개발 성공요인을 적용한 네트워크 보안 시스템 개선에 관한 연구

김 종 선* · 황 경 태**

A Study on the Improvement of Network Security Systems Based on Critical Success Factors for Systems Development

Chong Sun Kim* · Kyung Tae Hwang**

Abstract

This study proposes a method to improve network security systems based on critical success factors for systems development. To accomplish the research objective, the study analyzes required functions of network security systems and reviews existing methods to improve network security systems. Based on the analyses and literature review, critical success factors for development of network security systems are identified and a new method to improve network security systems based on the critical success factors is proposed.

The proposed method to improve network security systems is based on utilizing multi-core processors. A prototype is developed and validated. This study will provide a good case in the network security area where research incorporating both engineering and management disciplines lacks.

Keywords : Network Security Systems, Critical Success Factors, Prototype

논문접수일 : 2007년 09월 27일 논문게재확정일 : 2007년 12월 22일

* 시큐아이닷컴 대표이사

** 교신저자, 동국대학교 경영대학 경영정보학과 교수, (100-715) 서울 중구 필동 3-26, Tel : 02-2260-3708, e-mail : kthwang@dongguk.edu

1. 서 론

한국의 IT의 역사는 정부의 주도로 1978년 행정전산화 사업에서 시작되었다[행자부, 1978; 행자부, 1979]. 이후 각계 각층에서 전산화 사업의 증가로 각 기관과 기업들은 업무 혁신과 제품 생산 혁신을 이루어오고 있다[행자부, 1982]. 이러한 IT 시스템들은 1984년 국내 LAN 접속을 시작으로 1997년 전국 5대 도시가 45Mbps~155Mbps로 연결되기까지 서로 네트워크로 연결되면서 업무적으로 물리적인 거리를 무의미하게 만들었다. 이에 멈추지 않고 네트워크 대역폭은 2000년대 초에 이미 1Gbps급으로 성능 향상을 이루었으며, 최근에는 10Gbps급 네트워크가 보급되기 시작하였다[인터넷역사위원회, 2005]. 네트워크 보안 시스템은 성능뿐만 아니라 기능 측면에서 90년대에는 네트워크의 접근 통제에 대한 필요성만이 부각되고, 90년대 이후에는 네트워크 암호 및 인증만을 제공하면 보안이 이루어 질 것으로 생각되었다. 그러나 그 후 1.25 인터넷 대란 같은 서비스거부 공격에 따른 트래픽 폭주에 대한 대책이 필요하게 되었으며, 현재는 웹의 취약점을 이용한 침입의 활성화로 침입방지 기술의 고도화가 많이 요구되고 있다.

이러한 보안 시장의 요구에 따라 네트워크 보안 시스템 개발자들은 보안기능 처리에 중심이 되는 프로세서의 변화를 중심으로 네트워크 보안 시스템의 개선을 추구하였다. 이러한 방법의 예로는 개인 컴퓨터 및 서버에 사용되는 범용 CPU 기반의 플랫폼 및 네트워크 패킷 처리에 특화된 데이터 경로분산 기반의 플랫폼 등을 들 수 있다. 하지만 이러한 시도들은 새로운 프로세서의 성숙되지 않은 기술과 국내 개발진의 미흡한 개발체제로 실제 보안 시스템의 개발에 많은 시행착오를 겪게 되었고, 국내외에서 여러 기업이 고성능 및 다기능 보안 제품을 개발하였으나 실제 성공한 업체는 매우 적으며, 가장 먼저 개발한 업체가 이익의 대부분을 독점하는 경향이 있다. 이러한 시행착오는 네트워크 보안 시스템의 개선을 위해서는 공학과 경영학을 복합적으로 적용한 새로운 접근방법이 필요하다는 점을 시사한다.

본 논문의 목적은 시장의 요구에 부응할 수 있는 새로운 고성능/다기능 네트워크 보안 시스템을 개발하는 방법을 제시하는 것이다. 이를 위하여 네트워크 보안 장비의 필요 기능을 분석하고, 이러한 기능 및 성능을 제공하기 위해 제안된 다양한 기존의 네트워크 보안 시스템 기술을 분석한다. 이러한 기존 기술 분석과 문헌 분석 등을 통해서 고성능/다기능 네트워크 보안 시스템 개발을 위한 핵심성공요인을 도출한다. 도출된 성공 요인을 바탕으로 새로운 네트워크 보안 시스템을 제안하고, 그 프로토타입을 개발하여 제안된 방법을 검증하도록 한다.

2. 사전연구 분석

2.1 네트워크 보안 시스템의 필요기능 분석

네트워크 보안 시스템이 갖추어야 할 필요 기능은 시간에 따라 변화되어 왔다. 기능은 당시의 네트워크에 위협을 미치는 공격의 종류와 밀접하게 연관되어 있다. 네트워크를 통한 데이터 통신 초기에는 허가되지 않은 사람들이 허가되지 않은 응용을 이용하여 시스템에 접근하는 위협이 많았기 때문에 IP 주소와 응용의 포트를 이용하여 침입을 차단하는 침입차단시스템(Firewall) 기능이 시장에서 요구되었다. 근래에는 공격의 기술이 다양해지고, 시스템이 제공하는 서비스가 많아짐에 따라 더 이상 IP 주소와 포트로 막을 수 없는 위협이 증가하여 침입방지시스템(IPS : Intrusion Prevention System) 기능이 각광을 받고 있다. 또한 기술정보의 중요성이 커

지고 있어 데이터통신의 비밀성 및 무결성을 제공받으려는 서비스가 많아짐에 따라 가상사설망(VPN : Virtual Private Network) 기능이 대두되었다.

아래 <표 1>에는 최근의 네트워크 보안시스템이 어떤 기능으로 네트워크 보안 시장의 요구사항을 충족시키고 있는지를 정리하고 있다.

대표적인 네트워크 보안 시스템의 대부분은 <표 1>에서 언급한 보안 기능들을 제공하고 있다. 이외에 대부분의 네트워크 시스템들이 제공하는 네트워크 주소변환(NAT) 기능, 감사기록 생성 기능, 관리자 및 사용자 인증 기능, 바이러스 차단 기능, 콘텐츠 검사 기능과 같은 보안 기능들은 외부 DB를 사용하거나 프락시 기능으로 설명 가능하고, 본 논문의 주제에서 벗어나기 때문에 본 연구의 범위에서 제외하였다.

2.2 기존 네트워크 보안 시스템 분석

본 절에서는 기존에 제안된 네트워크 보안 시스템의 대표적인 개선 방법에 대해서 알아본다. 여기에는 범용 CPU에 기반한 고속화 시스템, 데이터 경로 분산에 기반한 시스템, 부하 분산을 이용한 고속화 시스템 등이 포함된다.

(1) 범용 CPU에 기반한 고속화 시스템

범용 CPU 기반 시스템은 일반적인 컴퓨터 구조에서 네트워크 패킷을 처리하는 구조로 CPU의 처리 속도가 발전하는 것을 최대한 이용하는 방식이며 이러한 보안시스템의 성능을 결정짓는 가장 중요한 요소는 범용 CPU 및 I/O 버스의 성능이다. 이외에도 하드웨어로는 I/O 디바이스와 시스템 버스의 성능이 중요하며, 소프트웨어로는 하드웨어를 운영하는 운영체제의 최적화 및 네트워크 프로토콜 스택의 최적화가 중요한 요소이다[Fieldman, etc., 2000]. 범용 CPU에 기반한 네트워크 보안시스템의 성능 향상 시도는 소프트웨어 또는 하드웨어 측면에서 이루어진다. 그런데, 한 가지 방식만을 선택할 것인

〈표 1〉 네트워크 보안시스템의 필요기능

지 원 기 능		기 능 설 명
방화벽	접근통제	패킷의 유효성을 검사하여 차단(Deny) 또는 허용(Allow)를 결정
	HTTP 프락시	악성코드 제거, 첨부파일 바이러스 검사, HTTP 사용 중 파일 첨부 금지
	SMTP 프락시	키워드 필터링, 발신/수신 메일주소 필터링, 발신/수신 메일 크기 제한
	SMTP 역방향 프락시	스팸메일 중계기 오용 차단, 특정 패턴의 제목 및 메일주소 차단
침입방지 시스템	다중패턴매칭 차단	패턴 매칭 알고리즘으로 특정 패턴을 보유하고 있는지 확인하여 차단
	LAND 공격 방어	출발지와 목적지의 IP 주소 및 포트가 같은 TCP SYN 전송 금지
	SYN Flooding 공격 차단	대량으로 SYN을 보내고 SYN/ACK에 대한 응답을 하지 않으면 차단
	SCAN 공격 처리	SCAN 공격은 서비스중인 취약한 TCP/UDP 포트를 탐색하므로 차단
	외부의 내부IP 주소 차단	외부에서 내부 IP 주소를 출발지 주소로 위장하여 들어오는 패킷 차단
	ICMP 차단	ICMP Destination Unreachable은 해커의 악용 가능성이 높으므로 차단
	미확인 발신지 주소 차단	외부망에서 오는 불명확한 발신지 주소 차단
	IP Source Route 차단	IP Source Route 옵션은 특정 서버를 경유하게 해 해커가 악용하므로 차단
VPN	암호처리 모듈	IPsec 프로토콜에 의한 암호화 알고리즘 연산 수행
	암호키 교환 모듈	암호통신을 하기 위한 암호키를 상호 교환
	IPsec 모듈	패킷 암호화(외부송신)/복호화(외부수신) 프로토콜을 수행
	보안 DB 모듈	보안 제휴 DB 및 보안 정책 DB 관리(추가/삭제/갱신)

지 두 가지 방식을 모두 선택할 것인지는 목표 시장의 성능적인 요구, 기능적인 요구, 개발 난이도 및 기간, 가격 경쟁력, 적시 시장 진출성 등 복합적인 요인들을 모두 고려해야 하고, 3~5년 후에 시장 변화, 기술의 연속성 및 변화에 대한 측면도 예측해야 한다.

초기의 네트워크 보안장비들은 대부분의 기능을 프락시 기반의 구조를 가지고 제공하였다. 프락시 기반의 보안모듈들은 한 개의 패킷을 처리하기 위한 처리과정의 90% 이상을 커널과 어플리케이션의 메모리 복사 및 TCP 프로토콜 처리하는데 소모하기 때문에 네트워크의 고속화에 따라 성능요구를 따라가지 못했다. 이러한 패킷 처리 과정에서 커널과 어플리케이션에서의 불필요한 전달과정 및 프로토콜 처리를 제거하기 위해서 커널에서 처리 가능한 보안모듈을 분리하고 커널에서 많은 기능을 처리하기 위한 노력을 시작하였다. 그 결과로 대부분의 패킷의 처리는 커널에서 처리함으로써 빠른 경로를 제공하고, 부가적인 처리가 필요할 때에만 응용계층을 통하여 보안기능을 제공하게 되었다.

근래의 범용 CPU 플랫폼 기반의 방화벽은 방화벽의 기본 기능인 접근 통제와 패킷 암호화, 패킷 유해성 검사를 커널에서 처리하여 시스템의 프로토콜 처리로 인한 과부하를 획기적으로 제거하여 패킷의 빠른 경로를 제공한다. 느린 경로에는 실시간성이 필요 없고, 복잡한 처리가 필요한 프락시, 동적 포트 프로토콜 처리, URL blocker 등을 처리하고, 컴퓨터의 운영체제에서 응용계층에 구현한다.

(2) 데이터 경로 분산에 기반한 시스템

데이터 경로 분산에 기반한 시스템은 NPU (Network Processing Unit) 기반 시스템을 의미한다. NPU는 네트워크 패킷을 고속으로 처리하기 위한 프로세서이다. 일반적으로 범용 CPU는 여러 가지 응용 프로그램을 구동하기 위해 제작되어 고속의 패킷 처리에는 한계가 있다. ASIC(Application Specific Integrated Circuit)은 이와 반대로 모든 필요한 기능을 하드웨어 로직으로 구현한 것으로서, 고속의 패킷 처리에는 유리하나 유연성이 떨어져서 새로운 기능의 추가가 전혀 불가능한 약점이 있다. NPU는 범용 CPU와 ASIC의 장점을 살리기 위해 여러 가지 구조로 설계되었으며, 고성능이 필요하며 기능의 변경이 없는 부분은 ASIC으로 제작하고 나머지 기능의 변경이 필요한 부분은 범용 CPU와 유사하게 제작하였다.

일반적으로 NPU는 RISC 명령어 세트의 일부와 네트워크 패킷 처리용 확장 명령을 갖는 코어(Core)가 다수 있고 각각의 코어는 다수의 쓰레드(Thread)를 갖거나 VLIW(Very Long Instruction Word)로 하나의 명령어에 의한 다수의 기능을 수행하는 병렬 처리의 방식을 채택하고 있다. 각각의 코어의 기능이나 성능을 줄이는 대신 부족한 처리 용량을 보충해 줄 수 있는 암, 복호화 모듈이나 패킷 분류기(classifier) 등 패킷 처리 전용 회로를 포함하고 있는 것이 보통이다.

데이터 경로 분산에 기반한 시스템은 네트워크 패킷마다 처리하여야 하는 많은 연산은 이 목적에 적합하도록 제작된 별도의 NPU 모듈에서 처리하도록 한다. 즉 대부분의 패킷은 NPU에서 처리하고 일부 복잡한 처리가 필요한 패킷만 범용 CPU에서 처리토록 한다. 데이터 경로 분산 기반 네트워크 보안시스템에서는 NPU가 처리하기 복잡한 각종 프락시와 동적 포트 프로토콜, URL 블로커와 관련된 패킷을 느린 경로, 즉 범용 CPU가 처리하고, 방화벽의 정책에 따라 패킷의 통과 여부를 결정하는 비교적 단순 작업은 빠른 경로, 즉 NPU(IXP2400, intel)가 처리한다.

(3) 부하분산을 이용한 고속화 시스템

부하분산이라고 함은 병렬 혹은 분산 시스템에서 실제 작업을 수행하는 시스템들을 여러 개 두고 중앙에서 이들에게 작업을 나누어주는 작업 분산 장치를 두어 성능 향상과 결함포용을 모두 제공하는 기법을 말한다. 기존의 방법들이 빠른 경로와 느린 경로를 분리하고 빠른 경로의 기능들을 특정 소프트웨어나 특수 프로세서를 사용하여 고속화를 시도하였다면, 본 절에서 설명하는 시스템은 고속의 부하분산 장치를 사용하여 고속 네트워크 보안시스템을 구현한 것이다. 이 시스템은 10기가급의 네트워크 보안기능을 수행하는 시스템으로, 기 개발된 2기가급 네트워크 보안 시스템들을 후단부(Back-end)에 여러 개 두고 이들에게 작업을 분산시켜주는 10기가급의 고속 부하분산기를 전단부(Front-end)에 장착한 것이다. 이스라엘의 이지칩(http://www.ezchip.com)사에서 2002년에 개발되어 출시된 NP-1c는 최초로 10기가급의 네트워크 인터페이스를 갖춘 네트워크 프로세서로서, 하드웨어로 만들어진 패킷 분류기(Packet Classification)와 정책 탐색기(Policy Search Engine)를 갖춘 패킷 프로세서이다.

이 프로세서의 단점으로는 대용량 메모리를 장착하지 못하고 (최대 크기 256MByte), 프로그램 저장 공간이 작아서 복잡한 프로그램을 수행시킬 수 없다는 점을 들 수 있다. 이러한 약점으로 인해 NP-1c는 패킷 처리용 메모리 공간이 기가바이트 이상이 요구되며 프로그램 구조와 기능이 복잡한 방화벽이나 VPN같이 기능을 구현하기에는 부적합한 프로세서이다. 하지만 이 프로세서의 장점인 고속 분류기능과 고속 탐색기능을 활용하여 10기가급의 부하분산과 같은 단순 고속기능을 구현하기에는 최적의 프로세서이다.

부하분산 기반 시스템은 하나의 PEM(Packet Engine Module), CEM(Control Engine Module)과 여러 개의 SEM(Session Engine Module)으로 구성된다. PEM(Packet Engine Module)은 NP-1c를 이용하여 제작된 10기가급 부하분산 장치이다. PEM은 외부에서 들어온 패킷을 후단의 SEM으로 전송하고 SEM에서 전송된 패킷을 외부 네트워크 포트로 전송하는 역할을 수행한다. SEM(Session Engine Module)은 범용 CPU 기반 네트워크 보안 시스템을 하드웨어 보드형태로 사용한 모듈이고, CEM(Control Engine Module) 또한 범용 CPU 기반 시스템을 사용하지만 시스템 전체의 제어 모듈로써 헬스 체크(Health Check) 및 고장 조치 등의 기능을 수행한다.

2.3 개발 성공 요인 문헌 분석 및 요인 도출

(1) 개발 성공요인 문헌 분석

신제품의 성공과 실패의 요인은 SAPPHO(Scientific Activity Predictor from Patterns of Heuristic Origins) 프로젝트[Rothwell, etc., 1974]를 시작으로 다양한 제품 분야에서 연구되어 왔다. 다음에서는 연대별로 주요한 문헌의 내용을 정리한다.

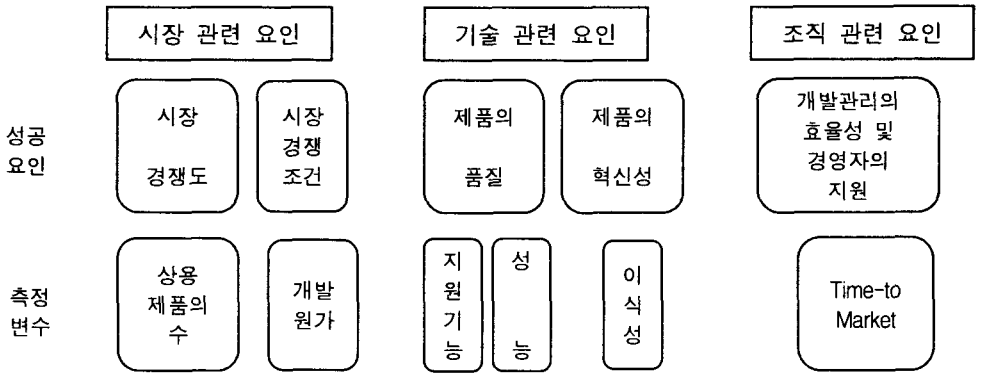
Rothwell 등[1974]이 1974년에 화학과 과학기기산업에서 신제품 86개를 대상으로 한 연구에서는 122개의 제안된 변수들 중에서 타당한 41개의 변수를 연구에 채택하였고, 연구결과로 고객의 요구사항에 대한 이해도와 마케팅능력, 개발효율성과 개발 책임자의 권한의 크기 및 외부기술 및 연구결과에 대한 적절한 활용이 신제품 성공의 주요 요인임을 밝혀내었다. 또한 Utterback 등[1976]은 서독에서 출시된 신제품을 연구하여 신제품의 성공요인은 시장경쟁우위와 같은 시장요인과 특허권, 법적 규제와 같은 환경적 요인을 언급하였다. 또한 신제품의 성공요인에 관

한 연구를 지속적으로 수행하고 있는 Cooper는 1979년에 제품의 독특성(Uniqueness)와 우월성(Superiority)이 신제품의 결정적 성공요인이라 주장하였고[Cooper, 1979a], 이어서 1985년과 1987년의 연구에서도 제품이 고객에게 주는 가치인 제품의 편익과 제품의 품질, 제품의 비용대비 효과, 경쟁제품대비 우위성과 같은 제품의 우월성과 독특성이 가장 중요한 성공요인임을 언급하였다. 본 연구와 비슷한 특성을 가지는 동일한 산업의 동일한 기업에서 개발한 신제품 중에서 성공요인과 실패요인을 분석한 연구[Cooper, 1979b]에서는 제품의 우월성과 독특성이 가장 중요한 성공요인이고, 다른 요인으로는 마케팅 능력, 개발/생산/마케팅/관리 조직들간의 통합 및 조정을 통한 시너지 효과, 시장 경쟁도와 경쟁조건, 시장수요 및 성장성 등이 중요 성공요인으로 언급되었다.

80년대의 연구에서 제품의 성공요인은 당시 포춘 1000대기업 중 700개의 기업의 신제품을 조사한 연구[Booz Allen and Hamilton; 1982]에서 시장요구의 적합성, 기업내부 강점과의 적합성, 기술적 우월성, 최고 경영자의 지원이 가장 중요한 요인으로 조사되었다. Maidique 등[1984]은 미국전자산업의 158개 신제품의 성공요인을 분석한 결과, 비용 대비 효과가 높은 제품, 연구개발과 마케팅간의 긴밀한 협조, 개발의 효율성 추구, 개발/생산/마케팅/관리 조직들간의 통합 및 조정을 통한 시너지 효과, 기업내부의 강점과 적합성이 제품이 성공하는데 가장 중요한 요인이라고 하였다. 또한 Cooper 등[1987]은 캐나다의 203개의 신제품을 분석하여 제품의 우월성, 개발 프로젝트의 효율적 운영, 마케팅과 기술의 결합효과를 중요한 성공요인임을 규명했다.

1990년대의 경우, Zirger 등[1990]은 다시 전자산업에서 330개의 신제품 사례를 분석하여 제품의 우월성 및 기업내부의 강점에 대한 적합성, 시장 수요 및 성장성과 시장 경쟁도를 가장 중요한 요인으로 보았다. Urban 등[1993]에서도 시장수요 및 성장성과 시장에서 경쟁도와 제품의 독특성 및 혁신성이 중요한 요인임을 주장하였다. 안기현[1993]은 국내 전자산업에서의 성공요인이 기술개발/마케팅/생산제조/정보관리/개발관리/경영지원능력 같은 회사 전체적인 자원 및 능력요인과 시장세분화의 과정, 제품수명주기, 시장규모 및 성장성과 같은 시장환경요인, 제품의 혁신성 및 독창성과 같은 제품특성요인을 제시하고 있다. 제조업체에서의 성공요인을 도출한 한 연구에는 제조업체의 특성을 나타내는 신제품 개발과정의 채택여부와 신제품 런칭 노력이나 시장환경이 도출되었다[최수호, 1994]. Kwaku[1996]는 시장요구 적합도와 마케팅 및 개발의 통합 및 조정으로 인한 상승효과를 제품의 성공요인으로 꼽았다. 중소기업과 대기업의 제품 성공요인을 비교한 연구에서는 기술전략 측면에서 기술선도 및 추종전략 및 제품 및 공정기술능력 축적 등 기업의 크기에 따라 달라질 수 있는 요인을 다수 도출하였다[김지대, 1999]. 뿐만 아니라 한국과 미국의 신제품 성패요인을 비교 분석한 연구[이재희, 2000]에서는 프로젝트의 조직화 방법 및 권한의 집중, 의사결정의 참여와 같은 문화적인 요인에 의해서 달라질 수 있는 성공요인을 도출하고, 탐색 및 개념개발 단계의 능숙도와 시제품 개발 및 시험단계의 능숙도, 시장출시 및 서비스단계의 능숙도 등 제품 개발의 전 과정에 대한 능숙도 관련 성공 요인을 도출하여 국가간 기술발달 차이에서 올 수 있는 성공요인도 도출하였다.

<표 2>에는 신제품의 성공요인을 도출한 기존 연구의 결과가 정리되어 있다. 각 연구에서 문구가 조금 다른 경우에는 가진 의미를 왜곡하지 않는 범위에서 통합하고, 큰 의미를 가진 요인이 부분적인 요인을 포함하는 경우에도 통합



〈그림 1〉 네트워크 보안 시스템의 개발 성공요인 및 측정변수

〈표 2〉 제품 성공요인 분류 및 관련연구

구분	소분류	관련연구번호																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
시장관련요인	시장요구 적합도	O					O	O		O							O		O
	시장수요/성장성					O							O	O		O		O	O
	시장경쟁도					O				O			O	O		O		O	O
	시장경쟁조건					O										O			
환경관련요인	외부기술/연구활용	O																	
	법적규제		O																
	특허권		O																
제품관련요인	제품의 품질		O		O	O	O	O	O	O	O	O	O				O	O	O
	제품독특성/혁신성				O	O			O	O				O	O			O	
조직관련요인	개발책임자 권한	O																	
	기업내부 적합도						O			O			O						
	경영자의 지원						O	O		O						O		O	O
	개발관리의 효율성	O						O			O		O		O	O			
	개발/생산/마케팅/관리의 통합/조정을 통한 상승효과			O		O		O			O				O	O	O	O	

주) 1. Rothwell. R, C. Freeman, A. Horlsey, V. T. P. Fevis, A. B. Robertson, and J. Townsend [1974]
2. Utterback, J. M., J. A. Thomas, and H. Gerstenfeld [1976]
3. Souder, W. E. and A. K. Chakrabarti [1978]
4. Cooper, R. G. [1979a]
5. Cooper, R. G. [1979b]
6. Booz, Allen and Hamilton [1982]
7. Maidique, M. A. and B. J. Zirger [1984]
8. Cooper, R. G. [1985]
9. Brentani, de. [1986]
10. Cooper, R. G. and Kleinschmidt, E. J. [1987]
11. Cooper, R. G. [1990]
12. Zirger, B. J. and Maidique, M. A. [1990]
13. Urban, G. L., & J. R. Hauser [1993]
14. 안기현[1993]
15. 최수호[1994]
16. Kwaku, A. G. [1996]
17. 김지대[1999]
18. 이재희[2000]

하여 총 4개의 영역에서 14개의 중요 제품 성공 요인을 식별하였다.

(2) 개발 성공요인의 도출 및 측정 방법

본 연구에서는 국외내 문헌 분석 결과를 바탕으로 <그림 1>과 같이 3개의 영역에서 5개 요인을 네트워크 보안 시스템의 개발 성공요인으로 결정하였다.

환경 관련 요인은 성공적인 신제품 개발에 중요한 요인으로 식별되었으나, 본 연구에서는 다음과 같은 이유에서 제외하였다. 외부 기술/연구의 활용의 경우, 네트워크 보안 시스템에서 가장 많이 활용된 기술은 다중패턴매칭 차단 기술인데, 본 연구의 모든 분석 대상 네트워크 보안 시스템에서 공히 사용하였으므로 제외하였다. 법적 규제 요인도 국내 네트워크 보안 분야에서는 CC(Common Criteria) 인증이나 국정원 보안성 검토 같은 법적, 제도적 규제가 존재하지만, 비교 분석대상이 모두 같은 조건을 적용받기 때문에 본 연구에서 성공요인으로 큰 의미가 없다. 또한 특허권은 인터넷 표준이나 잘 알려진 기술을 사용하는 네트워크 보안 분야에서는 기업의 기술력을 홍보하는 수단에 불과하여 본 연구에서는 성공요인으로 채택하지 않았다.

본 연구에서는 시장관련 요인으로 시장 경쟁도와 시장 경쟁조건을 포함시켰다. 시장 경쟁도는 다수의 제품이 경쟁하고 있는 시장인지 여부를 나타내는 척도로서, 상용 제품의 수, 즉, 국내에서 판매실적이 있는 국산 및 외산 제품의 수로 측정하였다. 시장경쟁 조건의 경우, 네트워크 보안 시스템 분야는 가격경쟁이 매우 치열한 분야이므로 원가경쟁력이 매우 중요하고, 원가경쟁력은 정량화하기 어려운 소프트웨어 개발비를 제외하고 시제품 하드웨어 1대를 제작하는데 소요되는 재료비로 측정하였다

반면, 시장요구 적합도는 네트워크 보안분야에서 고객이 요구하는 제품의 척도가 다기능, 고성능이 가장 중요하기 때문에 기술 관련요인 중 제품의 품질 요인과 중복되어 제외하였다. 시장수요 및 성장성 요인은 본 연구가 단일 산업에서의 비교 분석을 주제로 하기 때문에 모든 제품에 대해서 동일한 조건이라 고려하지 않았다.

기술 관련요인에서는 제품의 품질과 우월성/혁신성을 모두 포함하였다. 제품의 품질은 제품이 지원하는 기능과 성능을 측정하였는데, 지원기능의 경우에는 관련 기능의 제공 여부로 측정하고, 이 기능을 적용한 상태에서 스마트비트라는 모든 국제공인 성능측정단체가 사용하고, 성능측정에 대한 국제표준을 준수하여 작동하는 성능계측기를 사용하여 성능을 측정하였다. 제품의 우월성/혁신성의 한 척도로서 이식성을 측정하였다. 현재 네트워크 보안 분야는 초대형 네트워크와 대형 네트워크, 중소형 네트워크로 제품군을 나누어서 제품을 생산하고 있으며, 한 가지 기능의 제품마다 제공하는 네트워크 대역폭에 따라 4~5가지의 제품군을 개발하기 때문에 이식성은 매우 중요한 요인이다. 범용 CPU 기반 시스템의 코드를 모태로 하여 다른 제품들이 개발되었기 때문에 이식성은 범용 CPU 기반 시스템에서 이식한 코드수와 전체 코드수의 비율로 측정하였다.

조직 관련 요인에서는 개발관리의 효율성 및 경영자의 지원 정도를 중요한 요인으로 포함시켰다. 조직 관련 요인을 복합적으로 볼 수 있는 변수로 타임투마켓(Time To Market) 변수를 채택하였고, 타임투마켓은 개발 기간과 함께 개발 과정에 참여한 연인원(Man/Year)으로 측정하였다.

개발책임자 권한크기 및 기업 내부 적합도는 단일 기업에서 동일 기능제품의 개선에 관한 성공요인을 분석하는 연구에서는 분석 대상이 같은 조건을 가지고 있어서 선정하지 않았다. 또

한, 개발/생산/마케팅/관리의 통합 및 조정을 통한 시너지효과 요인은 본 연구가 네트워크 보안 시스템의 신기술 적용을 통한 시스템적인 개선 방안을 주제로 삼고 있고 조직의 변화를 통한 신제품의 성공/실패를 분석하는 본 요인은 다양한 산업분야와 여러 회사의 비교분석에서 고려해야 할 요인이라 배제하였다.

(3) 개발 성공요인을 적용한 기존 네트워크 보안 시스템의 비교 분석

본 절에서는 앞에서 도출한 개발성공요인을 중심으로 기존 네트워크 보안 시스템을 분석한 결과를 정리한다.

먼저, 시장 관련 요인 중 상용 제품의 수를 조사한 결과 범용 CPU 기반은 국산은 어울림정보기술, 퓨쳐시스템, 윈스테크넷, 시큐어소프트, 넥스지사와 외산은 넷스크린, 시스코, 포티넷, 노키아, 체크포인트사가 있었다. 데이터 경로 분산 기반은 국산으로 지모컴, 시큐어소프트사와 와산으로 시스코사가 있었다. 부하분산 기반은 국산은 없었으며 외산은 크로스빔사가 유일하였다.

기술 관련 요인 중에서 성능은 성능측정 도구인 Smartbits 600을 사용하여 측정하였다. 방화벽의 성능을 측정하기 위해서 방화벽에 설정된 1개의 룰을 사용하고, 64개의 UDP(User Datagram Protocol) 세션을 생성하여 성능을 측정하였다. 침입방지시스템은 방화벽과 같이 64개의 UDP 세션을 생성하고, 64개의 UDP 세션내의 모든 패킷을 침입방지기능을 사용하여 검사하는 방식으로 성능을 측정하였다. 가상사설망(VPN)의 성능은 네트워크보안시스템 2대를 사용하여 보안시스템간 VPN 암호화 터널을 형성하였다. 암호화 터널에 사용되는 암호 알고리즘은 3DES-SHA-1을 사용하였으며, 3DES와 SHA-1은 대중적으로 사용되는 공개된 암호 알고리즘일 뿐만 아니라, 회사간 경쟁적 성능비교 시 일반적으로 사용되는 암호알고리즘이다.

기술 관련 요인 중에서 기능은 범용 CPU 기반 시스템은 모든 기능을 제공하였고, 데이터 경로 분산은 방화벽의 모든 기능과 침입 방지의 일부 기능만을 제공하였으며, 부하 분산 기반 시스템은 방화벽의 모든 기능과 침입 방지에서 일부 기능 및 VPN의 모든 기능을 제공하였다.

기술 관련 요인 중에서 이식성은 범용 CPU 기반 시스템의 코드를 다른 시스템으로 이식한 코드 수를 백분율로 표시하였다. 범용 CPU 기반 시스템간의 이식은 전체 198만 라인의 코드 중 하드웨어 플랫폼 및 기반 운용 체제가 바뀌어도 그대로 사용하는 부분이 95%에 달했고, 데이터 경로분산 기반 시스템에서는 일부 기능을 지원하지 못하므로 전체 125만 라인의 코드 중에서 NPU와 관련이 없는 코드만 재사용할 수 있어서 54%의 이식성을 보였다. 부하분산 기반의 시스템에서는 전체 217만 라인의 코드 중에서 범용 CPU 기반에서 이식 가능한 코드 187만 라인을 그대로 사용하여서 이식성을 86%로 평가하였다.

다음의 <표 3>에는 분석 결과가 종합 정리되어 있다. 표에서 볼 수 있는 바와 같이, 범용 CPU 기반 시스템은 원가경쟁력, 기능, 이식성, 타임투마켓 측면에서 강점을 가지고 있는 반면에 상용제품의 수와 성능에서는 단점을 보이고 있다. 데이터 경로분산 기반 시스템은 상용 제품의수와 성능 측면에서는 우위를 보이지만 기능과 이식성에서는 심각한 열세를 나타내고 있다. 부하분산 기반 시스템 또한 상용 제품의 수와 성능, 기능 측면에서 장점을 가진 반면, 원가경쟁력은 매우 떨어져 시장에 출시하기 어려운 점을 보인다. 결론적으로 기존의 네트워크 보안 시스템 개선 방법은 모두 고성능 및 다기능 보안 시스템으로는 미흡한 면들이 있다는 것을 알

〈표 3〉 기존 개선방법의 종합 정리

구 분			범용CPU 기반	데이터경로분산 기반	부하분산 기반
시장	재료비		500만원	1000만원	3000만원
	상용 제품의 수		10개	3개	1개
기술	성능	방화벽	64byte 200M/ 최대 2Gbps	64byte 1.8Gbps/ 최대 3Gbps	64byte 1Gbps/ 최대 10Gbps
		침입방지	1.2Gbps	X	6Gbps
		VPN	2Gbps	X	10Gbps
	기능	방화벽(4)	지원	지원	지원
		침입방지(8)	지원	부분 지원(2/8)	부분 지원(4/8)
		VPN(4)	지원	미지원	지원
	이식성		95%(187만/198만)	54%(67만/125만)	86%(187만/217만)
조직	타임투마켓		1.5Year + 22 M/Y	3Year + 12 M/Y	2Year + 6 M/Y

수 있다.

(4) 개발성공요인에 따른 네트워크 보안 시스템의 요구사항

본 연구에서는 기존 네트워크 보안 시스템 개선 방안들을 분석한 후, 개발 성공요인별로 목표치를 설정하고, 이를 달성할 수 있는 개선방안을 제시한다. 시장 관련요인 중 재료비는 원가 경쟁력을 최대한 확보할 수 있도록 1,500만원 이하를 목표로 하였다. 이 목표는 기존 네트워크 보안 시스템 개선방안에서 산출된 최저 원가 1000만원에서 선도적인 제품 개발로 인한 재료비 상승을 시장 우위로 감당할 수 있는 최저 목표로 판단된다. 상용 제품의 수는 특정 기업이 통제 가능한 변수는 아니지만, 선도적인 제품이 되기 위해서는 관련 시장에서 상용 제품의 수가 최대 2개 정도라고 판단된다. 경쟁 상용 제품의 수가 3개 이상일 경우에는 가격 경쟁과 시장 분할로 인해서 신제품 개발의 투자를 회수하기 어려울 가능성이 높기 때문이다.

기술 관련요인 중 방화벽의 성능은 10Gbps를 목표로 설정하였다. 그 이유는 10Gbps의 성능을 보유한 국내/외 상용 제품이 없기 때문이다. 또한, IPS와 VPN도 각각 6Gbps와 4Gbps로 목표치를 설정하였고, 이 성능을 보유한 국내/외 상용 제품도 찾아보기 힘들다. 기능은 네트워크 보안 시스템의 필요 기능을 모두 지원하는 것을 목표로 하였다. 이식성은 최소 80% 이상을 목표로 하였는데, 이것은 80% 이상의 이식성을 가지면 획기적인 소프트웨어 개발 생산성 향상을 이룰 수 있다는 소프트웨어 이식성에 관한 연구 결과[Griss, 1993]에 근거하였다.

조직 관련 요인인 타임투마켓은 기존 범용 CPU의 1.5년, 데이터경로기반의 3년, 부하분산의 2년 대비 1.5~3배 향상할 수 있는 1년으로 목표로 하였다. 기존 제품의 개발 기간보다 1.5~2배 정도의 개발 일정 향상을 보이면 타임투마켓의 향상을 가져올 수 있다고 한다[Griss, 1993].

3. 개발성공요인에 따른 네트워크 보안 시스템 개발

3.1 개발성공요인에 따른 네트워크 보안 시스템 체계

위에서 설정한 개선된 네트워크 보안 시스템의 요구사항은 네트워크 보안 시장에서 상용제

품이 존재하지 않는 10Gbps 네트워크 패킷 처리와 동시에 낮은 원가, 다기능 처리, 높은 이식성과 빠른 시장진출을 위한 타임투마켓을 요구한다.

현재 10Gbps급의 네트워크 보안 시스템을 개발할 수 있는 플랫폼에는 다음과 같은 세 가지가 있다. 첫째, 부하분산을 이용한 고속화 시스템은 기존의 네트워크 보안 시스템 개발 방안으로 제시하여 분석하였듯이 10Gbps의 네트워크 패킷처리를 할 수 있지만 높은 원가와 세션편중으로 인한 성능저하와 DOS(Denial Of Service) 공격에 약한 구조를 가지고 있다. 둘째, ASIC (Application Specific Integrated Circuit)을 이용한 시스템은 10Gbps의 네트워크 트래픽을 처리할 수 있는 프로세서를 자체적으로 설계하여 제작하는 방법으로 개발비 및 개발기간이 매우 과다한 방법으로써 시장요인에서 원가경쟁력과 타임투마켓의 개발성공요인에 취약하다. 마지막으로 멀티-코어 프로세서를 이용한 시스템은 10Gbps의 네트워크 트래픽을 처리하기 위하여 특별히 제작된 멀티-코어 상용 프로세서를 사용하는 방법으로서, 기존의 네트워크 보안 시스템 소프트웨어의 이식성을 높일 수 있는 표준 C 개발 환경과 LINUX 기반 개발 환경을 제공하여 다기능 개발에 적합하고 개발기간을 단축하여 타임투마켓 면에서 유리한 장점을 가지고 있다.

현재 판매되고 있는 멀티-코어 상용 프로세서는 RMI(Raza Micro-electronics)사의 XLR 프로세서와 Cavium사의 Octeon 프로세서가 있다. 두 프로세서는 서로 다른 방법으로 설계되어 장단점이 있으나, Octeon 프로세서가 16개의 500MHz MIPS 코어를 사용하는 반면에 XLR 프로세서는 8개의 1.5GHz MIPS 코어를 사용하여 전체적인 처리 능력면에서 XLR 프로세서가 우수하다. Octeon 멀티-코어 프로세서와 XLR 멀티-코어 프로세서의 평가를 위해서 단순 프로토타입을 구축하여 성능을 비교하였다.

단순 프로토타입에서는 각 보안 기능의 일부 소프트웨어 부분만을 탑재하고, 멀티 코어 프로세서에서 제공하는 여러 개의 코어 중에서 일부 코어만을 이용하여 성능을 측정함으로써 개략적으로 멀티 코어 프로세서의 총용량을 추정하였다. 방화벽에서는 접근통제 규칙 검색 부분만을 이식하여 측정하였으며, Octeon 프로세서는 1500 바이트의 패킷을 최대 13.5Gbps까지 처리할 수 있는 용량을 가지고 있는 반면, XLR 프로세서는 최대 26Gbps까지 처리할 수 있는 용량을 가지고 있는 것으로 나타났다. 실제로 이 용량에 비해 방화벽 전체 모듈이 구현될 경우에 많은 세션 처리 기능과 동적 세션관리기능으로 인해 성능은 축소될 것이다. 침입방지시스템 기능은 다중 패턴 매칭 차단 기능 중에서 시그니쳐와 패킷의 패턴 매칭하는 부분만 이식하였고, Octeon 프로세서는 패킷 하나당 27000 CPU 사이클을 소모한 반면, XLR 프로세서는 1600 CPU 사이클을 소모하였다. 가상사설망 기능은 암호처리 모듈에서 암호가속기로 패킷을 보내고 받는 부분만 이식하여 성능을 측정하였고, XLR 프로세서가 4개의 코어만을 사용하여 16코어 전부를 사용한 Octeon 프로세서와 성능에서 동수를 이루었다. 이러한 사전 평가 결과, 성능 측면에서 XLR 프로세서가 Octeon 프로세서보다 우수한 것으로 판명되어 개선 시스템을 위한 프로토타입으로 선정하였다.

3.2 개선 시스템 프로토타입 개발

(1) 프로토타입의 요건

1) 하드웨어 요건

개선된 시스템의 프로토타입은 원가 경쟁력을 갖추기 위하여 1,500만원 이하의 원가를 목

표로 제작되어야 한다. 개선 시스템은 프로세서로 선정된 RMI사의 XLR 프로세서로 제작된 프로토타입을 1500만원의 원가로 제작하기 위하여 네트워크 인터페이스를 모듈화하였으며, 두 개의 프로세서 보드는 저렴한 기가 이더넷으로 연결하였다. 두 개의 프로세서 보드로 빠른 경로와 느린 경로를 물리적으로 분리하고, 멀티-코어 프로세서를 바탕으로 각 경로에서 분산처리를 하여 개선 시스템의 프로토타입은 10Gbps의 네트워크 패킷처리를 가능하게 하고 10Gbps급의 고성능을 통해 네트워크 보안시장에서 경쟁제품의 수를 제한하는 것을 지원하도록 한다.

2) 소프트웨어 요건

프로토타입을 제작하기 위한 소프트웨어 요건으로는 다기능의 네트워크 보안 시스템을 제작하기 위하여 표준 C 기반의 개발 환경과 임베디드 LINUX 기반의 개발 환경을 통해서 기존 네트워크 보안 시스템 기능의 이식성을 높여야 한다. 이러한 표준 개발 환경과 높은 이식성은 통합 네트워크 보안 시스템이 다양한 기능을 구현하기 좋은 환경을 제공할 뿐만 아니라 개발기간을 최적화하여 타임투마켓의 요건을 충족시킬 수 있도록 한다.

(2) 아키텍처

1) 하드웨어 아키텍처

개선된 시스템의 하드웨어 아키텍처는 각각 별도의 멀티코어 프로세서 보드에서 빠른 경로와 느린 경로를 분리 처리하기 위하여 전체 시스템은 6개의 보드로 구성되며, 이중 2개는 멀티코어 프로세서를 장착한 프로세서 보드이고, 1개의 매니지먼트 보드, 2개의 네트워크 인터페이스 모듈, 그리고 2개의 프로세서 보드와 매니지먼트 보드를 연결하는 미드-플레인으로 구성된다. 두 개의 프로세서 보드 중 하나는 XLR732 멀티코어 프로세서가 장착된 빠른 경로를 처리하기 위한 하드웨어 보드이고, 나머지 하나는 XLR532 멀티코어 프로세서가 장착된 느린 경로를 처리하기 위한 하드웨어 보드이다. 두 개의 프로세서 보드에는 각각 DDR2 533Mhz 메인 메모리가 4GByte 장착되며, 구동될 프로그램들이 적재될 공간으로 256MByte의 플래쉬(Flash) 메모리가 장착되어 있다. XLR732와 XLR532의 차이는 내부에 SPI(System Packet Interface) 인터페이스가 존재하느냐에 여부이며, SPI 인터페이스가 있는 XLR732(빠른 경로)로 네트워크 모듈이 장착되게 된다. SPI 인터페이스란 다양한 네트워크 인터페이스 모듈로부터 들어오는 패킷을 CPU로 전달하는 인터페이스 표준이다. 두 보드간 통신용 인터페이스는 4개의 기가 이더넷 인터페이스 중에서 3개를 사용하여 이 보드들을 연결한다.

2) 소프트웨어 아키텍처

고속의 네트워크 보안 장비에서는 빠른 경로(Fast Path)와 느린 경로(Slow Path)를 구분하여 패킷을 처리함으로써 특정 패킷의 처리지연이 전체적인 시스템 성능 저하를 야기하는 것을 방지한다. 따라서 고속 장비에서 패킷 처리에서의 지연을 줄 수 있는 요소는 느린 경로에 구현한다[Gupta, etc., 1999].

고전적인 방화벽의 경우에는 접근 통제를 위한 방화벽 정책을 찾는 과정을 두 과정으로 분리하여 특정 세션의 첫 번째 패킷은 정적 정책(Static Rule)로부터 정책을 참조하게 되고, 정적 정책으로 만들어진 동적 정책(Dynamic Rule)은 고속 캐쉬 구조로 만들어 두 번째 패킷은 이 고속 캐쉬 상에 놓여진 동적 정책을 참조하여 해당 정책을 수행하게 된다. 이때 고전적인 빠른 경로와 느린 경로의 구분에서 동적 정책은 빠른 경로에 구현되며, 정적 정책은 느린 경로

에 구현이 되었다. 그러나 이러한 구조는 세션의 두 번째 패킷부터 고속처리가 가능하며, 전송되는 패킷 중 많은 부분이 세션의 첫 번째 패킷에 해당한다면 느린 경로에 부하를 가중시켜 장비 자체에 위협을 가할 수 있다. 최근에 많이 볼 수 있는 SYN Flooding 공격과 스캔(Scan) 공격은 대부분이 세션의 첫 번째 패킷만으로 공격을 수행하게 되며, 고전적인 빠른 경로와 느린 경로의 구분에서 느린 경로에 상당한 부하를 주는 공격이 된다.

이런 문제점을 해결하기 위해서 본 장비에서는 고전적으로 빠른 처리가 필요한 기능들과 해당 기능들과 밀접하게 연관된 모든 기능들을 빠른 경로에 구현하였으며 빠른 경로를 위한 운영체제로는 RMI-OS라는 운영 체제를 사용하였다. 이 RMI-OS는 하드웨어 디바이스를 제어에 필요한 디바이스 드라이버들로만 구성된 멀티-코어 프로세서용 임베디드 운영체제이다. 이 RMI-OS 위에 이더넷 브릿지, 라우팅, VLAN과 같은 L2/L3 네트워크 기능이 구현되었다.

빠른 경로에 구현된 보안 기능으로는 입력된 패킷에 대한 방화벽 정책을 찾고, 찾아진 정책대로 패킷을 처리하는 접근통제기능을 들 수 있다. 이 기능은 다시 스테이트풀 인스펙션(Stateful Inspection)을 적용한 정책 기반 방화벽 기능과 URL 기반의 URL 차단기능을 제공한다. 정책 기반 방화벽 기능은 방화벽 정책 찾기와 세션 관리가 주요 기능이 된다. 세션 관리상에서 가장 부하를 주는 요소는 세션 생성과 세션 삭제이다. 세션이 생성되는 시점은 개별 패킷이 입력되는 시점이지만, 세션의 삭제는 매초마다 세션 테이블에서 세션 유지시간이 지난 엔트리들을 한꺼번에 삭제하게 된다. 동일한 코어가 세션의 삭제와 생성을 같이 수행할 경우 세션의 생성을 먼저 수행하여 삭제가 정상적으로 수행하지 않을 수가 있다. 이런 상황을 막기 위해서 32개의 하드웨어 쓰래드 중에서 1개의 쓰래드를 세션 삭제만을 전담하도록 만들어 세션 삭제가 원활히 수행되도록 하였다.

빠른 경로에 구현된 IPS 기능으로는 IPS 정책에 의해 이미 설정된 공격패턴들과 패킷의 IP 헤더를 포함한 페이로드(Payload)를 비교하여 유해한 패킷을 찾는 다중 패턴 매칭 차단기능과 LAND 공격방어, SYN Flooding 차단, 미확인 발신지 주소 차단, IP Source Route 차단 기능을 빠른 경로에 구현하였다. 다중 패턴 차단은 수백만번의 메모리 비교를 수행하기 때문에 L1/L2 캐쉬를 효율적으로 운용할 수 있도록 프로그램을 작성하는 것이 성능의 관건이 된다. 본 프로토타입에서는 32바이트 캐쉬 라인에 맞게 자료구조를 작성하였으며, 한번 캐쉬에 올라온 데이터에 대해서는 최대한 활용될 수 있도록 하였다.

LAND 공격방어는 출발지/목적지 IP 주소 및 포트가 같은 TCP SYN의 전송을 막는 기능이며, SYN Flooding 차단은 특정 호스트로 유효하지 않은 SYN 패킷이 과다하게 전송되어 서버의 TCP 리소스를 과다하게 점유시켜 정상동작 하지 않도록 만드는 행위를 차단시켜주는 기능이다. 미확인 발신지 주소 차단 기능은 외부에서 내부 IP 주소를 출발지 주소로 위장하는 패킷을 차단하거나 외부에서 사설 IP를 사용하는 트래픽이 내부망으로 유입되는 경우 차단시켜주는 기능이다. IP Source Route 차단 기능은 패킷의 IP 헤더내에 Source Route 옵션이 켜진 패킷을 차단하는 기능으로, 공격자가 패킷이 특정서버를 경유시키는 우회공격을 막는다.

이러한 LAND 공격방어, SYN Flooding 차단, 미확인 발신지 주소 차단, IP Source Route 차단 기능들은 매 패킷마다 모두 검사되어야 하며, 이런 기능들을 느린 경로에 구현할 경우 모든 트래픽을 느린 경로로 보냈다가 되받아야 하므로 빠른 경로와 느린 경로 사이의 트래픽 처

리 용량이 문제가 된다. 왜냐하면 본 장비에서는 10기가 트래픽이 처리되어야 하므로 적어도 빠른 경로와 느린 경로사이에는 20기가 트래픽이 처리되도록 물리적인 링크가 제공되어야 하기 때문이다. 하지만 실제로 본 구현에서는 빠른 경로와 느린 경로 사이에 3기가 링크로 구현되기 때문에 위와 같은 기능을 느린 경로에서 제공하는 것은 불가능하다.

빠른경로에서 구현된 또 다른 기능은 ICMP Destination Unreachable 패킷의 해킹 가능성을 방지하는 ICMP 차단 기능이다. 이 기능을 느린 경로에 구현할 경우 느린 경로로 패킷을 주어 검사후 빠른 경로에서 다시 받아 네트워크 단으로 전송시켜야 한다. 이때 빠른 경로에서는 느린 경로로 패킷을 전송시켰다가 되돌려 받는 작업을 수행해야 하며, 이 작업 자체가 오히려 빠른 경로에서 공격을 검사하는 방식에 비해 시스템에 더 많은 부하를 주게 된다.

가상 사설망을 위해서 빠른 경로에서는 IPSec 모듈과 보안 데이터베이스 모듈, 암호처리 모듈이 구현되었다. 본 프로토타입에서 사용한 프로세서는 멀티코어를 제공하여 프로세싱 성능을 고도화 하였을 뿐만 아니라 프로세서 내에 DES/3DES/AES/SHA-1/MD5와 같은 암호화 기능을 하드웨어적으로 제공하므로 가상 사설망의 주요 기능들을 빠른 경로에서 제공하더라도 운용시 소프트웨어적인 부하는 많이 들지 않게 한다.

본 시스템에서 느린 경로에는 내부 호스트가 외부 웹 서버에 접속하는 경우 웹 서버에서 유해한 내용이 내부로 유입되는지를 검사하는 HTTP 프록시와 SMTP로 메일 전송할 때 유해한 내용이 있는지를 검사하는 SMTP 프록시, 외부 사용자가 내부 메일서버에 접속을 시도할 때 유해한 공격을 가하는지를 검사하는 역방향 SMTP 프록시가 구현되어 있다. 프록시 처리를 위해서는 TCP 패킷들의 재조합, 트래픽의 재구성, HTTP나 SMTP같은 L4 수준의 프로토콜 해석 같은 복잡한 작업이 필요하므로 느린 경로에 구현하였다. 또한 빠른 경로와 느린 경로에서 생성된 로그들을 취합하는 기능과 시스템 관리를 위한 GUI 처리부가 느린 경로에 구현되어 있다. 한편, 수집된 로그를 분석하여 공격을 탐지하는 SCAN 공격처리부가 느린 경로에 구현되었다.

이러한 보안 기능들 외에도 빠른 경로와 느린 경로 사이의 데이터를 주고 받기 위한 프로토콜 해석기가 빠른 경로와 느린 경로 양편에 구현되었다. 이 프로토콜 해석기를 구현할 때 가장 고려해야 할 문제가 두 가지 있다. 하나는 이 두 경로 사이의 통신이 물리적으로 데이터의 파괴나 손실이 있느냐는 것이다. 또 하나는 트랜젝션이 일어날 경우 한번에 원하는 데이터를 모두 보낼 수 있느냐 혹은 분할해서 보내야 하느냐는 것이다. 느린 경로 보드와 빠른 경로 보드가 일반 통신 케이블이 아닌 커넥터로 연결되어 있으므로 통신시 데이터 파괴나 누수가 생길 가능성이 상당히 낮지만 확률적으로 0이 아니므로 통신시 반드시 데이터의 무결성을 검증하도록 하였다. 빠른 경로와 느린 경로는 3개의 기가비트 이더넷 채널로 연결되어 있어서 한번에 최대로 전송할 수 있는 데이터 크기는 MTU로 결정되며 이 MTU는 최대 8192 바이트이다. 하지만 통신시 하나의 트랜젝션이 최대 500 메가바이트 정도가 될 수 있으므로 빠른 경로와 느린 경로 사이의 통신에서는 데이터 분할과 데이터 조합 기능이 모두 구현되었다.

4. 개선 시스템의 평가 결과

본 절에서는 본 연구에서 제시한 멀티-코어 프로세서 시스템을 개발 성공요인의 목표치에 대비하여 평가한 결과를 제시한다.

〈표 4〉 멀티-코어 시스템의 검증 결과

구 분			목표치	검증 결과
시장	원가경쟁력 (재료비)		1,500만원 이하	약 1,000만원
	상용제품		2개 이하	0개
기술	성능	FW	10Gbps	64byte 7Gbps / 최대 10 Gbps
		IPS	6Gbps	10 Gbps
		VPN	4Gbps	4 Gbps
	기능	FW(4)	지원	지원
		IPS(8)	지원	지원
		VPN(4)	지원	지원
	이식성 (코드수)		80% 이상	82% (184만/225만)
조직	타임투마켓		개발기간 1년	1Year + 15 M/Y

<표 4>에서 볼 수 있는 바와 같이, 본 연구에서 제안한 멀티-코어 프로세서 시스템은 목표치를 모두 충족시키고 있는 것을 알 수 있다. 다음에서는 각 항목별로 검증한 결과를 세부적으로 정리한다.

시장 관련요인 중 원가경쟁력(재료비) 항목의 경우, 목표한 1,500만원에 비해 프로토타입을 약 1,000만원에 구축하여 원가 경쟁력을 더욱 높였다. 상용제품 항목의 경우, 아직까지 국내에 출시된 상용 제품은 없는 것으로 조사되었다.

기술 관련 요인 중 성능 항목의 경우에는 10 Gbps를 목표로 하였는데 개선된 시스템의 성능을 Smartbits 600 계측기를 사용한 결과, 128 바이트 이상의 패킷에서는 모두 10Gbps의 성능을 달성하였다. 침입방지시스템의 성능 측정은 최소 5Gbps, 최대 10Gbps의 침입방지시스템 성능을 달성하였으며, 가상 사설망의 성능은 최소 0.7Gbps, 최대 4Gbps의 가상 사설망 성능을 달성하였다.

또한 기술 관련 요인 중 기능 항목의 경우에는 전 기능을 지원하는 것을 목표로 하였는데, 방화벽, 침입방지시스템, VPN의 모든 기능을 지원할 수 있었다. 또한 이식성 항목은 80%이상을 목표로 하였는데, 225만 라인의 전체 코드 수에 184만 라인의 코드를 이식하여 82%의 이식성을 가진 것으로 확인되었다.

조직 관련 요인의 경우에는 15명의 인력을 투입하여 프로젝트 기간을 1년으로 단축하고, 시장 출시 시기를 앞당기는 개발 전략을 달성하였다.

5. 결 론

본 연구에서는 네트워크 보안 시스템을 개선하기 위한 여러 가지 방법을 분석하고, 하나의 대안을 제시하였다. 기존의 개선 방법들은 네트워크 보안 시스템 개발에 관련된 복합적인 요인들이 체계적으로 고려하지 못한 측면이 존재하였다.

이에 따라 본 연구에서는 종합적인 연구문헌 분석을 통해서 네트워크 보안 시스템 개발의 성공요인들을 도출하고, 이에 대한 목표치를 설정하여 개선된 네트워크 보안 시스템의 개발 방법을 제시하였다. 제안한 방법은 멀티-코어 프로세서에 기반한 방법으로서 빠른 경로와 느린 경로에 대해서 각각 별도의 멀티-코어 프로세서를 사용하는 구조이며, 이는 NPU로 구현하는 방법에 비해 표준 C 언어를 사용함으로써 기능 및 이식성의 측면에서 우수한 장점을 보였고 타임투마켓 요인을 만족시키는 중요한 요소가 되었다. 제시한 개선 네트워크 보안 시스템은 프로토타입의 구현을 통하여 6개의 성공 요인에 대한 목표치를 모두 충족시켰다.

개발 성공 요인에 대한 분석은 프로젝트가 일정 부분 진행되기 전에는 알 수 없는 부분들이 많으므로 본 연구과 같이 체계적으로 개발성공요인에 대한 접근을 하지 않으면 일부 성공요인을 만족시킬 수 없어도 프로젝트 종료 시점

까지 계속 진행을 하는 경우가 많다. 이러한 면에서 본 논문에서 제시된 성공 요인은 다른 프로젝트에도 많은 도움이 될 것으로 판단된다. 또한 본 논문은 이러한 성공 요인을 고려하여 실제로 프로토타입을 구축하고 성공 요인에 대한 목표치가 달성 가능함을 보였다. 마지막으로, 본 논문에서는 네트워크 보안 시스템을 개발하는 방법을 종합 정리하였다. 이전의 단편적인 연구에서는 어느 한 가지 방법만을 연구하였으므로 이를 체계적으로 비교 분석하여 장단점을 밝히는 것이 미흡하였다. 본 논문에서는 다양한 방법을 분석함으로써 다른 네트워크 보안 시스템 개발에도 많은 도움이 되리라고 판단된다.

향후 연구 과제로는 본 연구에서 제시한 10G급 네트워크 보안시스템 보다 고성능을 제공할 수 있는 시스템에 대한 연구가 필요하다. 또한 본 연구에서는 빠른 경로의 고속화 방법에 주로 초점을 맞추었으나 근래에는 바이러스 등 악성 코드의 영향으로 느린 경로의 고속화에 대한 요구가 점차 높아지고 있다. 이를 위한 성공요인의 목표치 도출 및 기술적인 해결 방법에 대한 연구도 매우 중요하리라 예상된다.

참 고 문 헌

[1] 김지대, "소기업과 대기업의 신제품개발 성공요인에 관한 비교연구", 한국생산관리학회지 제10권 제2호, 1999, pp. 147-181.

[2] 안기현, "신제품개발 성패예보관리주조의 모형화", 성균관대학교 석사학위논문, 1993.

[3] 이재희, "한국과 미국의 신제품개발 성패요인에 대한 국제 비교 연구", 한국과학기술원 테크노경영대학원 경영공학 박사학위논문, 2000.

[4] 인터넷역사위원회, "한국 인터넷 약사", 2005년 4월.

[5] 최수호, "우리나라 주요 제조업체의 신제품 성공/실패 결정요인과 신제품 개발 전략에 관한 실증적 연구-특히 국내 주요 소비재 및 산업재를 중심으로", 고려대학교 박사학위논문, 1994.

[6] 행정자치부, "행정전산화 기본계획", 1978년 2월.

[7] 행정자치부, "행정전산화 수정계획", 1979년 12월.

[8] 행정자치부, "제2차 행정전산화 기본계획", 1982년 12월.

[9] Brentani, de.(1986) "Do firms need a custom designed new product screening model?", Journal of Product Innovation Management, pp. 109-119.

[10] Booz, Allen and Hamilton. *New Product Development in the 1980's*. Booz, Allen and Hamilton, New-York, 1982.

[11] Cooper, R. G., "The Dimensions of Industrial New Product Success and Failure", *Journal of Marketing*, Vol. 43, No. 3, Summer 1979a, pp. 93-103.

[12] Cooper, R. G., "Identifying Industrial New Products Success : Project NewProd", Industrial Marketing Management, Vol. 8, May 1979b, pp. 315-326.

[13] Cooper, R. G., "New Product : What Separates Winners from Losers?", Journal of Product Innovation Management, Vol. 4, 1987, pp. 169-184.

[14] Cooper, R. G., "Selecting Winning New Product Projects : Using the NewProd System", Journal of Product Innovation Management, Vol. 2, 1985, pp. 34-44.

[15] Cooper, R. G. and Kleinschmidt, E. J. What makes a new product a winner :

success factors at the project level. *R&D Management*. Vol. 17, No. 3, 1987, pp. 175-189.

[16] Cooper, R. G. and Kleinschmidt, E. J. , "New Product Success Factors : A Comparison of Kills versus Success and Failures", *R&D Management*, Vol. 20, No. 1, 1990, pp. 47-63.

[17] Chapman, D. B. and E. D. Zwicky, Building Internet Firewalls, O' Reilly & Associates, 1995.

[18] Cisco PIX Firewall Software (http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd_products_support_series_home.html).

[19] Davey, A, and Jozef Wroblewski., "Concepts & Example : ScreenOS Reference Guide", Release 5.3.0, Rev.B, Juniper

[20] Feldman, A. and S. Muthukrishnan. "Tradeoffs for packet classification", *Proceedings of Infocom*, Vol. 3, March 2000, pp. 1193-202.

[21] Griss, Martin L., "Software Reuse : From Library to Factory", IBM Systems Journal, August 1993.

[22] Gupta, Pankaj, and Nick McKeown. "Packet Classification on Multiple Fields" *ACM SIGCOMM '99, September 1999.*

[23] Kwaku, A. G., "Marketing Orientation and Innovation", Journal of Business Research, Vol. 35, 1996, pp. 93-103.

[24] Kaufman. C, "Internet Key Exchange (IKEv2) Protocol", December 2005.

[25] Kent, S., "IP Authentication Header", RFC 4302, December 2005a.

[26] Kent, S., "IP Encapsulating Security Payload", RFC 4303, December 2005b.

[27] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[28] Kumar, S. and E. Spafford, "A Pattern Matching Model for Misuse Intrusion Detection." *In Proc. of the 17th National Computer Security Conf.,* Oct. 1994, pp. 11-21.

[29] Montoya-Weiss, M. M. and Calantone, R. "Determinants of new product Performance : A review and meta-analysis", Journal of Product Innovation Management, 1994, pp. 397-417.

[30] Maidique, M. A. and B. J. Zirger, "A study of Success and Failure in Product Innovation : the Case of the U. S. Electronics Industry", IEEE Transactions on Engineering Management, Vol. 31, November 1984, pp. 192-203.

[31] Qin, X. D. Dagon, G. Gu, and W. Lee, "Worm Detection Using Local Networks", Technical report, College of Computing, Georgia Tech., February 2004.

[32] Rothwell. R, C. Freeman, A. Horlsey, V. T. P. Fevis, A. B. Robertson, and J. Townsend, "SAPPHO Updated : Project SAPPHO Phase II", Research Policy, 1974, pp. 258-291.

[33] Souder, W. E. and A. K. Chakrabarti, "The R&D/Marketing Interface: Results from an Empirical Study of Innovation Projects", IEEE Transaction On Engineering Management, Vol. 25, No. 4, November 1978, pp. 88-93.

[34] Spirent communications, "Performance Measurement within the Tolerances of the

IEEE Specifications", March 2003.

[35] Sourdis, I. and D. Pnevmatiktos, "Pre- decoded CAMs for Efficient and high-Speed NIDS Pattern Matching", *in Proc. of 12th IEEE Symp. on Field Programmable Custom Computing Machines*, Apr. 2004.

[36] Urban, G. L. and J. R. Hauser (1993), Design and Marketing of New Products, 2nd ed., Englewood Cliffs, NJ : Prentice-Hall.

[37] Utterback, J. M., J. A. Thomas, and H. Gerstenfeld, "A Study of Successful Projects, Unsuccessful Projects, and Projects in Process in West Germany", IEEE Transactions On Engineering Management, Vol. 23, August 1976, pp. 116-123.

[38] Withey, James. "Investment Analysis of Software Assets for Product Lines", Software Engineering Institue, Carnegie Mellon, CMU/SEI-96-TR-010.

[39] Zirger, B. J. and Maidique, M. A.(1990), "A Model of New Product Development : An Empirical Test", *Management Science*, Vol. 36, No. 7, pp. 867-883.

■ 저자소개

김 종 선

현재 시큐아이닷컴(주) 대표이사로 재직 중이고, 삼성SDI CIO, 삼성SDS 상무 등을 역임하였다. 서강대학교 수학과를 졸업하고, 동 대학교에서 경영학 석사를 취득하였고, 동국대학교에서 경영정보학 박사과정을 수료하였다. 주요 관심분야는 정보전략, 전사적자원관리(ERP), IS성과관리, 정보보호 등이다.

황 경 태

현재 동국대학교 경영대학 경영정보학과 교수로 재직 중이다. 연세대학교 상경대학을 졸업하고, Geroge Washington University에서 경영학 석사, State University of New York at Buffalo에서 경영정보학 박사학위를 취득하였다. 주요 관심분야는 정보 전략, IT 서비스 관리, IT 거버넌스 등이다.

◈ 이 논문은 2007년 09월 27일 접수하여 1차 수정을 거쳐 2007년 12월 22일 게재확정되었습니다.