IGI PUBLISHING **ITB14889**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Web Services Security and E-Business**
edited by **G. Radhaman & G. S. V. Radha Krishna Rao © 2007, IGI Global**

Chapter XIX

IPSec Overhead in Dual Stack IPv4/IPv6 Transition Mechanisms: An Analytical Study

M. Mujinga, University of Fort Hare, South Africa

Hippolyte Muyingi, University of Fort Hare, South Africa

Alfredo Terzoli, Rhodes University, South Africa

G. S. V. Radha Krishna Rao, University of Fort Hare, South Africa

Abstract

Internet protocol version 6 (IPv6) is the next generation Internet protocol proposed by the Internet Engineering Task Force (IETF) to supplant the current Internet protocol version 4 (IPv4). Lack of security below the application layer in IPv4 is one of the reasons why there is a need for a new IP. IPv6 has built-in support for the Internet protocol security protocol (IPSec). This chapter reports work done to evaluate implications of compulsory use of IPSec on dual stack IPv4/IPv6 environment.

Introduction and Background

The Internet protocol (IP) is the protocol that operates at the backbone of the Internet, and networking in general. The initial IP was first published in 1981, in RFC 791 [DARPA IP Spec., 1981] and is now generally known as IPv4. Internet protocol version 6 (IPv6) is the next generation Internet protocol proposed by the IETF in RFC 2460 (Deering & Hinden., 1998; Doraswamy & Harkins, 1999), published in 1998 to supplant IPv4. IP security (IPSec) is provided by a set of protocols, the main protocols being authentication header (AH) and encapsulating security payload (ESP) protocols (Kent & Atkinson, 1998). IPSec operates at the network layer in a way that is completely transparent to the applications, and much more powerful, because the applications do not need to have any knowledge of IPSec to be able to use it (Farrel, 2004). In IPv4, IPSec headers are inserted after the IPv4 header and before the next-layer protocol header. While with IPv6, this is applied in the form of additional extension headers (Loshin, 2003). This obviously increases the overhead of an IP datagram, and since this protocol is mandatory on IPv6, this overhead becomes increasingly significant.

There was some research done on the performance implications of IPSec deployment. In Ronan et al. (2004), the authors evaluated the performance overheads under a range of different bandwidth and different processors, on throughput and processor; single and dual, when communicating over a secured VPN on IPv4 infrastructure, using Linux 2.6.1 kernel. The findings showed that the overhead differs from one processor type to the other, and this was consistent when dual processors were used of the same type. The other work (Ariga et al., 2000) evaluated the performance of data transmissions with IPv4 and IPv6 networks. The results showed that IPSec obviously degrades the network performance in terms of throughput and end-to-end delay for the large data transmission and for the actual application. The authors concentrated on digital video (DV) transmission as the application. Their results showed that, for large data transmissions, when authentication and encryption are applied, the throughput degrades to 1/9 compared with the throughput without authentication or encryption.

Dual stack translation mechanism (DSTM) was our primary method in the IPv6 experiments; 6to4 in particular. 6to4 is a tunneling addressing mechanism that enables communication between two IPv6 computers that live in an IPv4 environment (Carpenter & Moore, 2001). In this paper, we will investigate the cost in terms of performance when transmitting traffic on computer networks, with IPSec enabled on IPv4 and IPv6. Our research focuses on Windows IPv6 and IPSec implementations, and evaluates a variety of IP traffic over HTTP, FTP, TFTP, and ICMP protocols. We evaluated the additional frame overhead induced by IPSec on both IPv4 and IPv6 on these protocols, noting also its impact on average round-trip times. This is achieved by comparing traffic with IPSec on and IPSec off. The research we are conducting will give an insight into the quantitative expense, which the mandatory use of IPSec will bring into our networks, and we will give a model of how and when to use it on your network. Knowing when and how to deploy IPSec efficiently will help to save two of our most valued resources in the Internet community: the scarce and expensive bandwidth and computer processing power.