



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. Pushendra 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:
CHAPTER 1	1-7
1. INTRODUCTION	1
1.1 Background	1
1.2 Overview	3
1.3 Problem Definition	5
1.4 Objective	6
1.5 Thesis Organization	7
CHAPTER 2	8-30
2. ANALYSIS OF AUTHORIZATION	8
2.1 Authentication Vs Authorization	8
2.2 Access Control Mechanisms	11
2.3 Implementation of Security Service Environment	12
2.4 Elements of the security service environment	14
2.4.1 Interface agents	14
2.4.2 Authentication agents	14
2.4.3 Authorization agents	15
2.5 Authorization Framework Elements	16
2.6 Access Control	19
2.6.1 Access Control Technologies	19
2.6.2 Access Control Models	24
2.6.3 Access Control Techniques	25
2.7 Authorization Process	27

CHAPTER 3	31-41
3. METHODOLOGY	31
3.1 Automated Authentication and Authorization Tool (Shibboleth)	32
3.1.1 Identity Provider (IDP)	33
3.1.2 Service Provider (SP)	34
3.1.3 Where are you from? (WAYF)	34
3.1.4 Federations	35
3.1.5 Relying Parties	35
3.1.6 Applications	35
3.2 The working structure of Shibboleth system	36
3.2.1 Authentication Procedure	36
3.2.2 Shibboleth Flow	38
3.2.3 Advantages of using Shibboleth	39
3.2.4 Requirements of Shibboleth Identity Provider (IDP)	40
3.2.5 Requirements of Shibboleth Service Provider (SP)	40
CHAPTER 4	42-67
4. DESIGN AND IMPLEMENTATION	42
4.1 Concept Development	42
4.2 Implemented Roles in System	42
4.3 Flowcharts for Different Role Permissions	46
4.4 Security Defined for different Modules	50

4.5	User Interfaces	53
4.5.1	Company Interfaces	53
4.5.2	Department Interfaces	54
4.5.3	Project Interfaces	56
4.5.4	User Interfaces	58
4.5.5	User Group Interfaces	60
4.5.6	Project Team Interfaces	62
4.5.7	Service Request Interfaces	64
CHAPTER 5		68
5.	CONCLUSION	68
REFERENCES		69-70

List of Tables

Details	Page No
Table 4.4.1: Access control for company module	50
Table 4.4.2: Access control for department module	50
Table 4.4.3: Access control for User module	51
Table 4.4.4: Access control for User Group module	51
Table 4.4.5: Access control for Project module	52
Table 4.4.6: Access control for Project team module	52
Table 4.4.7: Access control for Service Request module	52

List of Figures

Details	Page No.
Figure 2.1: Authentication vs. Authorization	9
Figure 2.3: Security service environment	13
Figure 2.4.2: Authentication agent architecture	15
Figure 2.4.3: Authorization layer	16
Figure 2.5: Distributed Environment with two domains along with framework elements	18
Figure 3.2: The Structure of Shibboleth System	36
Figure 3.2.1: Authentication procedure	37
Figure 3.2.2: Shibboleth Flows	38
Figure 4.2: Entity Relationship Diagram of the proposed model	45
Figure 4.3.1: Access control for creating company, department and projects	46
Figure 4.3.2: Access Control for creating user and assign groups	47
Figure 4.3.4: Access control for adding users and assign Project roles to team-members	48
Figure 4.3.5: Access control for creating SRs, setting and updating various values	49
Figure 4.5.1.1: Company Interface for Host User	53
Figure 4.5.1.2: Company Interface for Non Host User	54
Figure 4.5.2.1: Department Interface for Host User	55
Figure 4.5.2.1: Department Interface for Non Host User	56
Figure 4.5.3.1: Project Interface for Host User	57
Figure 4.5.3.2: Project Interface for Non Host User	58
Figure 4.5.4.1: User Interface for Host User	59
Figure4.5.4.2: User Interface for Non Host User	60
Figure4.5.5.1: User Group Interface for Host User	61
Figure4.5.5.2: User Group Interface for Non Host User	62
Figure 4.5.6.1: Project Team Interface for Host User	63
Figure 4.5.6.2: Project Team Interface for Non Host User	64

Figure 4.5.7.1: Service Request Interface for Host and Non Host User	65
Figure4.5.7.2: Service Request Interface in Update Mode for Host User	66
Figure4.5.7.3: Service Request Interface in Update Mode for Non Host User	67

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