

SOHO VPN 시스템에 특화된 암호가속카드의 설계 및 구현

이 완복*

요약

암호화 기술을 이용하여 고비도의 정보보호를 달성하고자 하는 VPN 시스템에서는 암호 가속 성능이 관건이다. 그러나 암호 연산은 많은 계산량을 필요로 하고 소프트웨어로 구현되었을 경우에는 그 성능에 한계가 있기 때문에, 전용의 암호 가속 하드웨어를 이용하여 구현하는 것이 필수적으로 요구된다. 본 논문에서는 많이 사용되어지는 블록 암호 알고리즘인 DES, 3DES, AES, SEED가 실장된 암호 가속 칩을 이용하여 PCI 카드를 설계 제작한 사례를 소개하고 있다. 제작한 암호가속카드는 상용 VPN 시스템에 실장된 후 그 성능이 평가되었다.

Design of A Cryptographic Add-on Card Dedicated to SOHO VPN

Wan Bok Lee*

ABSTRACT

The performance of a cryptographic module is the most important thing to achieve a high performance VPN system which realizes information security by encrypting and decrypting all the communicating data packets. However the cryptographic operations require much computation power and software cryptographic systems reveal bad performance. Thus, it is strongly recommended to develop a VPN system employing hardware component. This paper introduces a case study of developing a PCI add-on card which supports several block cipher algorithms such as DES, 3DES, AES, and SEED.

The performance of them was measured by embedding the card in a commercial VPN system.

Key words : 암호가속카드, VPN, 암호프로세서

* 중부대학교 게임학과

1. 서 론

최근 들어 전 세계적으로 급속히 보급된 인터넷은 거의 모든 정보를 가장 빠르게, 그리고 손쉽게 얻을 수 있는 정보의 보고로 자리 잡게 되었고, 이제는 인류 경제 활동을 비롯한 모든 활동에 있어서 없어서는 안 될 주요 기반구조의 하나가 되었다. 그러나 인터넷은 본질적으로 신뢰할 수 없는 네트워크들의 집합체로, 정보의 흐름을 통제하기가 대단히 어렵다. 따라서 인터넷에 산재한 자원을 충분히 활용하는 반면 내부의 중요한 자원을 인터넷으로부터 보호해 줄 수 있는 인터넷/인트라넷 보안이 가장 심각한 문제로 대두되고 있다. 따라서 인터넷 사용의 증가함에 따라 인터넷을 통한 정보 교환 시 정보 보호의 중요성 또한 날로 증대하고 있다.

인터넷 보안은 크게 액세스 제어 서비스와 통신 보안 서비스의 적절한 조합에 의해 달성될 수 있다. 액세스 제어는 컴퓨터/네트워크 자원의 접근제한을 통해 외부 혹은 내부의 사용자들로부터 보호하는 기술이며, 통신 보안은 사용자 인증이나 데이터 무결성, 데이터의 비밀보장 등의 암호 기술들을 이용해 인터넷에 유통되는 정보를 불법적인 사용자들로부터 보호하기 위한 것이다.

대부분의 네트워크 보안 전략은 조직 네트워크 외부의 공격에 대한 보호에 집중하고 있으며, 방화벽, 보안 라우터, 전화 접속 액세스의 토큰 인증 등은 외부 위협에 대해 보호하려는 관리 시도의 예이다. 대부분의 인터넷 보안 제품은 다양한 보안 프로토콜들을 이용하여 액세스 기능을 구현한 것으로 볼 수 있으며, 현재 인터넷 보안의 주류를 이루는 것이 VPN(Virtual Private Network), 방화벽(Firewall)과 침입탐지시스템(Intrusion Detection System)이다[1].

방화벽과 침입탐지시스템은 인터넷과 자신의

네트워크 사이에 위치하여 불특정 다수의 인터넷 사용자에 대한 접근제어를 통해 자신의 네트워크를 보호하고자 하는 방안이다. 반면에 VPN은 적절한 암호기술을 이용하여 양단간의 안전한 정보 교환이 가능하도록 하는 차세대 네트워크 인프라 기술이다[1, 2].

그러나, VPN은 기본적으로 통신하는 모든 데이터 패킷들을 암호화하는 메카니즘에 의해 보안성을 구축하기 때문에, 저렴한 가격에 고성능의 장비를 개발하려면 전용의 암호가속카드를 제작하여 사용하는 것이 필수적으로 요구된다. 특히 암호화 연산은 단순한 연산 모듈로 구성되어 있으나, 암호화 강도를 높이기 위해 많은 반복 연산을 동원하고 있기 때문에 범용 프로세서를 이용하여 소프트웨어적으로 처리하는 것보다 전용 하드웨어를 이용할 때 그 효율성이 극대화되며 고비도의 암호 성능을 보장할 수 있게 된다.

이러한 배경에서 Hifn[3], Broadcom, Analog Device사 등 다수의 해외 업체들이 암호가속 칩을 개발한 바 있으며, 이들 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)시큐어 넥서스에서는 독자적으로 암호가속칩 XCP-01을 개발하였으며, 본 논문에서는 이 칩을 이용하여 암호가속 보드를 제작하고 그 성능을 테스트한 결과를 소개한다.

논문의 구성은 다음과 같다. 2장에서는 본 논문에서 사용한 암호가속 칩 XCP-01과 이를 이용해 개발한 암호가속 보드에 대해 설명한다. 3장에서는 제작한 암호가속 보드의 성능을 평가하였으며, 4장에서 결론을 맺는다.

2. 암호가속 보드의 설계

2.1 암호가속 엔진

본 논문에서 사용한 암호가속 엔진은 (주)시큐어넥서스에서 개발한 암호칩 XCP-01이며 칩 외양은 (그림 1)과 같다. 이 칩은 DES, 3DES, AES[4, 5], SEED[6] 네 종류의 블록 암호알고리즘을 지원하며, 먼저 Xilinx FPGA를 이용해 개발되었으며, 추후 0.18um 공정으로 다시 개발되었는데, (그림 1)에서 개발된 칩의 외형을 보이고 있다.

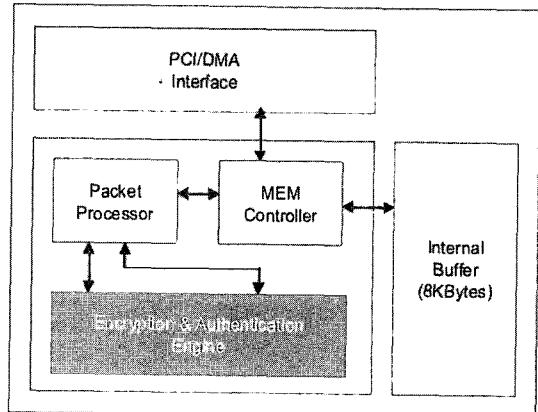
개발한 칩은 암호 연산이 고속으로 이루어질 수 있도록 메인프로세서와의 인터페이스로 32bit/33MHz의 PCI 인터페이스를 지원하고 있다.



(그림 1) XCP-01 : 암호가속 엔진이 탑재된 칩

상기 암호가속 칩은 내부적으로 PCI/DMA Interface 블록, Packet Process 블록, MEM Controller 블록, Encryption & Authentication Engine 블록과 Internal Buffer 블록의 총 5개의 블록으로 구성되어진다. (그림 2)는 암호 가속 엔진의 구조도를 나타낸다.

PCI/DMA Interface 블록은 PCI와 DMA를 통하여 입출력되는 데이터의 인터페이스를 담당하며, MEM Controller 블록은 PCI/DMA Interface 블록으로부터 들어온 데이터를 Packet Process 블록과 Internal Buffer 블록 사이에 데이터를 전달하거나 저장하는 역할을 하며, Packet Process 블록은 Encryption & Authentication Engine 블록의 입력데이터 형식에 맞추어 데이터를 전달하거나

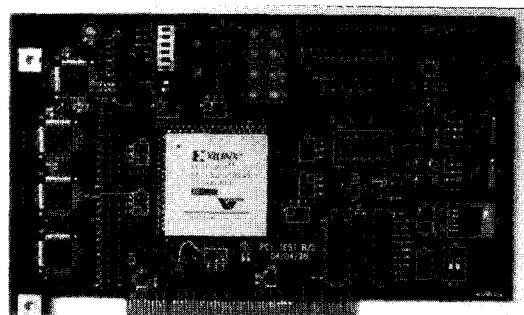


(그림 2) 암호가속 엔진의 구조도

Encryption & Authentication Engine 블록에서 출력된 데이터를 조합하는 역할을 한다. Internal Buffer 블록은 내부에서 사용되는 임시 데이터 저장 장소이다.

2.2 암호가속 보드의 설계

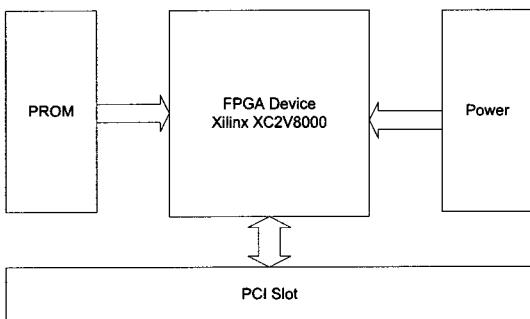
제작한 카드의 외형은 (그림 3)에 보여지고 있다. 제작한 암호가속 카드는 Xilinx FPGA를 이용한 것과 위 XCP-01칩을 이용한 것 두 가지가 있는데, 본 논문에서는 FPGA를 이용하여 제작한 카드를 사용하고 있다.



(그림 3) 제작한 암호 가속카드의 외형

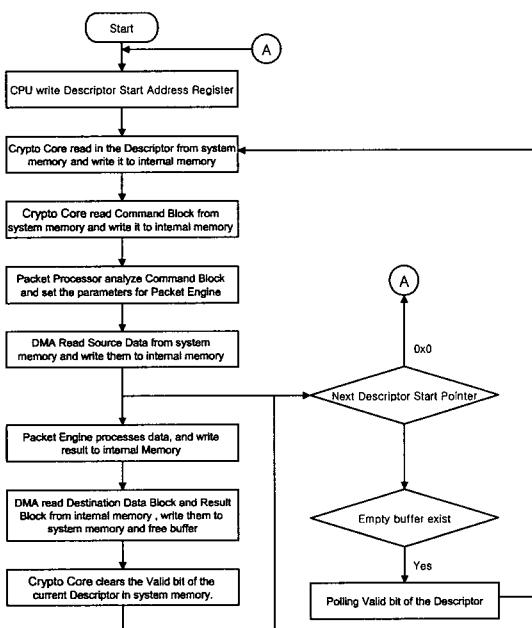
암호가속 카드는 크게 PROM, PCI I/F와 암

호 및 인증 알고리듬이 One Chip으로 구성된 자일링스 디바이스, 전원을 공급하는 Power와 PCI Slot으로 구성되어 있다. (그림 4)는 암호가속 카드의 블록도를 나타낸다.



(그림 4) 암호가속 카드의 블록 구성도

(그림 5)는 암호가속 보드의 동작 흐름에 대하여 나타낸다. 그림에서 알 수 있듯이 CPU에서 디스크립터의 시작을 알리는 레지스터 값을



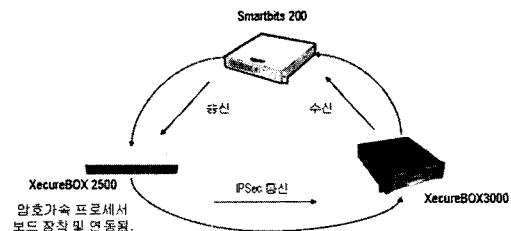
(그림 5) 암호 가속 보드의 동작 흐름도

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 현재 디스크립터의 시작 비트를 클리어 한다. 결론적으로, 암호가속 카드는 호스트 CPU의 도움을 최소로 받으면서 암호 패킷을 처리할 수 있도록 DMA를 최대한 활용하고 있다.

3. 성능 평가

3.1 측정 환경의 구축

설계된 암호 시스템의 성능을 평가하기 위해 FAB공정에 사용되기 직전에 동작성 검증이 끝난, Xilinx FPGA를 이용하여 (그림 3)과 같은 보드를 구성하고, (그림 6)과 같은 환경에서 VPN Tunnel을 구축하였을 시의 성능을 측정하였다.



(그림 6) 성능 측정 환경

3.1.1 측정 대상 장비

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

- XecureBOX 2500 Gateway
- 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

3.1.2 상대 통신 장비

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

〈표 1〉 알고리즘별 성능 측정

알고리즘	패킷 크기	성능
DES	64 bytes	19.6 Mbps
	1400 bytes	81.7 Mbps
DES/MD5	64 bytes	16.1 Mbps
	1400 bytes	73.7 Mbps
DES/SHA-1	64 bytes	14.3 Mbps
	1400 bytes	66.5 Mbps
3DES	64 bytes	8.1 Mbps
	1400 bytes	49.3 Mbps
3DES/MD5	64 bytes	6.2 Mbps
	1400 bytes	44.9 Mbps
3DES/SHA-1	64 bytes	5.7 Mbps
	1400 bytes	40.7 Mbps
AES	64 bytes	22.8 Mbps
	1400 bytes	83.5 Mbps
AES/MD5	64 bytes	17.4 Mbps
	1400 bytes	75.1 Mbps
AES/SHA-1	64 bytes	15.7 Mbps
	1400 bytes	67.2 Mbps
SEED	64 bytes	7.6 Mbps
	1400 bytes	39.4 Mbps
SEED/MD5	64 bytes	5.9 Mbps
	1400 bytes	37.1 Mbps
SEED/SHA-1	64 bytes	5.7 Mbps
	1400 bytes	36.3 Mbps

역은 다음과 같다.

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

3.1.3 측정 장비

NetCom Systems사의 Smartbits 200을 측정 장비로 채택하였다.

3.2 실험 결과

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

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

4. 결 론

VPN은 정보 교환 시에 IP 패킷에 대한 보호를 제공해주는 기술이며, 투명하고 자동화된 인터넷 정보 서비스를 제공 할 수 있다. 기술적 기반이 되는 IPSec 엔진은 간단히 소프트웨어로 구현할 수도 있으나 그 경우 처리 속도가 느려진다는 단점이 있다. 이러한 처리 속도 상의 단점을 극복하기 위해서는 알고리듬의 하드웨어 구현이 필연적이다.

본 논문에서는 SSL과 VPN에 적합하도록 개발된 암호 카드의 설계에 대해서 소개하였다. 개발된 프로세서는 암호 패킷처리를 위한 기능들로 구성되어 있다. 가장 큰 특징은 국내 전용 알고리듬인 SEED를 탑재하고 있어서 국내 공공기관이나 금융기관의 장비 개발에 적용이 손

쉬울 뿐 아니라 차세대 블록암고리즘인 AES를 탑재하여 해외 경쟁력도 확보하고 있다.

개발된 암호가속 카드는 네트워크 보안 장비의 구성에 있어서 주 프로세서 외에 별도의 암호화 코프로세서로 탑재되어 제품의 성능을 높이는데 사용된다. 따라서 x86 프로세서와 같은 범용 프로세서나 네트워크 프로세서를 활용한 장비개발에 사용되면 저가격에 고수준의 암호장비를 제작하는 경우에 활용될 수 있다.

참 고 문 헌

- [1] 이만용외, '최신정보보호개론', 홍릉과학출판사, 2005.
- [2] 최용락, 소우영, 이재평, 이임영, '통신망 정보 보호', 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 Cipher Candidate Algorithm Finalists", IEEE Transactions on VLSI System, Vol. 9, No. 4, August 2001.
- [6] 한국정보보호센터, "128비트 블록 암호알고리듬(SEED) 개발 및 분석보고서", KISA, 2003.



이완복

1993년 한국과학기술원 전기및전자공학과(공학사)
1995년 한국과학기술원 전기및전자공학과(공학석사)
2004년 한국과학기술원 전자전산학과(공학박사)
2004년 ~ 현재 중부대학교 컴퓨터공학부 교수
관심분야 : 시뮬레이션, 컴퓨터 게임, 정보보호, 이산사건 시스템