차세대 네트워크 보안 시스템

정연서* · 김환국* · 서동일*

*한국전자통신연구원 네트워크보안연구부

Network Security System for Next Generation Network Environment

Youn-Seo Jeong* · Hwan-Kuk Kim* · Dong-il Seo*

*Dept. of Network Security Research, ETRI

E-mail : jys847@etri.re.kr

요 약

컴퓨팅 기술과 네트워킹 기술이 급속도로 발전하였다. 현재 인터넷 환경은 우리에게 음성, 멀티미디어 데이터 및 동영상 서비스까지도 제공해 주고 있다. 그러나 해킹 건수 늘어나고 있으며, 그 피해가 심각해지고 있다. 본 논문에서는 해킹기술과 보안 패러다임의 변화에 관하여 살펴보고 보안시스템들의 현황을 조사 분석한다. 그리고, 마지막으로 차세대 네트워크 환경에서 고려해야 할 네트워크 보안 시스템에 관하여 고찰한다.

ABSTRACT

Computing and Networking technologies are rapidly developed. Currently, Internet environment can offer voice, multimedia data as well as real-time movie services. But, the number of hacking has increased very much and the damages become serious. In this paper, the change of hacking method and security paradigm is investigated. And, we study in existing network security systems including newly developed security systems. Finally, we describe development directions of network security system for next generation network environment.

키워드

네트워크 보안, 네트워크 보안시스템, 해킹

Ⅰ. 서 론

웹 서비스의 출현으로 인터넷이 급속하게 발전하게 되었으며, 많은 컴퓨터 시스템들이 네트워크로 연결되어 있다. 전 세계는 이와 같은 환경에서 시간과 장소의 제약 없이 통신이 가능하게 되었으며, 정보사회로 한걸음씩 다가서고 있다. 그러나, 이에 반하여 구석구석 연결된 네트워크를 통하여 이루어지는 불법적인 침입과 정보 유출, 시스템 마비로 인한 많은 문제들이 발생하고 있다. 기관과 네트워크 관리자들은 외부로부터의 유해한 침입과 행위들에 대처하기 위해서 데이터를 암호화하여 전달하거나 침입차단(Firewalll), 침입탐지(IDS : Intrusion Detection System), 취약성 분석(Scanner), 바이러스 탐지/차단 등의 다양한 기능들을 가진 보안시스템들을 설치하여 운영하고 있다. 허나 네트워크의 트래픽이 증가하고, 공격기법이 지능화되고 복잡해지고 있는 추세여서 소프트웨어 기반의 단일 기능 위주의 보안 시스템들로는 이에 대처하기가 어렵다. 그러므로, 새로운 환경에 적합한 보안 시스템의 필요성이 커지고 있다.

본 논문에서는 Ⅱ장에서 해킹 기술의 발전에 대해서 조사 분석한다. Ⅲ장에서 네트워크 보안시스템들의 개발 동향에 대해서 분석한 후 차세대 네트워크 환경을 위한 네트워크 보안시스템에 대해서 고찰한다. 그리고, 마지막으로 Ⅳ장에서 결론을 맺는다.

Ⅱ. 해킹 기법과 보안 패러다임의 변화

1. 해킹 기법의 변화[3,4]

해킹 기법들은 점차 자동화, 지능화, 대중화,

분산화, 대규모화, 고속화, 은닉화, 범죄화 되어 가고 있으며, 공격 유형도 특정 호스트 중심에서 네트워크 전체에 대한 공격으로 바뀌고 가고 있다. 기법들을 살펴보면 점차로 간단하고 취약점을 이용한 자동화된 툴들을 제작해서 분산 공격이 이루어지고 있는 것을 알 수 있다[그림 1].

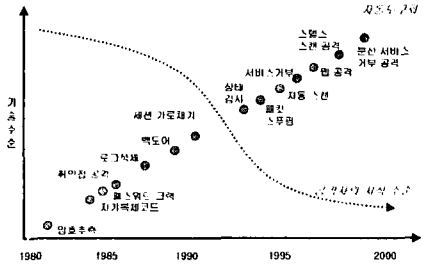

그림 1. 해킹 기법의 변천과 공격자의 지식 수준

최근 심각한 피해를 입히고 있는 공격들은 웜 바이러스 형태를 띄고 있는데, 이러한 웜바이러스들은 단시간내(수분 내지 수십분)에 해당 지역이나 국가의 기간망을 마비시킬 수 있는 피해를 줄 수 있다.

향후로는 리눅스 운영체계 대중화에 따라 이를 기반으로 하는 바이러스와 PDA, 휴대폰 등 모바일 디바이스를 기반으로 하는 바이러스, 현재 많은 피해를 가져다 주고 있는 e메일을 통한 웜과 바이러스의 대량 유포가 더욱 기승을 부릴 것으로 보인다. 그리고, 유무선이 통합되고 방송과 정보 및 통신이 융합되는 차세대 네트워킹 환경에서는 기존의 유선망과 마찬가지로 무선 네트워크와 이동 통신망도 사이버 테러의 위험성이 높아 이에 대한 대안 마련이 시급하다[5].

2. 보안 패러다임의 변화[1]

기존에는 기관이나 연구소 등의 특정 시스템들을 해킹하거나 금융 시스템들을 침입하여 정보를 불법으로 갈취하거나 과시용으로 시스템을 변조/훼손시키는 형태의 공격들이 이루어졌다. 그러나, 최근에는 네트워킹 장비들을 공격하거나 웜의 유포로 트래픽을 증가시켜 네트워크 소통을 지연시키고, 감염된 시스템이 또 다시 다른 시스템들에게 이를 대량으로 유포되는 등의 전체 네트워크를 대상으로 공격이 이루어지고 있다. 이러한 공격들은 지극히 짧은 시간에 이루어지기 때문에 많은 피해를 가져다 주고 있다. 최근 발생했던 "1.25 슬래머 웜 사태"가 이것을 대표적으로 반영해 준 대표적인 사례로 볼 수 있으며[그림 2], 이 사건을 계기로 기존의 지역 네트워크를 보호하는 단일 기능 위주의 소프트웨어 기반 보안시스템들에서 벗어나 사전에 네트워크단에서 미리 예측하고 방어할 수 있는 개념들이 추가된 고속의 하드웨어형 시스템들에 대한 연구가 주목을 끌고 있다. 우리 나라를 비롯한 세계 각국에서는 기존의 보안체계를 보완하고 새로운 체계 수립에도 박차를 기하고 있다. 정부에서는 현재 국가적 차원의 인터넷망 보호 체계 구축 작업을 추진 중에 있으며, 국내의 인터넷 트래픽에 대한 감시와 공동 대응, 정보 공유를 위해 필요한 법, 제도 제정과 이를 위한 시스템 구축과 기술 개발에 박차를 기하고 있다.

그림 2. 슬래머 웜의 확산 속도(30분 경과)

III. 네트워크 보안 시스템의 현황과 전망

1. 현황[3]

현재 운용되고 있는 대표적인 네트워크 보안 시스템들로는 침입차단시스템(Firewall), 침입탐지시스템(Intrusion Detection System: IDS), 바이러스 방지 시스템(Anti-Virus) 등이 있다. 침입차단시스템은 차단 리스트에 따라 외부망으로부터 내부망으로의 패킷 유입을 차단하는 기능을 수행하며, 침입탐지시스템은 패킷들을 분석하여 유해한 패킷을 탐지하고 통보하는 기능을 위주로 하고 있다. 이외에도 파일 서버나 메일 서버에 설치되어 바이러스 감염을 사전에 수행하는 바이러스 월 시스템과 사전에 네트워크의 취약점을 분석하여 보완하는 취약점 분석 제품들도 운용하고 있다. 침입차단시스템의 보안 정책은 주로 네트워크 주소와 프로토콜 정보들로만 정책을 수립하고 있기 때문에 상세한 차단이 어려워 많은 취약점(우회기법)을 갖고 있으며, 침입탐지시스템의 경우도 정해 놓지 않은 패턴을 벗어나는 경우가 많고 다양한 우회 기법들이 존재하고 있다. 그리고, 사용자의 급격한 증가로 인한 망의 고속화와 방대한 트래픽의 증가로 기존의 소프트웨어(software) 기반의 보안 시스템[그림 3]으로는 이러한 방대하 트래픽들을 처리하기 어렵다.

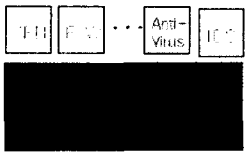

그림 3. S/W 기반의 보안시스템

가. 침입차단시스템(방화벽)

방화벽은 접근제어목록(Access Control List)에 따라 내부 네트워크의 자원들의 보호를 담당하고 있는 솔루션이다. 제품 동향을 살펴 보면 초고속망의 사용증가에 따른 고속장비의 요구에 따라 넷스크린사와 시스코, 서브게이트(Servgate)사 등에서 이미 기가급의 방화벽을 출시하였으며, 이동전화 단말기 업체인 노키아에서도 체크포인트의 방화벽 S/W를 하드웨어 플랫폼에 탑재하여 기가급 솔루션을 내놓고 있다.

제공되고 있는 대부분의 방화벽 제품은 자체의 기능인 네트워크 접근 차단 기능 외에 바이러스 차단, 컨텐츠필터링, 메일제어, NAT, VPN등 많은 다양한 보안 기능들이 포함되고 있으며, 최근에는 단독으로 운용되기 보다는 침입탐지 시스템과 연계되어 동작되는 경우가 많다. 일반적으로 최근 방화벽 제품들은 트래픽의 고속 처리를 위해 스위칭 장비 기반의 플랫폼에 탑재되는 형태로 많이 개발되고 있으며, 고속의 프로세싱을 위한 전용 칩을 사용하고 있다. 국내에서도 고속의 성능을 위해서 전용의 네트워크 프로세서에 탑재하는 형태의 제품도 개발완료 단계에 있다. 그리고 정적인 차단 리스트에 의한 동작을 개선하기 위해 침입탐지를 내장하여 동적으로 정책을 변경하여 대응하는 제품들의 연구 개발이 활발하게 이루어지고 있다.

나. 침입탐지시스템

침입탐지시스템은 네트워크 패킷을 분석하고 이러한 패킷 중 해킹의 징후를 띠고 있는 것이 발견될 경우 관리자에게 경보 메일 송신, 공격 세부사항 로깅 또는 접속 단절 등 여러 다양한 대응 옵션을 제공하며 대부분의 침입과 공격을 탐지할 수 있는 시스템이다. 그러나 대부분이 패턴에 일치되는 경우의 탐지가 주를 이루고 있으며 이를 벗어난 경우 탐지가 어려운 단점이 있다. 침입탐지시스템은 패킷의 내용을 분석하고 이를 분석하고 침입인지를 저장된 공격패턴(signature)와 비교 분석하여야 하기 때문에 여기에서 오는 많은 부하가 발생한다. 이를 해결하기 위한 다양한 노력들이 이루어지고 있다. 고속의 장비와 4 계층 스위칭 장비를 이용한 로드 밸런싱 장비를 이용해서 해결하고 있으며, 침입탐지시스템도 고속 프로세서를 채택한 하드웨어 장비에 탑재하여 고속화를 꾀하거나, 보안 ASIC(Application Specific Integrated Circuit) 칩 업체에서 개발한 IDS 칩을 장착하여 패킷 탐지율을 높이고 있다. 침입탐지시스템은 단독으로 설치 사용하기보다는 침입차단시스템이나 타 보안 시스템들과 연계해서 사용하여야 효과를 볼 수 있다. 이를 반영하듯이 많은 침입탐지 솔루션들이 침입차단시스템과 상호연동이 가능하다. 새로 개발되고 있는 차세대 침입탐지 솔루션들은 브리지 모드로 동작될 수 있으며 침입탐지와 차단 기능을 동시에 지원 가능하도록 개발되고 있다.

다. 안티 바이러스(Anti -Virus)

컴퓨터 바이러스는 초창기 감염된 파일이 다양한 경로를 거쳐 컴퓨터에 복사된 후 감염 파일의 실행으로 인해 다른 파일에 감염되거나 시스템을 손상시키는 형태로 존재했으나 네트워크의 확산과 기술의 발전으로 다른 해킹 수법들과 마찬가지로 많은 변화를 가져왔다.

컴퓨터 바이러스는 운영체제와 관계없이 네트워크를 통한 다운로드, 웹 다운, 응용 프로그램의 실행, 메일 전송 등의 다양한 수단을 통해 급속한 속도로 전세계의 컴퓨터 시스템을 마비시킬 수 있다. 대부분이 매크로 형태의 바이러스로 최근의 컴퓨터 바이러스는 웜과 트로이 목마의 기능을 복합한 복잡하고 지능적인 특징을 갖는 형태로 출현하고 있다. 또 무선 인터넷을 통한 형태의 바이러스 전파가 새롭게 나타나 많은 피해가 우려되고 있다. 메신저 프로그램을 통해 전파되거나, WAP 바이러스, 무선 단말기 자체에 상주하거나, 스스로 감염할 목표물을 찾아가는 스텔스 바이러스, 하드웨어에 들어가는 칩 내부에서 작동하는 바이러스 등 다양한 형태의 출현이 예상되고 있으며, 향후 무선 정보 단말기의 보급에 따라 가장 큰 보안 위협으로 떠오르게될 것으로 보인다.

안티 바이러스 제품은 주로 개인용 컴퓨터에 설치하게 되는 형태와 메일서버나 파일 서버에 두고 감염여부를 확인하는 형태, 그리고 최근 웜 바이러스의 출현으로 인해 게이트웨이용 제품을 개발하여 선보이고 있다. 최근 바이러스 백신업체들은 마케팅의 중심을 데스크톱 PC에서 기업 및 공공기관의 네트워크 안티바이러스 시장으로 옮겨가고 있다. 근래 들어 네트워크형 바이러스 출현이 잦아지면서 각 기업이 네트워크 바이러스 대응시스템 구축에 관심을 갖기 시작했으며, 몇몇 회사에서는 고속처리를 위한 하드웨어형 시스템을 출시하고 있다.

네트워크 차원의 대응 추세에 따라 바이러스 솔루션도 게이트웨이 형태로 네트워크에 설치 하여 모든 프로토콜을 대상으로 바이러스를 방어하는 형태로 연구 개발 되고 있으며, 무선 개인정보 기기들을 위한 PDA용 백신들도 잇달아 개발 출시되고 있다.

이외에도 최근 시만텍의 게이트웨이 시큐리티(Gateway Security)나 소닉월(SonicWALL)의 Internet Security Appliances, 시큐어소프트의 앱솔루트(Absolute)처럼 동일 플랫폼에 다양한 보안 제품들이 통합된 일체형 장비들도 선보이고 있다.

그리고, 침입탐지 기능을 방화벽에 내장하고, 실제 유해 패킷에 대해서는 내부 네트워크로의 유입을 차단하는 형태의 침입방지시스템(Intrusion Prevention System)들도 출시되고 있다.

2. 분석[3,4]

해킹 기술의 변화와 보안 패러다임의 변화에 따라 보안 시스템들도 많은 변화를 가져오고 있다.

먼저, 고속화 경향을 살펴 볼 수 있다. 기존의 소프트웨어 처리 방식으로 동작되는 보안시스템들은 네트워킹 장비들의 데이터 처리량을 감소시킬 뿐 아니라 각 네트워크의 병목 지점이 되고 있다. 이를 해결하기 위해 고성능의 전용 플랫폼[그림 4]이나 주요 기능의 하드웨어 구현으로 고속화를 꾀하고 있다[그림 5]. 그리고, 복합화의 경향을 띠고 있다. 기존의 단일 독립 기능 위주로 동작되는 보안 시스템들은 개별 보안 기능 제품에서 통합 보안 제품의 형태로 발전하고 있다[그림6].

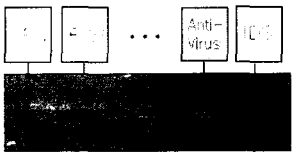

그림 4. 통합보안시스템

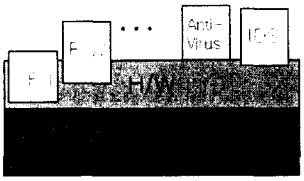

그림 5. 고속처리를 위한 하드웨어 구현

다음은 능동화이다. 기존 침입차단시스템과 침입탐지시스템, 바이러스 백신 등과 같은 단일 기능을 갖춘 독립적인 형태로 보안 시스템들이 개발되어 왔으며, 단순하게 주소위주의 차단 정책과 탐지후 보고라는 수동적인 형태의 기능을 갖고 관리자의 분석에 의한 사후 대응에 의존하고 있었다. 그러나, 갈수록 복잡해지고 변화되어 가는 악성 기법들을 차단하기 위해서 사전 차단이라는 능동적인 형태의 대응 기능을 갖춘 제품들이 나타나고 있다. 그리고, 지능화를 위한 여러 가지 연구가 진행되고 있다. 패턴 매칭의 단순기법에서 나타나는 오탐지를 줄이기 위해서 광범위하게 수집된 정보들을 바탕으로 사전 공격 예측과 정확한 탐지, 효과적인 대응 방안 수립을 위한 여러 가지 노력들이 진행되고 있다.

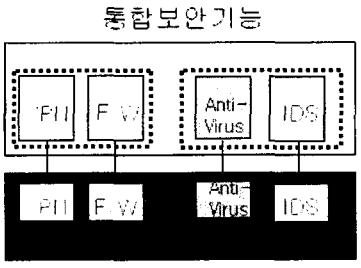

그림 6. 통합보안형태의 시스템

IV. 차세대 네트워크 환경에서의 네트워크 보안 시스템[4]

현행 보안 시스템들은 독립적인 단순 기능을 갖고 개별적으로 설치, 운영되고 있으며, 성능과 여러가지 제약들로 인해서 지역망 위주로 운영되고 있다. 그렇기 때문에 유해 패킷의 침입이나 바이러스 유포와 같은 행위들에 대해 원천적인 봉쇄가 불가능하다. 악의적인 사용자들의 공격 행위들이 근원적으로 탐지되기 전까지는 공중망에서의 활동이 전혀 제약을 받지 않게 된다. 따라서 지역망 위주의 방어에서 벗어나 사전에 침입이나 바이러스 웜과 같은 유해 패킷들을 차단하고 시스템들이 연계되어 단계별로 방어하기 위한 방안들이 필요하다.

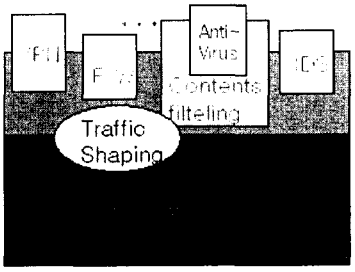

그림 7. 차세대 네트워크 보안 시스템

이를 수용하기 위해서는 다양한 기능들을 탑재하고 침입이나 사이버 공격에 대응해서 복합 처리가 가능한 고속의 하드웨어 기반 시스템이 요구된다[그림 7]. 고성능 스위칭을 기반으로 전용칩이나 하드웨어로 고속의 처리가 가능하고 침입탐지, 침입차단, 바이러스 차단, 컨텐츠 필터링, 가상 사설망 등의 다양한 기능들이 통합된 형태의 시스템 개발이 필요하다. DDoS나 트래픽 과다로 인한 대량의 패킷 유입시에 전체 네트워크가 마비되지 않기 위한 패킷 흐름 조절 기능도 필수적일 것으로 보인다.

V. 결 론

보안 기능들은 이제 네트워킹 장비에 탑재되어야 하는 필수 기능으로 자리잡아 가고 있다. 공격 대상과 해킹 기법들은 바뀌고 있으며 이에 대응하기 위한 방안들도 많은 변화를 가져오고 있다.

네트워크 보안 시스템들은 이러한 추세에 발맞추어 통합화, 복합화, 고속화 되어 가고 있으며, 차후로 지능화 되고, 능동화 되어 갈 것으로 전망되고 있다. 본 논문에서는 이러한 흐름에 발맞추어 차세대 네트워킹 환경에서 적용될 네트워크 보안 시스템에 관하여 고찰하여 보았다. 이러한 시스템은 가입자들의 네트워크로 유입되는 유해

한 트래픽들을 사전에 탐지, 차단하고 네트워크를 보호하기 유지하기 위해서는 일관된 관리 프레임 워크하에서 정보 교환과 공유를 통한 원할한 운영이 뒷받침이 되어야 할 것으로 보인다. 그리고 시스템에 필요한 고속화와 지능화를 위한 여러 가지 기술에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] 손지윤, 국가적 차원의 인터넷망 보호 체계 구축, KISA 정보보호뉴스 통권 66호, 2003. 4

[2] David Moore, The Spread of the Sapphire /Slammer Worm, http://www.caida.org/analysis/security/sapphire/, 2003. 1

[3] 정연서, 류걸우, 남택용, 손승원, 사이버 위협에 대한 보안솔루션 기술 동향, ETRI 주간기술동향, 1068호, 2002. 10

[4] 정연서, 장종수, 손승원, 네트워크 정보보호 시스템 발전 방향, Telecommunication Review, 제13권 2호, 2003. 4

[5] 이현우, 향후 인터넷 웜 발전방향 및 대응방안, http://www.securitymap.net/sdm/docs/virus/worm-in-the-future.doc, 2001. 11