr. Shashidhar Ram Joshi, Prof. Dr. Onkar P. Sharma (Marist College, USA), Mr. Sudarshank Karanjit, Mr. Min Bahadur Khati, Mr. Bishnu Gautam, Mr Hemanta G.C, Mr Dinesh Bajracharya and others for granting me broad knowledge and inspirations within the time period of two years of study.

I wish to express my profound gratitude of my parents and all my family members for their constant support and encouragement. My special thanks goes to my dear friends Sharmila Thapa, Mohan Kumar Niroula, Jagendra Khadka, Krishna Godar, Susil Pahari and to all those who directly or indirectly extended their hands in making this project work a success.

Dedicated

to

my parents

Abstract

As more resources are being made available over the internet and intranet, it is important to ensure that appropriate resources are accessed by appropriate users. In a large scale service oriented computing environment where thousands of computers, storage systems, networks, scientific instruments and other devices distributed over wide area networks presents unique security problems that are not addressed by traditional client-server/distributed computing environments. Thus, a need for authorization is required.

Authorization implementation enables users and organizations to have secure, protected, and private access to remote services. It has been found that early design of authentication and authorization eliminates a high percentage of application vulnerabilities. This thesis report focuses on need for an authorization, its requirements and how access of the protected resources from unauthenticated users in a distributed, web-based system is controlled by using the several controls and mechanisms provided by various authorization techniques and tools. This thesis focuses on Shibboleth, the most widely used automated authentication and authorization tool. It is a system designed to exchange information across realms for authentication and authorization.

Finally, an implementation is shown demonstrating how an authorization can be used in an organization to ensure a secure access to the protected resources based on different access controls.

Table of Contents

Details **Page No:**

List of Tables

Details **Page No**

List of Figures

Details **Page No.**

List of Abbreviations

AAA	Authentication, Authorization and Accounting
AA	Attribute Authority
AAP	Attribute Acceptance Policies
AC	Access
ACM	Access Control Mechanisms
ACS	Assertion Consumer Service
AP	Authentication Policy
AR	Attribute Requester
ARP	Attribute Release Policies
ATA	Authentication Agents
AUA	Authorization Agents
AUP	Authorization Policy
CA	Certification Authority
CEO	Chief Executive Officer
DO	Domain
DP	Domain Policy
FAA	Foreign Authorization Agents
FDA	Foreign Delegation Agents
FQAN	Fully Qualified Attribute Names
HS	Handle Service
IA	Interface Agents
IDP	Identity Provider
IIS	Internet Information Service
ISP	Internet Service Provider
IT	Information Technology
MP	Management Policy
NAA	Native Authorization Agents
PAP	Policy Administration Point
PDP	Policy Decision Point

PEP	Policy Enforcement Point
PIP	Policy Information Point
PO	Policy
PP	Privacy Policy
PRP	Policy Retrieval Point
R	Resource
RBAC	Role Based Access Control
RM	Resource Manager
SAML	Security Assertion Markup Language
SHIBD	Shibboleth Daemon
SP	Service Provider
SPKI	Simple Public Key Infrastructure
SR	Service
SSO	Single Sign On
SU	Subject
TP	Trust Policy
WAYF	Where Are You From
XACML	Extensible Access Control Markup Language