차세대 네트워크 보안 서비스

김환국* · 정연서* · 서동일*

*한국전자통신연구원 네트워크보안연구부

Network Security Service for Next Generation Network Environment

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

*Dept. of Network Security Research, ETRI

E-mail : rinyfeel@etri.re.kr

요 약

최근 인터넷 사용자가 급증하면서 침해 사고 역시 크게 증가되고 있다. 이에 해킹과 침입으로부터 시스템과 네트워크를 보호하기 위해 정보보호 제품이 개발되고 있으나, 해킹 기법과 바이러스들도 점차 자동화, 지능화, 분산화, 대규모화, 은닉화 되어 가고 있다. 따라서, 이러한 위협에 대처하기 위해 종합적인 네트워크 보안 서비스가 필요하다. 본 논문에서는 역추적, 복구, 네트워크 취약성 분석, 공격 예측 등의 새로운 네트워크 보안서비스들과 이를 위한 고려사항들에 대해서 고찰한다.

ABSTRACT

Recently the number of internet users has very fast increased, and the number of intrusions has also increased very much. Hence, Security production developed to prevent systems and network from being hacked and intruded. However, hacking and virus getting on automation, intelligence, decentralization, large-scale and concealment. Therefore, Network security service necessary to deal with such threat. In this paper, we investigate about new network security services of trace-back, recovery, network vulnerability analysis, attack prediction and consideration for these services.

키워드

보안 서비스, 네트워크 보안, 통합보안관제, 해킹 대응

Ⅰ. 서 론

컴퓨터, 네트워킹 기술의 발전과 인터넷 문화의 보급으로 인해 지식 정보화 사회로의 이전이 급속화 되고 있다. 우리나라는 세계의 다른 나라들과 비교하여 손색이 없을 정도의 네트웍 기반 시설을 갖추었으며, 폭 넓은 사용자들이 있다. 인터넷은 수많은 정보의 공유와 사회 문화 경제 교류의 확대, 편리한 생활 제공 등으로 인해 삶의 질을 높여주고, 다방면에서 긍정적인 효과를 미치고 있으나, 개방적인 특성과 네트워크 프로토콜 (TCP/IP Protocol)의 근본적인 문제점 및 정보 시스템 자체의 취약성 등으로 인해서 악의적인 불법 침입에 의한 접근 정보의 오용 및 도청, 위조 및 변조 행위들이 쉽게 이루어 질 수 있다. 개인뿐만 아니라 기업과 정부의 정보 시스템 의존 비율이 확대됨에 따라 국가 기반 구조의 마비까지 생겨나는 사태가 우려되고 있다.

이를 방지하기 위한 많은 보안 장비들이 설치되어 있으며 이들 장비를 활용한 다양한 서비스들이 이루어지고 있다. 최근에는 아웃소싱의 개념이 들어간 MSS(Managed security service) 제공 업체들도 생겨났으며, 보안 점검과 대안 마련을 위한 보안 컨설팅 업체들도 있다.

본 논문에서는 Ⅱ장에서 인터넷의 발전 현황과 이에 따른 해킹 기법의 현황과 전망, 각국의 대응 상태에 대해서 조사 분석한다. 그리고, Ⅲ장에서는 기존 네트워크 보안 솔루션들과 네트워크 보안서비스의 현황에 대해서 분석한다. Ⅳ장에서는 역추적, 복구, 네트워크 취약성 분석, 공격 예측 등의 새로운 네트워크 보안서비스들과 이를 위한 고려사항들에 대해서 고찰한다.

Ⅱ. 해킹 기법 현황 및 전망

최근 발생하는 여러 해킹 사건에 사용되어지는 방법들은 지능화, 자동화, 대중화 되어가고 있으며,

특히 대규모화, 분산화, 은닉화 되어가는 경향을 보이고 있다. 또한 기존에는 서로 다른 영역으로 간주되어 왔던 바이러스 역시 해킹 영역에 포함되어지고 있으며, 해킹과 바이러스가 통합된 형태의 고도의 지능화된 해킹 프로그램들이 다수 발견되고 있는 실정이다[1].

가. 해킹기술과 바이러스 기술의 통합화

기존에는 서버에 침입하거나 악성 코드를 관리자 모르게 설치하여 자료를 삭제하거나 시스템을 훼손시키는 등의 기법들을 많이 사용하였다. 그러나 최근의 피해 현황에서 볼 수 있듯이 코드레드(Cordred), 님다(Nimda), 클레즈(Klez), 프레템(W32.Frethem.J@mm) 등 웜 바이러스에 의한 피해가 많이 나타나고 있다.

나. System Attack에서 Network/Service Attack으로 변모

해킹 기법 변화에서 알 수 있듯이 해당 특정 시스템을 침입하여 자료를 파괴하거나 획득하는 등의 시스템 공격에서 이제는 DoS나 DDoS, DRDoS 공격과 같이 트래픽을 대량으로 발생시켜 해당 서버나 라우터 등 네트워크 장비의 동작을 방해하거나 네트워크를 마비시킬 수 있어 특정 호스트를 목표로 하기 보다는 네트워크 인프라기반 자체에 대한 공격이 시도되고 있다.

다. Hacktivism 확산

해킹의 또 다른 변화는 개인적 단순한 목적에서 정치, 사회, 군사, 산업적 목적으로 변화되어 가고 있는 점이다. 핵티비즘이란 '해커(hacker)'와 행동주의를 뜻하는 '액티비즘(activism)'의 합성어로 급진적인 정치·사회적 목적을 달성하기 위한 컴퓨터 해킹을 말한다. 온라인 상에서는 10명의 인원만 있어도 해당 사이트를 마비 시키거나 해를 가할 수 있을 정도로 위력을 발휘할 수 있기 때문에 점차 소정의 목적을 위한 도구로 이용되는 사례가 늘고 있다.

라. Worm Attack

최근 웜과 해킹 기법이 결합된 형태가 나타나고 있다. 근래의 피해 사례를 보면 순위에 올라있는 대부분의 수법들이 웜 바이러스에 의한 피해가 주를 이루고 있다. 최근의 프레덤.E(Frethem.E), 시멀리.D(Simile.D) 뿐만 아니라 코드레드, 님다, 클레즈 등의 웜 바이러스들이 불특정 다수의 컴퓨터와 사용자들에게 피해를 입히고 있다. 님다와 코드레드 웜의 경우 웜 바이러스와 전통적인 해킹 방식이 결합되어 나타난 형태로 복제와 확산을 위해 다양한 방식과 기법이 사용됐다. 님다의 경우 여러 가지 감염 방식이 사용되었으며, 다수의 전자우편 전송자 처럼 움직이면서 취약한 웹사이트에서 복제를 수행했다. 그리고 감염된 웹사이트를 방문한 사용자들의 시스템에도 다운로드를 수행하였다. 감염된 해당 네트워크와 서버는 그 영향으로 마비되는 경우가 발생하여 업무에 막대한 지장을 초래하였다. 웜 바이러스 공격들의 또 다른 주요 특징은 급속한 전파속도로 피해를 입히게 되는데 2003년 1.25 인터넷 대란 알려져 있다.

마. Wireless Hacking 등장

최근 휴대폰 문자 메시지를 이용한 광고 발송으로 인한 프라이버시 침해가 늘어나고 있는 등 휴대폰과 PDA등 무선 기기들의 등장과 보급으로 인해 점차 무선 개인정보 단말기들에 대한 피해도 늘어날 전망이다. WPKI(무선 공개키기반구조)나 PDA용 무선 VPN(가상사설망) 솔루션 등의 다양한 솔루션들이 속속 개발되고 있지만, 아직까지 이러한 개인 정보 기기들을 위한 보안은 연구단계에 불과하여 많은 피해가 예상되고 있으며 계속해서 늘어날 것으로 보인다.

III. 네트워크 보안 서비스

위험을 사전에 방지하기 위해 대부분의 공공기관, 기업들이 네트워크를 위한 보안대책 마련방안의 하나로 설치되고 있는 대표적인 네트워크 보안 솔루션은 방화벽(firewall), IDS(Intrusion Detection System), VPN(Virtual Private Network), Anti-Virus 시스템, 생체 인식 시스템 등이 있다.

1. 국외 네트워크 보안 제품/서비스

다음 표 1은 미국 I3P(Institute for Information Infrastructure Protection) Report에서 정의하는 보안 서비스/도구 분류이다[2].

국내의 대표적인 정보보안 서비스로는 보안 컨설팅과 통합보안관제가 있다. 한국정보보안산업협회(KISIA)의 국내 정보보호시장현황에 따르면 일반적인 컨설팅, 인증, 관제서비스가 전체 서비스의 64.31%, 나머지는 정보보호 교육과 취약점 분석 등이 차지할 것으로 보았다.[3][4][5].

표 1. I3P 서비스/도구 분류

Audit and Post-Event Analysis	광범위한 행위의 재편성과 이러한 이벤트에 대한 책임을 확립하기 위한 목적으로 보안 관련 이벤트를 탐지하고 로깅하기 위한 메커니즘
Authorization/ Access Control	부여된 기준을 기반으로 사용자 또는 프로세스에 의한 행위를 허락(allowing)하거나 방지하는(preventing) 메커니즘
Boundary Protection	정보 리소스 집합들의 논리적 또는 물리적 경계를 정의하고 어느 한방향에서 경계를 지나 허가되지 않은 정보 교환을 막기 위한 메커니즘

Boundary Protection	정보 리소스 집합들의 논리적 또는 물리적 경계를 정의하고 어느 한방향에서 경계를 지나 허가되지 않은 정보 교환을 막기 위한 메커니즘
Cryptographic Controls	보안 정책 목적을 위한 암호 응용 기술로서 데이터 기밀성, 데이터 무결성, 책임추적성을 가진다. PKI 는 가장 대표적으로 구현된 암호기반 보안 시스템
Identification and Authentication	사용자, 프로세스, 디바이스 또는 소프트웨어 Instance의 유일한 식별자를 할당하는 메커니즘
Integrity Protection	변조되고 손상되지 않은 시스템, 리소스를 보장하기 위한 기술로 바이러스 탐지를 위한 기술과 시스템 소프트웨어의 무결성, 그리고 어플리케이션 레벨 혹은 프로토콜 레벨에서 전송되는 mobile 코드를 filter 하기 위한 메커니즘을 포함
Intrusion/ Anomaly Detection	보안 경계를 침해하기 위한 시도나 권한 보호, 정보 리소스 이용의 기대되지 않는 이용 패턴을 나타내는 이벤트를 탐지하는 메커니즘
Non-Repudiation and Related Controls	데이터에 대한 책임부여를 설정하기 위한 메커니즘으로 데이터가 포함된 행위에 대한 책임의 거부로부터 사용자, 프로세스, 디바이스의 보호를 제공
Secure Configuration Management and Assurance	정보 리소스 집합의 보안 상태에 대한 신뢰를 유지하고 평가하기 위한 메커니즘으로 식별, 인증, 감사, 무결성, 부인방지/신뢰 서비스가 있다.
Security Administration	보안관리자에게 시스템을 위한 보안 셋팅, 시스템 구성, 일반적으로 조직의 선정의된 보안 정책과 일관된 환경 내에서 시스템을 유지하기 위한 서비스
Secure Backup/ Recovery/ Reconstitution	파괴적이고 의심스러운 이벤트로부터 정보시스템의 복구를 제공하기 위한 메커니즘으로 백업의 예비 조치와 복구 등 사후 복구 조치를 포함하는 서비스

2. 국내 보안 서비스

(1) 인증 서비스

현재의 인증 서비스는 사용자 ID와 패스워드에 의한 사용자 인증 기술이 갖는 취약점을 보완하기 위해 인증서를 통해 클라이언트 및 서버의 인증을 수행하는 사용자 인증의 용도로 주로 사용되고 있다. 그러나 전자상거래가 일반화되고, 네트워크 거래가 보다 복잡하고 다양한 용도로 사용됨에 따라, 인증 서비스는 복잡한 기능을 수행 하는 신원, 내용, 신용인증이 있다.

(2) 통합 보안관제 서비스

통합 보안관제 서비스는 통합 관제 센터에서 고객의 정보통신 시스템에 대한 실시간 모니터링을 통하여 불법침입을 감시하고, 문제 상황에 대한 대응 및 재해 복구를 원격지에서 제공하는 서비스를 말하며, 또한 이를 확장하여 백업, 정보통신 시스템 취약점 점검, 오/남용 감시 서비스 등을 제공하기도 한다.

(3) 보안 컨설팅

보안 컨설팅이란 네트워크 및 전산장비에 대한 취약점 분석 및 대응책 제시를 하고, 보안정책을 수립하며, 교육을 통한 보안기술 이전으로 기업이 파괴, 유출, 변조로부터 자신의 정보자산에 대한 보안을 강화할 수 있도록 하는 서비스를 말한다.

IV. 차세대 네트워크 보안 서비스

보안서비스는 여러 가지 보안기술들을 복합적으로 적용하여 사용자에게 안전하고 신뢰할 수 있는 통신 환경을 제공하는데, 보안 서비스는 적용 범위와 대상에 따라 다양한 유형의 서비스가 창출 될 수 있으므로 서비스를 규정하기는 어렵다.

대표적인 보안서비스인 통합 보안관제 서비스는 서버, 네트워크 장비, 보안 시스템 등을 원격지에서 안전하게 종합 관리할 수 있어야 하며, 다양한 이기종의 보안 시스템을 하나로 묶을 수 있는 기능이 제공되어야 한다.

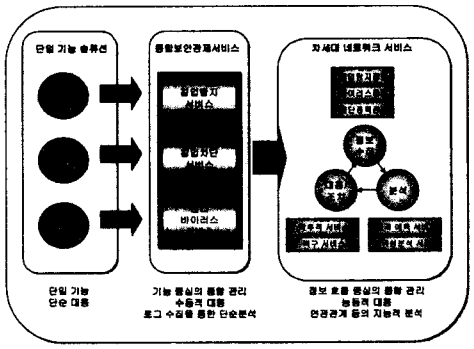

그림 1. 네트워크 보안 서비스 개념

현재까지의 보안 관제 서비스에서는 침입 차단 서비스, 침입 탐지 서비스, 안티바이러스 서비스가 대표적으로 제공되고 있다. 이러한 서비스는 단순 기능 위주의 서비스, 개별 호스트나 지역망 위주의 단편적이고 수동적인 대응에 머무르고 있다.

알려진 위협에 대해서 탐지하고, 대응하는 기존의 보안 시스템/서비스로는 여러 기법을 복합하여 개인 호스트나 주요 서버 뿐만 아니라 네트워크 장비와 네트워크 전체에 대해 공격을 가하는 형태의 위협에 효과적인 대응을 어렵게 한다[6].

따라서, 단순한 로그 수집, 지역적인 범주에 있는 보안 장비들의 통합/관리, 수동적인 대응에서 지능적, 전역적, 능동적인 대응을 위한 역추적, 자동복구, 공격예측, 네트워크 취약성 분석 서비스들이 네트워크 보안 서비스에 필요할 것이다.

(1) 역추적 서비스

일부 보안제품에서 역추적 서비스를 제공하고 있으나 Traceroute, whois 정보를 이용한 단순 서비스에 불과하다. 그러나 중간경유지를 우회하여 시되는 연결체인 형태의 공격에 대한 공격자의 실제 위치를 찾는 의미의 진정한 역추적이라 볼 수 없다. 따라서 TCP connection Traceback, IP Packet Traceback의 역추적 기술을 개발하여 공격자의 근원지를 자동화하여 찾아내는 역추적 서비스가 필요하다.

(2) 자동 복구 서비스

복구 서비스는 물리적인 장비를 비롯해 바이러스나 웜에 감염된 시스템과 프로그램을 복구하는 서비스를 나타내며 지금까지의 복구 서비스는 개별 호스트에 대해 수동적인 패치나 개별 복구가 대부분이다. 그러나 웜 바이러스 등 새로운 네트워크형 바이러스 형태의 공격에 신속하게 대응하기 위해서 이러한 개별적인 복구 차원에서 보다 자동화된 복구와 패치 서비스가 필요하다.

(3) 공격 예측 서비스

최근의 해킹기술이 웜과 바이러스의 통합화로 인한 웜 공격과 DoS 형태의 네트워크 공격이 주를 이루고 있다. 이러한 공격 형태는 네트워크의 자원을 마비 시키는 심각한 피해를 일으키므로 시간별, 날짜별 Traffic의 추이를 분석하여 DoS 형태의 Bandwidth Consumption 공격에 대해 분석 예측하는 서비스가 필요하다.

(4) 네트워크 취약성 분석 서비스

현재의 취약성 분석은 알려진 취약성에 대한 개별 호스트의 취약성을 보고하는 수준에 있으나, 전체 네트워크 관점에서 개별 호스트의 취약성들을 수집, 분석하여 취약 호스트지점을 분석하고 네트워크 상에서 해당 취약 지역에 의해 인근 네트워크로의 파급 등 전체 네트워크 단에서의 취약성 분석 서비스가 필요할 것이다.

V. 결 론

지금까지의 네트워크 보안 제품과 서비스는 주로 접근 제어 및 시스템 보안에 초점을 맞춘 것으로 최근까지 시스템 하나하나가 독단적으로 설치 운영되는 형태를 보여 왔다. 그러나, 최근 MS SQL 슬래머 웜 공격으로 인한 "1.25 인터넷 대란"에서 볼 수 있듯이 개별 보안 시스템의 설치가 분산서비스거부공격과 같은 DoS류 공격을 막기에는 한계를 드러내고 있다. 따라서, 분산적으로 시도되는 공격에 대응하기 위해서는 각종 보안 시스템들을 하나의 거대한 보안 구조(infrastructure)로 구성하여 설치 운영이 필요하며, 전체 네트워크의 안전성을 강화하고 보호하기 위한 관점과 단순 기능위주의 통합에서 자동화, 능동적인 네트워크 보안 서비스로 진행될 것이다.

본 논문에서는 이러한 요구사항에 맞는 능동적 대응, 자동화, 지능적인 네트워크 보안 서비스로서의 역추적 서비스, 복구 서비스, 공격 예측 서비스, 네트워크 취약성 분석 서비스의 필요성과 고려사항을 살펴보았다.

참고문헌

[1] 정연서, 류걸우, 남택용, 손승원, 사이버위협에 대한 보안 솔류션 기술 동향, ETRI 주간기술동향, 1068호, 2002.10.

[2] http://www.thei3p.org ,Survey of Products, Tools and Services, I3P Report, 2002.9.

[3] http://forum.kjist.ac.kr , 인터넷 보안 서비스, KISTI

[4] 김명은, 정연서, 남택용, 국내보안관제 서비스 기술 동향, ETRI 주간기술동향, 1045호, 2002.5

[5] 한국정보보호산업협회, 국내 정보보호 시장 현황과 전망(2002)

[6] 정연서, 장종수, 손승원, 네트워크 정보보호 시스템 발전 방향, Telecommunications Review 제13권 2호, 2003.4.