CRITICAL SECURITY ISSUES FOR ORGANISATIONS IN TRANSITION FORM IPV4 TO IPV6

By

Gayantha Mendis

058268

This dissertation was submitted to the
Department of Computer Science and Engineering of the University of Moratuwa
in partial fulfillment of the requirements for the Degree of

Masters in Computer Science specializing in Computer Networks

University of Moratuwa

92296

Department of Computer Science and Engineering

University of Moratuwa - Sri Lanka

April 2008

DECLARATION

In accordance with the requirements of the Degree of Master of Computer Science in Specialization of Computer Networks, I wish to present the following thesis entitled "Security Issues on network that are in transition from IPv4 to IPv6" to fulfill my Master's research project. This work was performed under the supervision of Mr. Mr. Shantha Fernando - Senior Lecturer / Chartered Engineer in IT– University of Moratuwa and Mr. Priyanka Jayatilake Partner, KPMG Ford Rhodes Thornton & Co

I declare that the work submitted in this thesis is my own, except as acknowledged in the Text and footnotes, and has not been previously submitted in part or as whole to any other university or institution.

Gayantha Mendis
058268

Certification of Research Supervisors

I hereby certify the work presented in the dissertation is a work carried out by Gayantha Mendis under our supervision.

UOM Verified Signature

Mr. Shantha Fernando
Research Supervisor

25/04/'08
Date

UOM Verified Signature

Mr. Priyanka Jayatilake
Research Supervisor

24/4/08
Date

Abstract

In 1994, the Internet Engineering Task force embarked on the IP Next Generation (IPnG) project which ultimately aimed to draft a replacement for IP version 4, the protocol that facilitated the birth of the world wide web and numerous other services while sustaining for more than 30 years.

In 1998, the first blue print of the IPnG was cleared and IP version 6 was designated as the rightful replacement. Despite the efforts to increase the longevity of the previous version, IPv6 has slowly but steadily made it's way to commercial networks, making the question "Is it safe to migrate and is the migration safe?" a timely one in today's context.

Contributing to the above thought, this research was conceded to establish some "Critical Security Issues for organizations in Transition from IPv4 to IPv6". The research herein aimed to surface numerous security issues and oversights, which a typical organization encounter while in the transition.

Firstly, a firewall's migration towards an IPv6 ready network was considered followed by a "web server" migration. These two platforms were selected, as a "firewall" would be one network device that shows the most sensitivity towards change in the IP protocol and related network topological changes and, a "web server" would be one of the first servers to be linked to the IPv6 network showing sensitivity towards the IPv6 changes made on the Operating system it resides, the client browsers, the IPv6 DNSs and the IPv6 network which it operate.

This thesis also has made a number of contributory findings & recommendations along the way especially with reference to variations of implementations in Dual Stacks and associated vulnerabilities of it.

Overall, the thesis aims to assist practitioners such as IT Security Consultants and Network Administrators, who do not necessarily have the time to go through a large body of literature on a crucial topic in todays' context.

Keywords: IPv4, IPv6, IPv4-IPv6 Transition, IPv4-IPv6 Transition Security, IPv6 Network Design

Acknowledgements

This dissertation has been carried out in the Department of Computer Science and Engineering, University of Moratuwa during the year 2006/07. First of all, I wish to express my sincere gratitude to my supervisors, Mr. Priyanka Jayatilake and Mr. Shantha Fernando for their inspiring support and counseling whenever called upon during the course of this study. Without their excellent guidance this work could not have reached completion.

I would also like to thank the preliminary examiners of this dissertation, namely Professor G. Dias, Dr. C Gamage and Mr. S Fernando of the Department of Computer Science and Engineering, University of Moratuwa for their insightful comments on the thesis.

I am also grateful to KPMG for an inspiring working environment and providing me with the possibility to test my ideas in real organization. Special thanks go to my fellow skilful IS security professionals at Information Risk Management (IRM) for fruitful co-operation and interesting and inspiring professional discussions.

My sincerest thanks are due to my family. Before all others, I wish to express my deepest gratitude to my parents "Ammi" and "Thaththi" and my wife "Gayathri" for her love and immense support throughout this MSc research process.

This research has been supported in its different phases by numerous people, colleagues. Without such support, completing the present study would have been much harder.

Table of Contents

Table of Figures