[5B-89]

Design of IPSec Hardware Accelerator IP

Chang-Soo Ha, Joo-Hong Kim*, Hyun-Sook Cho**, Myoung-Soo Park*** and Byeong-Yoon Choi**

***Dept. of Computer Engineering, Dong-Eui University,**
Gaya-Dong, Jin-Ku, Busan, 614-714, Korea
****ETRI, ***Glotrex Corporation**

Abstract

This paper describes ASIC design of IPSec hardware accelerator for network security which can execute tunnel-mode AH and ESP algorithm of IPSec protocol suite. The processor supports AES-128/192/256, TDES, HMAC-MD5 and HMAC-SHA-1 algorithm to encrypt and authenticate the packet data and operates as hardware coprocessor to accelerate cryptographic routine of FreeS/WAN software. The IPSec hardware accelerator consists of AMBA interface, 2KB packet memory, parameter registers, global controller, and cryptographic module. It was designed using 0.25um CMOS standard cell library and consists of about 80K gates and 2KB memory. Its throughput of ESP-AES128-HMAC-SHA1 operation is approximately 200 Mbps at 125Mhz for 120-byte test packet.

1. Introduction

The need for securing the Internet has become a fundamental issue over the last decade and the Interest Protocol Security (IPSec) protocol suite which incorporates cryptographic and authentication algorithms, has been developed as one solution to this problem. It is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. These services are provided at the IP layer below the transport layer, making it transparent to applications and users, meaning there is no need to change network application on a user's desktop when IPSec is implemented in the firewall router. Typically, hardware implementations of cryptographic algorithms provide physical security and high speeds. Several of the operations that need to be done on the incoming and outgoing traffic to guarantee security, are very resources demanding. This is why it is interesting to perform these operations in application specific hardware, instead of software running in an ordinary CPU. An implementation of IPSec in software will put heavy load on the CPU.

With recent development of very large scale integration (VLSI) circuit and field programmable gate array (FPGA) technology, researches on hardware implementation of cryptographic algorithm are on the increase [1]. The goal of this research is to investigate how IPSec can be implemented efficiently in a conventional network processor (*VIOLIN* Processor) [2] developed by Glotrex Inc in Korea.

This paper is arranged as follows. In section 2, a brief description of IPSec is presented. Design details of IPSec hardware accelerator is explained in Section 3 and its performance figures are provided in section 4. Section 5 contains some concluding remarks.

2. IPSEC Protocol suite

There are numerous security solutions at high levels within the OSI model. The problem of the above algorithms is that each algorithm can only be applied to dedicated application. It would be better to move our security efforts to a lower level within the OSI model. IPSec has been developed as one solution to this problem [3].

IPSec(Internet Protocol Security Architecture) operates at Network Level. All communication applications can take advantage of IPSec security efforts. Interest Protocol Security (IPSec) protocol suite is a set of the IP protocol and is used to provide privacy and authentication services at the IP layer. The set of security services offered includes authentication, confidentiality, data integrity, and dynamic replay protection. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP). Both the AH and ESP are used in accordance with a security association (SA). The security association is the agreement between two or more bodies on the security services.

IPSec supports two methods of operation, tunnel-mode and transport mode. In transport mode, only the upper-layer protocol data segment of the IP packet is authenticated or encrypted and is typically used for end-to-end protection of data packets between two hosts. In tunnel-mode the entire IP packet is authenticated or encrypted. Tunnel mode can be used between firewalls to create a virtual private network (VPN).

2.1. ESP

ESP provides confidentiality by the use of encryption algorithm and provides data source authentication and data integrity by the use of one-way hash function. Resistance to replay attacks is accomplished by the use of a sequence number. Figure 1 shows an ESP packet in tunnel mode. The algorithms to implement ESP are as follows:

- TDES and AES in CBC mode
- HMAC with MD5 and SHA-1