경제적인 VPN 시스템 구축을 위한 2-Chip 기반의 암호가속기 성능분석

이완복* · 김정태**

Performance Analyses of Encryption Accelerator based on 2-Chip Companion Crypto ASICs for Economic VPN System

Wan-Bok Lee* · Jung-Tae Kim**

요 약

본 논문은 저비용 고성능으로 패킷암호 처리를 할 수 있는 VPN 시스템의 구조와 그 설계에 대해서 소개한다. 제안하는 시스템 구조는 보안장비용 다기능 네트워크 프로세서와 전용 암호패킷 처리 칩의 2개의 컴페니언 칩들로 구성되어 있으며, 즉각적인 활용을 위해 필요한 운영체제의 구축 및 디바이스 드라이버, 컴파일러와 이를 기반으로 한 IPSec VPN의 핵심 엔진에 대해 구축한 방안이 언급된다. 특히, 계산력을 많이 필요로 하는 블록 암호 알고리즘인 3DES, AES, SEED는 별도의 칩으로 구현되어 범용성이 뛰어난 것이 특징이며, 이 칩의 성능 평가 결과를 소개한다.

ABSTRACT

This paper describes about the design concept and the architecture of an economic VPN system which can perform fast crypto operations with cheap cost. The essence of the proposed system architecture is consisting of the system with two companion chips dedicated to VPN: one chip is a multi-purpose network processor for security machine and the other is a crypto acceleration chip which encrypt and decrypt network packets in a high speed. This study also addresses about some realizations that is required for fast prototyping such as the porting of an operating system, the establishment of compiler tool chain, the implementation of device drivers and the design of IPSec security engine. Especially, the second chip supports the most time consuming block cipher algorithms including 3DES, AES, and SEED and its performance was evaluated.

키워드

VPN, ASIC, 암호가속, 정보보안

Ⅰ. 서 론

VPN 시스템은 기본적으로 통신하는 모든 데이터 패킷들을 암호화하는 메카니즘에 의해 보안성을 구축하기 때문에, 저렴한 가격에 고성능의 장비를 개발하려면 전용의 암호가속카드를 제작하여 사용하는 것이 필수적으로 요구된다.[1][2] 특히 암호화 연산은 단순한 연산 모듈로 구성되어 있으나, 암호화 강도를 높이기 위해 많은 반복 연

* 중부대학교 컴퓨터 · 게임학부
** 목원대학교 정보전자영상공학부

접수일자 : 2006. 1. 5

산을 동원하고 있기 때문에 범용 프로세서를 이용하여 소프트웨어적으로 처리하는 것 보다 전용 하드웨어를 이용할 때 그 효율성이 극대화되며 고비도의 암호 성능을 보장할 수 있게 된다. 최근에 발표되는 암호 프로세서 들은 크게 두 부류로 구분 된다. 즉, 성능 최적화된 High-end 제품 군과 많은 페리퍼럴을 확보하여 원칩화된 시스템 구현이 용이한 Low-end 제품군이 그것이다. 이외에도 모바일 환경에서의 적용을 위한 저전력 소모를 특성을 강조한 제품군이 등장할 것으로 추측된다. High-end 제품군에 속한 칩셋 들은 암호 알고리즘의 성능 향상을 위해서 다중 대칭키 연산 코어를 내장한 칩셋이 그 주류를 형성하고 있으며, 암호 연산 자체를 고속화 하는데 초점을 맞춘 제품들이다. 또한, 이 제품군의 성능 다운그레이드를 통한 Low-end 제품군이 존재한다. 이밖에 암호 알고리즘 코어와 범용 Processor를 내장하고, MAC등 주변 인터페이스를 내장하여 최소 주변 회로로 브로드밴드 급 네트웍 보안 장비를 만들 수 있도록 설계된 제품군이다. 국외에서는 Hifn[3], Broadcom, Analog Device사 등 다수의 해외 업체들이 암호가속 칩을 개발한 바 있으며, 이 들 칩을 이용하여 암호가속 카드를 제작한 사례들이 있다. 그러나, 외산 칩들은 기본적으로 국내 표준 블록 암호 알고리즘을 제공하지 않으며, 암호엔진을 공개하지도 않기 때문에, 국내 시장에 적용하거나 임베디드 프로세서 내에 암호엔진을 추가하는 것이 어렵다. 이러한 배경에서 국내 (주)시큐어넥서스는 경제적인 VPN 시스템 구축을 할 수 있는 2칩 기반의 솔루션을 마련하였다. 한 칩은 보안장비용 다기능 네트워크 프로세서이며, 다른 한 칩은 전용 암호 가속 칩이다. 본 논문에서는 이 두 칩의 기능과 특징 등에 대해 소개하며, 암호가속 칩의 경우, 제공되는 암호가속 보드를 이용하여 측정한 성능 결과를 소개한다.

논문의 구성은 다음과 같다. 2장에서는 2칩 컴페니언 암호 ASIC의 구성에 대하여 소개하며, 3장에서는 시스템 구축을 위해 고려해야 할 각종 요소들에 대해 언급한다. 4장에서는 개발된 암호가속 보드의 성능을 평가하였으며, 5장에서 결론을 맺는다.

Ⅱ. 2칩 컴페니언 암호 ASIC의 구성

2.1 보안장비용 다기능 네트워크 프로세서

네트워크 프로세서는 RISC 코어와 각종 암호화 엔진 및 네트워크 인터페이스를 포함한 표준 인터페이스를 내장하고 있어서 암호화 기술에 기반한 네트워크용 보안 장비의 제작에 핵심 부품으로 사용될 수 있다. 초기 VPN 제품들은 개발에 있어 접근이 유리한 x86 프로세서 등의 범용 프로세서 기반에 소프트웨어 형태로 VPN 기능을 구현하였다. 하지만 시장이 성장하고 기술이 성숙됨에 따라 가격 경쟁력 있는 제품은 끊임없이 요구되고 있고, 이미 기술 선진국에서는 암호화 전용 프로세서를 이용하여 VPN 장비를 설계하는 것이 기본이 되고 있다. 특히 SOHO(*Small Office Home Office*)나 *SME*(*Small and Medium Enterprise*)를 위한 저가형 VPN 시장에서는 IPSec 엔진과 RISC계열의 프로세서가 일체형으로 구현된 ASIC을 기반으로 한 저가의 고성능 VPN 장비 제작이 절실히 요구되고 있다. 다기능 네트워크 프로세서는 350pin PBGA 형태의 칩으로, RISC 프로세서를 내장하고 있으며 대표적인 대칭키 알고리즘(DES/3DES)과 해쉬 알고리즘(MD5/SHA-1)을 지원하는 보안장비 전용 프로세서이다. 네트워크 접속을 위해 3개의 이더넷 MAC을 내장하고 있으며, SEED 또는 국가형 알고리즘의 하드웨어(Chip)의 수용을 위해 별도의 PCI 보드와 연동할 수 있도록 PCI 인터페이스를 내장하고 있다. 세 개의 이더넷 MAC을 내장한 것은 본 네트워크 프로세서가 단지 VPN 장비만이 아니라, 라우터나 개인용 IDS, IPS 또는 방화벽과 같은 다양한 네트워크 장비 구축에 활용될 수 있기 위함이다. 가령 방화벽 구축시에는 내부 네트워크(LAN), 외부 네트워크(WAN) 외에도 DMZ라 불리는 중간수준의 보안 영역이 구축되는 경우가 자주 있기 때문이다.

일반적으로 네트워크 보안용 암호화 장비 H/W를 구성하기 위해서는 다음과 같은 부품이 필요하다.

- Main Processor:
  운영체제, 응용프로그램의 구동을 위한 프로세서
- Security Processor:
  각종 암호화 연산의 가속을 위한 코프로세서
- PCI Controller:
  프로세서간의 인터페이스를 위한 PCI 컨트롤러
- Memory:
  Flash 메모리와 DRAM 등의 외부 메모리
- *Ethernet MAC & PHY*:
  이더넷 인터페이스를 위한 칩셋

이러한 부품들을 집약하기 위해 네트워크 프로세서는 그림 1의 블록도에서 알 수 있듯이 주 프로세서와 암호화 연산을 위한 코프로세서, 이더넷을 위한 MAC, 추가적인 외부 인터페이스를 위한 PCI 컨트롤러, 각종 페리퍼럴이 하나의 칩으로 구현되어 있어야 한다. 따라서, 다기능 네트워크 프로세서는 네트워크 보안장비에 있어서 핵심 부품이 되며 장비 제작에 있어서 추가 부품을 최소화 할 수 있게 된다.

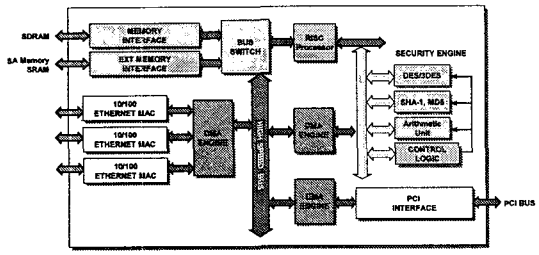

그림 1. 다기능 네트워크 프로세서 칩의 블록 다이어그램
Fig 1. Block Diagram of Network Processor with Various Function

2.2 전용 암호 패킷 처리칩

전용 암호 패킷 처리칩은 상기 네트워크 프로세서와는 달리 일반 연산을 위한 프로세서를 탑재하지 않기 때문에 x86 프로세서나 상기의 패킷 프로세서에 암호화 가속을 위한 코 프로세서 형태로 사용된다. 네트워크 프로세서와 마찬가지로 VPN 또는 SSL/TLS 장비와 같이 암호화 연산을 필요로 하는 장비에 널리 사용될 수 있다. 특히, 국내 표준 블록 암호 알고리즘인 SEED를 탑재하고 있어 공공기관이나 금융기관을 위한 장비 제작에 적용될 수 있으며, AES의 탑재를 통하여 해외 경쟁력도 갖추었다고 볼 수 있다. 전용 암호 패킷 처리 칩의 구조는 다음 그림 2와 같다. 이 칩은 DES, 3DES, AES[4][5], SEED[6] 네 종류의 블록 암호알고리즘을 지원하여, VPN 장비에서 가장 많은 계산력을 사용하는 블록 암호 연산을 가속시켜 주는 기능을 제공한다. 개발을 용이하도록 하기 위하여, 먼저 Xilinx FPGA를 이용해 개발되었으며, 추후 0.18um 공정으로 다시 개발하였다. 개발한 칩은 암호 연산이 고속으로 이루어질 수 있도록 메인프로세서와의 인터페이스로 32bit/33MHz의 PCI 인터페이스를 지원하고 있다.

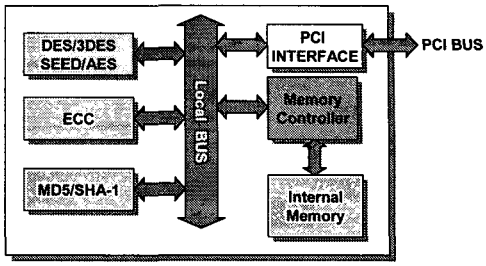

그림 2. 전용 암호 패킷 처리 칩의 블록 다이어그램
Fig 2. Block Diagram of Private Encryption Packet Processing Chip

상기 암호가속 칩은 내부적으로 PCI/DMA Interface 블록, Packet Process 블록, MEM Controller 블록, Encryption & Authentication Engine 블록 과 Internal Buffer 블록의 총 5개의 블록으로 구성되어진다. PCI/DMA Interface 블록은 PCI와 DMA를 통하여 입출력되는 데이터의 인터페이스를 담당하며, MEM Controller 블록은 PCI/DMA Interface블록으로부터 들어온 데이터를 Packet Process 블록과 Internal Buffer블록 사이에 데이터를 전달하거나 저장하는 역할을 하며, Packet Process 블록은 Encryption & Authentication Engine 블록의 입력데이터 형식에 맞추어 데이터를 전달하거나 Encryption & Authentication Engine 블록에서 출력된 데이터를 조합하는 역할을 한다. Internal Buffer 블록은 내부에서 사용되는 임시 데이터 저장 장소이다.

Ⅲ. VPN 시스템 구축을 위한 요소들

VPN 시스템은 단순히 두 개의 칩만으로 동작할 수 있는 것이 아니라, 네트워크 패킷을 처리할 수 있는 커널 모듈과 운영체제, 그리고 응용 어플리케이션 들이 적절히 조합되어야만 동작되어질 수 있다. Time to Market이 매우 중요한 보안 장비 시장에서 경쟁력을 갖추려면 이러한 다양한 요소들을 동시에 개발할 수 있는 여건을 제공하는 것이 매우 중요하다. 최단 시간 내에 시스템을 구축할 수 있도록, 두 칩의 평가보드(Evaluation Board)를 제공하는 것이 필수적인 사항이며, 평가보드와 운영체제 및 컴파일러 구축 등은 다음과 같이 정리된다.

3.1 다기능 네트워크 프로세서 FPGA를 위한 Evaluation H/W

보안장비용 다기능 네트워크 프로세서는 VPN 또는 SSL용 H/W를 위한 부품들이 하나의 칩으로 구현된 SoC(System-on-a-Chip)이다.

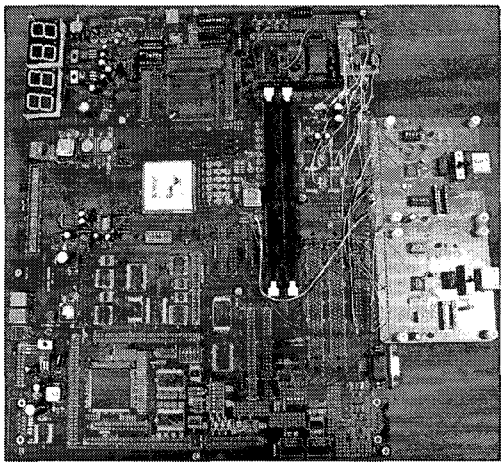

그림 3. 다기능 네트워크 프로세서 FPGA를 위한 Evaluation H/W
Fig 3. Evaluation H/W for Network Processor FPGA with Various Function

네트워크 프로세서는 많은 병렬처리 인터페이스와 컨트롤러를 포함하기 때문에 그 검증을 위해서 먼저 FPGA로 구현하는 것이 바람직하다. 또한 장비를 쉽게 개발할 수 있도록 Evaluation 보드를 구성하였다. 메인 프로세서로서 Arm Core가 사용되었기 때문에, 기존의 임베디드 리눅스를 쉽게 탑재할 수 있다. 더욱이 Arm 프로세서는 리눅스 이외에도 pSOS, VxWorks 등의 운영체제를 지원하므로 개발할 수 있는 경우의 수가 다양 해 진다. 그림 3은 Evaluation H/W의 모습이다.

3.2 전용 암호 패킷 처리 FPGA를 위한 Evaluation H/W

제작한 카드의 외형은 그림 4에 보여지고 있다. 제작한 암호가속 카드는 Xilinx FPGA를 이용한 것과 위 XCP-01 칩을 이용한 것 두 가지가 있는데, 본 논문에서는 XCP-01 칩을 이용하여 제작한 카드의 경우가 그림 4에 나타나 있다.

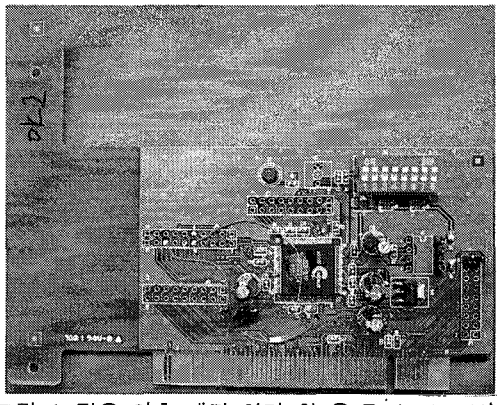

그림 4. 전용 암호 패킷 처리 칩 용 Evaluation H/W
Fig 4. Evaluation H/W for Private Encryption Packet Processing

암호가속 카드는 크게 PROM, PCI I/F와 암호 및 인증 알고리듬이 One Chip으로 구성된 자일링스 디바이스, 전원을 공급하는 Power와 PCI Slot으로 구성되어 있다. 암호가속 보드의 동작 흐름은 다음과 같다. 먼저, CPU에서 디스크립터의 시작을 알리는 레지스터 값을 세팅함으로써 암호 가속 보드의 동작이 시작된다. 암호 코어는 시스템 메모리와 DMA를 통해 디스크립터, 커맨드, 데이터를 차례로 읽어와 내부 메모리에 저장하고 Packet Processor에 전달한다. Packet Processor은 암호 코어 블록에 데이터를 전달하고 처리된 결과를 내부 메모리에 저장한다. 암호 코어는 처리가 완료되면 다음 디스크립터를 받을 수 있도록 시스템 메모리의 현제 디스크립터의 시작 비트를 클리어 한다. 결론적으로, 암호가속 카드는 호스트 CPU의 도움을 최소로 받으면서 암호 패킷을 처리할 수 있도록 DMA를 최대한 활용하고 있다.

3.3 소프트웨어 작업

보안장비로서 동작하게 하려면, 운영체제와 그 상위에서 동작하는 어플리케이션 작성이 동반되어야 한다. 어플리케이션을 제작하려면, 또한 컴파일러 구축 과정이 필요한데 이러한 것을 가장 쉽게 할 수 있는 방안은 공개 소프트웨어를 이용하는 것이다. 이러한 소프트웨어 작업을 구분하면 다음 5단계로 나눌 수 있다.

- 운영체제 이식:
  본 논문에서 설계한 네트워크 프로세서의 코아는 Arm 프로세서이므로, 이식할 수 운영체제로는 VxWorks,

pSOS, Linux, Windows CE 등 여러 가지가 있다. 그러나, 컴파일러 환경 구축 등의 문제점을 고려하여 Embedded Linux를 탑재하였다.

- 컴파일러 환경 구축:
  Arm 프로세서용 컴파일러로는 GNU gcc 계열중 Arm core용 크로스 컴파일러를 이용하였다.
- 칩셋 구동을 위한 Device Driver:
  운영체제가 Linux이므로 Linux용 Device Driver를 구현하는 것이 필수적이다. 각종 페리퍼럴의 Device Driver는 IP Vendor의 매뉴얼을 참고하여 구축할 수 있었다.
- IPSec Security Engine 구축:
  VPN 시스템은 대부분 Layer 3 레벨 아래에서 데이터 패킷을 암복화 하는 일을 주로 하지만, 보안 정책의 수립과 집행, 접근 제어 등을 위해 그 상위 레벨에까지 액세스를 하는 경우가 많다. IPSec 엔진을 바닥에서부터 모두 설계하여 구현하는 것은 결코 쉬운 일이 아니지만, Freeswan이나 BSD Free Source를 참조하여 구축하는 것은 비교적 쉬운 일이다. 본 논문에서는 Freeswan을 이용하여 IPSec Engine을 구축하였다.
- 응용 소프트웨어 구축:
  Embedded Linux와 크로스 컴파일 툴체인이 구축이 되면 X86 계열에서 개발된 응용 프로그램들을 비교적 수월하게 이식할 수 있다. 이러한 프로그램들의 예로써, 장애관리 시스템, 트래픽 모니터링, DHCP relay, Load Balancing 모듈, VPN Manager 등의 어플리케이션 들이 있다.

Ⅳ. 암호 가속 성능 평가

4.1 측정 환경의 구축

설계된 암호 시스템의 성능을 평가하기 위해 FAB공정에 사용되기 직전에 동작성 검증이 끝난, Xilinx FPGA를 이용하여 VPN Tunnel을 구축하였을 시의 성능을 측정하였다. 양 끝단에 설치된 장비는 크로스 케이블로 연결되었으며, 그 뒷단에 Smartbits 장비를 두었다.

4.1.1 측정 대상 장비

암호화 전용 프로세서 FPGA 보드를 장착한 (주)시큐어넥서스의 IPSec 전용 장비로 세부 내역은 다음과 같다.

- XecureBOX 2500 Gateway[7]
- x86 기반, Intel Pentium III 1.0GHz CPU, 128Mb Memory, Three Ethernet I/F, Two PCI Slot
- 암호화 전용 프로세서 FPGA를 통해 IPSec 프로세싱을 수행하도록 수정 개발됨

4.1.2 상대 통신 장비

측정 대상이 되는 장비와 통신하는 상대 통신 장비는 측정 대상의 성능에 영향을 미치지 않을 만큼 상위의 성능을 가져야 하며, 세부 내역은 다음과 같다.

- XecureBOX 3000 Gateway[7]
- x86 기반, Intel Pentium IV 2.8GHz CPU, 256Mb Memory

4.1.3 측정 장비

NetCom Systems 사의 Smartbits 200을 측정 장비로 채택하였다.

4.2 실험 결과

이상의 환경에서 각 알고리즘 별로 성능을 측정한 결과는 표 1과 같다.

표1. 알고리즘별 성능 측정
Table 1. Performance Measurement of Various Algorithm

알고리즘	패킷 크기	성능
DES	64 bytes	19.6 Mbps
	1400 bytes	81.7 Mbps
3DES	64 bytes	8.1 Mbps
	1400 bytes	49.3 Mbps
AES	64 bytes	22.8 Mbps
	1400 bytes	83.5 Mbps
SEED	64 bytes	7.6 Mbps
	1400 bytes	39.4 Mbps

실험결과를 살펴보면, 짧은 길이의 패킷에 대해서는 프로토콜 스택을 통과하는 패킷의 개수가 증가하기 때문에, 속도 저하가 어쩔 수 없음을 알 수 있다. 그러나, 패킷의 길이가 1400 바이트 정도가 되면 100 Mbps 와이어 스피드에 근접하는 결과가 나오는 것을 확인할 수 있었다.

V. 결 론

본 논문에서는 VPN/SSL 등의 보안 시스템에서 사용되고 있는 데이터 암복호화 과정을 고속으로 처리할 수 있는 2-Chip ASIC에 대해 소개하였다. 특히, 개발한 칩들은 평가보드를 통하여 쉽게 장비로 개발될 수 있는 형태로 구축이 되었다. 지원되는 블록 암호 알고리즘으로는 DES/3DES, AES, SEED가 있다. 특히, 국내 전용 알고리즘인 SEED를 탑재하고 있어서 국내 공공기관이나 금융기관의 장비 개발에 적용이 손쉬울 뿐 아니라 차세대 블록 알고리즘인 AES를 탑재하여 해외 경쟁력도 확보하고 있다. 두 칩이 동시에 적용되면, 초소형의 보안장비 구현이 가능하며, 암호가속 칩만이 사용될 경우에도 별도의 암호화 코프로세서로 이용되어 제품의 성능을 높이는데 사용될 수 있다. 따라서 x86 프로세서와 같은 범용 프로세서나 네트워크 프로세서를 활용한 장비개발에 사용되면 저가격에 고수준의 암호장비를 제작하는 경우에 활용될 수 있다.

참고문헌

[1] 이만용외, 최신정보보호개론, 홍릉과학출판사, 2005.

[2] 최용락, 소우영, 이재광, 이임영 통신망 정보보호, 그린출판사, 1996.

[3] HIFN Inc. Available at http://www.hifn.com.

[4] Joan Daemen, Vincent Rijmen, AES Proposal : Rijndael,(http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf)

[5] A. J. Elbirt, W.Yip, et.al, "An FPGA-Based Performance Evaluation of the AES Block Ciper Candiate Algorithm Finalists", IEEE Transactions on VLSI System, Vol.9, NO. 4, August 2001.

[6] 한국정보보호센터, "128비트 블록 암호알고리듬(SEED) 개발 및 분석보고서", KISA, 2003.

[7] XecureNexus Inc. Available at http://www.xecurenexus.com.

저자소개

이 완 복(Wan-Bok Lee)

2004년 2월 : KAIST 전자전산학과 박사

2003년 3월 ~ 현재 : 중부대학교 이공대학 컴퓨터 · 게임학부 교수

※ 관심 분야: Information Security, Discrete Event System Simulation, Computer Game

김 정 태(Jung-Tae Kim)

2001년 8월 : 연세대학교 대학원 전자공학과 박사

1991년 8월 ~ 1996년 2월 : 한국전자통신연구원(ETRI) 선임연구원

2002년 10월 ~ 현재 : 목원대학교 공과대학 정보전자영상공학부 교수

※ 관심 분야: Optically fed wireless communi cation system design, Information security system design, Network Security, ASIC Design.