APPLYING ROLE BASED ACCESS CONTROL FOR INTRANET SECURITY

A PROJECT REPORT PRESENTED BY

H.B. KOTUWEGEDARA

to the Board of Study in Statistics & Computer Science of the

POSTGRADUATE INSTITUTE OF SCIENCE

in partial fulfillment of the requirements
for the award of the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

of the

UNIVERSITY OF PERADENIYA

SRI LANKA

2010

APPLYING ROLE BASED ACCESS CONTROL FOR INTRANET SECURITY

H. B. Kotuwegedara

Postgraduate Institute of Science

University of Peradeniya

Peradeniya

Sri Lanka

Today most of the organizations use intranet based computerized systems. Their all valuable information is stored in those computerized systems and should protect from access of unauthorized people. Therefore, in an organizational environment, users are not allowed to access each and every network resources as they wish. Resources in an organization intranet such as file server, web server are allows to access relevant users only. But it is a challenge to allow and constraint to access intranet resources in that way. The main reason for this problem is identified as inaccurate user authenticates and user authorization of current access control systems.

As a solution to that problem, this project is proposed an implementing Role Based Access Control for organizational intranets. After, identifying security structure and polices of the organization it was developed and implemented with using mordent software techniques. In developing the system, intranet servers, network objects, users and intranet environment were also considered.

According to the organizational security policies, permissions are created over server, and network objects (all the resources which are located in servers). All these permissions are collected and assigned to roles in relevant way. Roles are divided into Global Roles and Local Roles. Global Roles define permissions to access intranet servers and Local Roles define how to access network objects located on each server. Finally created roles are assigned to the system users according to the organization policies.

In this way, only correct users receives correct permissions to access both servers and their network objects according to their daily duties