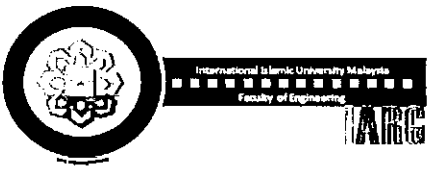
Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM PRESS
2011



Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM Press
2011

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Mohammad Umar Siddiqi, Sigit Puspito Wigati Jarot and Othman Omran Khalifa: Topics in Coding, Cryptography and Information Security

ISBN: 978-967-418-169-7

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

Topics in Coding, Cryptography and Information Security

Contents

Chapter 19

Secure IPv6 Address Generation

Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot

19.1. Introduction

This chapter gives an overview of IPv6 address generation and the underlying security implications. IPSec is a mandatory protocol in IPv6 for providing base security in IP layer. IPv6 addresses may be generated in stateless or stateful mode. Many researches have been proposed to improve the security of IPv6 address generation.

The chapter is organized as follows: Section 19.1 describes an introduction to IPv6 and IPv6 address definition. Section 19.2 explains related work in IPv6 security. Section 19.3 explains existing mechanisms for IPv6 address generation. Section 19.4 shows the current research in IPv6 address generation and its security implications. Finally, Section 19.5 summarizes the chapter.

19.1.1. IPv6

An IP (Internet Protocol) address is a unique address which is used to identify electronic devices that communicate with each other in a computer network utilizing the IP. Almost all IP today is still using IPv4 (internet protocol version four) which has 32 bit address space[1]. Meanwhile, since 1990s researchers started realizing the limitation of the IPv4 in terms of the address space. IPv4 network has been growing beyond the design intention so that all the central IPv4 address pools will be depleted by 2015 [2].

For that reason and also experiences gained from the IPv4 development, a next generation protocol, IPv6 (IP version six) has been proposed to solve the problem of IP address depletion and also making the IP protocol more efficient, secure and flexible. For example, IPv6 uses 128 bits to represent IP address which can get 340, 282,366,920,938,463,463,374,607,431,768,211,456 compared to IPv4 that uses "only" 32 bits. This change provides us with almost unlimited number of address so that IP address space will not be problem anymore. If we calculate the IP address density on the earth surface, we can assign 3.4 trillion IP address per square centimeters of earth surface. This will allow us to give a unique (global) IP address to almost any device conceivable in the future.