특 집

1.25 인터넷 침해사고의 분석과 대책

서 동 일*, 이 상 호**

*한국전자통신연구원, **충북대학교 컴퓨터과학과

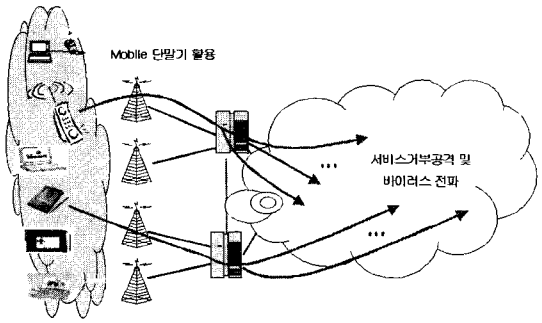
요 약

최근 정보화가 고도화되면서, 우리의 경제·사회 활동 기반구조는 인터넷과 같은 정보통신인프라에 절대적으로 의존하고 있어 사이버 안전이 확보되지 않은 정보사회는 어떤 재난보다 치명적인 위험에 직면할 가능성이 점점 더 커지고 있는 상황이다. 최근 발생되었던 1.25 인터넷 침해사고는 그러한 위험에 대한 극적인 실례를 보여준 것이라 할 것이다. 따라서, 본 기고문에서는 지난 1.25 인터넷 침해사고의 원인을 분석하여 보고, 향후 이러한 공격에 대한 대응 방안을 개인적 측면, 제도·정책적 측면, 기술적 측면에서 살펴보고자 한다.

I. 서 론

21세기 들어 정보화가 고도화되면서, 우리의 경제·사회 활동 기반구조는 인터넷과 같은 정보통신인프라에 절대적으로 의존하고 있어 사이버 안전이 확보되지 않은 정보사회는 어떤 재난보다 치명적인 위험에 직면할 가능성이 점점 더 커지고 있는 상황이다.

특히, 현재의 해킹·바이러스 기술의 추세를 살펴보면, 시스템 공격 일변도에서 점차 네트워크 인프라에 대한 공격으로 변화하고 있으며, 기존의 단위 기술에서 복합적이고 유기적으로 연동되는 통합기술로 발전되고 있음을 보여주고 있으며, 이는 치명적인 침해사고의 위험성에 그만큼 더 다가서고 있다는 실증이 되는 것이다. 이러한 공격의 예를 들어보면, 첫 번째 형태는 주소록을 통하여 대규모 트래픽을 발생시키는 경우로써, 웜 바이러스가 감염된 e-mail을 전송하여 수신측 마이크로소프트 아웃룩 주소록을 이용하여 e-mail을 재전송하는 형태의 공격 기술을 들 수 있다. 두 번째로는 응용 프로그램의 취약점을 통하여 전파되는 경우로써, 금번 인터넷 침해사고에서 사용된 SQL 슬래머 웜처럼 임의의 IP 주소를 생성하여 자신과 동일한 취약점을 가지고 있는 시스템을 네트워크에서 검색하여 감염·확산시키는 형태가 있다. 세 번째로, 〈그림 1〉처럼 최근에는 휴대폰과 같은 Mobile 기기를 통해 전파되는 경우로써, 기존의 고정된 시스템 위치에서 공격이 발생되지 않고, 공격 위치가 수시로 변화될 수 있는 형태 등이 있다. 최근 발생된 Mobile 바이러스로는, 2001년 8월, 일본 NTT 도코모의 휴대폰으로 바이러스가 유포되어, 다량의 긴급전화 110(국내 911)이 자동 호출되는 사



〈그림 1〉 Mobile 단말기를 활용한 공격

고로 국가의 기간 인프라가 일부 마비되는 사태가 발생하였던 것을 들 수 있다.

또한, 인터넷 기간망 시설인 DNS(Domain Name Service) 서버에 대한 공격을 통해 국내 주요 네트워크가 마비된 사례에서 처럼, 국내의 경우 ADSL 시스템에 대한 공격, 다음(Daum)과 같은 대규모 서버에 대한 공격, DHCP(Dynamic Host Configuration Protocol) 서버의 공격, 인증체계에 대한 공격 등이 시도된다면, 또다시 국내 주요 네트워크가 마비될 가능성이 매우 높으며, 금번 사고에서처럼 특수한 사용자만이 사용하고 있는 포트 번호가 아니라 일반 대중이 사용하고 있는 포트를 이용한 웜 해킹 공격이 시도 된다면 더욱 더 큰 혼란이 초래될 가능성이 매우 높은 게 국내의 현실이다.

미국의 경우에는 이러한 사이버 공격에 대응하기 위해서 올해 2월에 [5]번 참고문헌을 발표하였으며, 이 문서에서는 Homeland Security 전략과 사이버 공격을 예방하고, 취약점을 줄이며, 사후 피해를 최소화하기 위한 국가적인 우선순위와 실천 방안 등을 적시하고 있다. 이는 지난 클린턴 행정부가 공표한 주요 자산의 물리적 보호 전략 PDD(Presidential Decision Directives) 63의 후속 작업이라고 볼 수 있다. PDD63이 중요기간망인 농수산물, 수도, 전력, 공중의료, 비상체계 서비스, 뱅킹, 국방, 정보통신 등의 보호를 위한 각종 프로그램을 제안했다면, 이번 문서는 보다 구체적인 운영전략과 실천 방안을 수록하고 있다. 또한, 이 문서는 각 중앙정부, 지방정부, 사설기업과 조직 및 개인의 역할을 우선순위를 가지고 추진할 수 있도록 했고, 공공과 민간조직간 협력과 계약을 바탕으로 자국의 사이버 스페이스 전략에 공헌할 수 있도록 한 것이다.

본 기고문에서는 국내 사이버 스페이스의 안전성을 확보하기 위해, 지난 1.25 인터넷 침해사고의 원인을 분석하여 보고, 이러한 침해사고를 방지하기 위한 여러 가지 대응 방안들에 대해 논의해 보고자 한다.

제2장에서는 1.25 인터넷 침해사고의 주요 원인이 되었던 MS SQL 슬래머웜과 같은 악성코드 기술을 소개한다. 제3장에서는 1.25 인터넷 침해사고의 원인을 지난 2월에 발표된 정보통신부 자료를 중심으로 하여 분석한다. 제4장에서는 침해사고를 예방하고 대응하기 위한 주요 대책들을 논한다. 마지막으로 제5장에서는 간단한 결론과 추후 연구에 대해 이야기 한다.

II. 인터넷 웜 해킹 기술

최근 1.25 인터넷 침해사고를 기점으로 하여 악성코드의 일종인 인터넷 웜 해킹기술에 대한 관심이 부쩍 증대된 상태이다. 악성코드란 주로 다른 사람에게 피해를 주기위한 목적으로 제작된 모든 컴퓨터 프로그램을 의미하며[3], 여기에는 전통적인 컴퓨터 바이러스, 트로이 목마, 웜이 해당된다.

컴퓨터 바이러스란 감염 대상 프로그램 혹은 일반파일에 자신의 코드 및 변형코드를 감염시키며, 이로 인하여 컴퓨터 자원을 소모시키거나 데이터를 변형시키는 역할을 한다. 국내의 경우, 1988년경 처음으로 발견된 Brain virus가 있으며, 최근까지도 많은 피해를 주고 있는 CIH Virus, 미켈란젤로 바이러스 등이 있다.

트로이 목마의 경우, 일정한 조건 혹은 시점에 동작이 수행되는 프로그램을 의미하며, 대표적으로 감염된 대상 컴퓨터를 원격에서 제어할 수 있는 백오리피스 2000(Back Orifice 2000), 서브세븐(Sub7), 스쿨버스(School Bus), 넷버스(NetBus) 등이 있다.

웜(worm)이란 기억장소에 코드 형태로 존재하거나 혹은 실행 파일로 존재하며 작동시 파일이나 코드 자체가 네트워크를 통하여 다른 시스템으로 감염되는 악성 코드이다. 대표적으로는 1999년경 윈도우기반의 아웃룩 소프트웨어의 주소록을 통하여 급격히 확산되어 많은 피해를 입혔던 멜리사 웜이 있으며, 최근의 러브 바이러스, Nimda 바이러스, 코드레드 바이러스, 그리고 1.25 인터넷 침해사고의 원인으로 밝혀졌던 MS

SQL 슬래머 웜 등이 여기에 해당된다.

이외에도 다른 사람에게 거짓된 악성 정보를 유포하여 사용자에게 심리적인 위협이나 불안감을 조장하는 혹스(Hoax), 프로그램이 실행되면서 물리적인 피해는 없으나 사용자를 놀라게 하거나 심리적인 위협, 불안감을 심어주는 조크 프로그램 등이 악성코드라 할 수 있을 것이다.

Ⅲ. 침해사고의 원인 분석

1. 침해사고 현황 및 조치경과[4]

지난 1월의 인터넷 침해사고는 크게 두 번의 공격이 있었다. 첫 번째 공격은 슬래머 웜 해킹에 의해 국내 인터넷망이 마비되었던 1.25 인터넷 침해사고이며, 며칠 뒤에 멀티캐스트 트래픽 공격에 의해 네트워크 접속장애를 불러 일으킨 1.30 침해사고가 있었다. 이때의 침해사고 현황 및 조치 경과를 지난 2월에 발표된 정보통신부 정보통신망 침해사고 합동조사단의 조사결과 보고서인 [4]번 참고문헌을 통하여 알아보면 아래와 같다.

먼저, 1.25 인터넷 침해사고의 현황 및 조치경과를 알아보자.

- 1. 25일 14:10경 : 미국, 호주 등을 통해 국내로 슬래머웜이 유입된 것으로 추정되며, 드림라인에서 최초로 트래픽 이상 징후 발견
- 1. 25일 14:35~ : 국제회선 및 ISP(Internet Service Provider)의 주요 DNS(Domain Name Service) 서버, IDC 내부망 과부하 현상 발생
- 1. 25일 15:30 : 정보통신부, 장애현상 인지 및 긴급대책반 구성
- 1. 25일 16:00 : 한국정보보호진흥원(KISA), MS-SQL 관련 취약점을 이용한 공격으로 추정하고 각 ISP에 UDP 1433, 1434번 포트 차단을 권고하였으며, 각 ISP는 15:40~17:00 사이에 긴급조치를 실시하여 백본 라우터의 UDP 1433, 1434 포트를 차단
- 1. 25일 20:00 : 정통부와 KISA는 이번 장애의 원인을 "MS-SQL 슬래머웜"으로 확정하고, 메일링리스트(Sec-Info), 시큐어메신저, 홈페이지를 통해 대처방안 및 긴급경보를 발령(21:00)
- 1. 26일 14:30 : KT 및 하나로통신, 가입자 수용 라우터의 1433, 1434 포트차단
- 1. 26~27일 : KT, 구로 인터넷센터에 DNS 부하가 증가하여 DNS 수용구조를 지방으로 분산하고, 혜화 및 구로에 DNS 서버 17대를 증설(혜화 : 12→27, 구로 : 3→5)

며칠 후에 발생되었던 1.30 인터넷 침해사고의 현황 및 조치경과를 알아보자.

- 1. 30일 05시 40분경 : KT, 서울 구로 등 전국 11개 지역에서 ADSL 접속장애가 발생하였으며, 출발지가 255.255.255.255 : 80인 비정상적인 멀티캐스트 트래픽이 대량으로 유입되어 ADSL망의 L2 스위치에 장애발생
- 1. 30일 08:40 : KT, ADSL망의 L2 스위치에서 멀티캐스트 패킷을 처리하는 기능을 차단
- 1. 30일 09:30 : 하나로통신에서도 KT에서 발견된 것과 유사한 트래픽 (목적지가 255.255.255.255 : 80)이 다량 발생되어 라우터의 부하가 다소 증가하였으나 인터넷 장애에는 이르지 않음
- 1. 30일 18:00~21:00 : KT, ADSL망의 L2 스위치에서 문제가 되는 멀티캐스트 출발지 IP를 차단한 후 인터넷 서비스 접속지연 현상 해소
- 타 ISP는 1.30일 비정상적인 멀티캐스트 트래픽이 탐지되지 않았음(미국의 보안 전문사이트(securityfocus)에 따르면 국외에서도 출발지 주소가 255.255.255.255 : 80인 트래픽이 산발적으로 발견된 것으로 보고 되고 있어, 전세계적으로 이러한 이상 패킷이 발생한 것으로 추정)

2. 침해사고 원인 분석[2,4]

1) 슬래머 웜의 유입과 확산

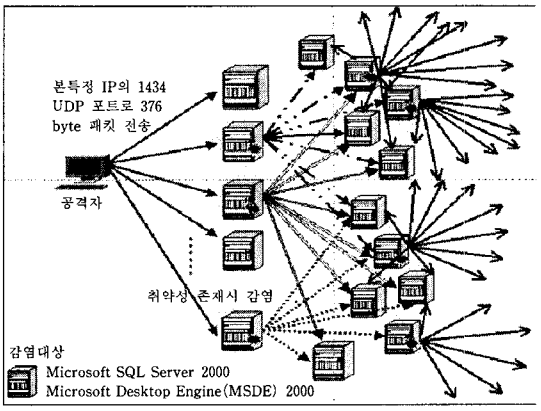
2003년 1월 25일 오후 해외로부터 유입된 슬

래머 웜은 초당 1만~5만개의 404 바이트 패킷을 대량 생성하여 뿌림으로써 네트워크 공격을 하는 악성 프로그램으로 국내에 8천 8백여 시스템을 급속히 감염시켰으며, 이로 인하여 전체 네트워크에 트래픽 폭주현상을 야기시켜 최종적으로 네트워크 전체의 마비 현상을 불러 일으킨 것으로 추정되고 있다.

이러한 슬래머 웜은 UDP(User Datagram protocol) 1434 포트를 통해 전파되는 404 바이트 크기의 메모리 상주형 웜으로서 2002. 7. 24일 공표된 "Microsoft SQL 서버 2000 및 MSDE (Microsoft SQL Server 2000 Desktop Engine) 2000 시스템의 버퍼오버플로우 취약점"을 이용하여 전파시키는 악성 웜 코드의 일종이다. 따라서, 방화벽에서 UDP 1434 포트를 차단한 경우에는 감염되지 않지만, 이러한 조치를 취하기 이전에 슬래머 웜은 UDP 특성을 이용해 확산되므로 그 속도가 매우 빠른 특징을 가지고 있다. 즉, TCP 에서는 세션(session)을 설정한 후 통신을 시작하지만, UDP 에서는 세션을 설정하지 않고 데이터를 상대 주소로 곧바로 전송하므로 상대방의 상황에 관계없이 패킷의 발송이 가능하므로 확산 속도가 매우 빠른 것이다.

금번 1.25 인터넷 침해사고의 경우, CAIDA (Cooperative Association for Internet Data Analysis)의 보고에 따르면 1월 25일 출현한 웜에 의해 전세계의 취약점이 존재하는 마이크로소프트 SQL 서버 2000의 90%가 10분 이내에 감염된 걸로 나타나고 있다. 국내에서는 전세계 감염 시스템(약 7만5천개)의 11.8%인 8천8백여

〈그림 2〉 슬래머 웜 확산 30분간 감염분포



〈그림 3〉 슬래머 웜의 확산 경로

개가 감염되어 일본의 약 7배, 중국의 약 2배에 달한 것으로 조사 되었다.

슬래머 웜이 작동하게 되면 감염된 서버의 성능 및 네트워크 환경에 따라 초당 약 1만~5만개의 UDP 패킷을 생성하여 랜덤한 IP 주소로 보내게 되며, 이로 인해 감염된 서버는 웜을 전파하기 위해 공격 패킷을 반복적으로 생성. 전송하므로 다른 일을 하지 못하는 과부하가 발생하여 결과적으로 서버에 대한 서비스거부(DoS, Denial of Service) 공격을 받은 것과 같은 결과를 초래하게 되는 것이다.

2) 인터넷 장애 분석

앞서 살펴본 슬래머 웜에 의해 국내 인터넷에 접속 장애가 발생된 과정을 살펴보면 다음과 같다. 먼저, 슬래머 웜은 취약점이 있는 윈도우 서버(Microsoft SQL서버 2000)를 감염시켜 감염 서버가 자동으로 불특정 다수의 다른 컴퓨터를 공격하여 네트워크 트래픽을 폭발적으로 증가시킴으로써 감염된 서버를 이용하는 대학, 연구소, 기업 등 이용자의 인터넷 접속경로를 차단하게 된다. 또한, 감염된 서버가 있는 인터넷 사이트인 경우 서비스 제공이 불가능하여 접속경로에 장애가 없는 이용자들도 인터넷 서비스를 이용할 수 없는 상황이 발생하게 된다. 특히, 정보통신시설이 집적되어 있는 IDC에서 LAN으로 연결되어 있는 서버중의 하나가 감염된 경우 내부망 트

래픽이 폭주하여 연결된 서버전체(포탈, 쇼핑몰, 게임 등)에 인터넷 접속장애가 발생하게 되는 것이다.

이렇게 감염된 서버로부터 발생한 공격패킷의 목적지 IP주소는 임의로 부여되는데, 국제 인터넷 주소할당 분포상 확률적으로 93.2%의 패킷은 국제관문국에 집중되므로 각 ISP의 국제관문국에서 심한 병목현상이 발생하여, 해외 인터넷 사이트 및 해외 Root DNS에 접속할 수 없었고, Root DNS 접속 재시도를 하는 과정에서 각 ISP들의 DNS에 과부하가 발생하여 국내 인터넷 마비 현상이 초래하게 된 것이다.

2003년 1월 현재 국제 IP 할당 현황을 살펴보면 〈표 1〉과 같다.

〈표 1〉 2003년 1월 국제 IP 할당 현황

구분	할당된 IP				다른 용도	미 할당
	미국	한국	중국	일본		
IP (천개)	1,240,314	26,208	29,396	95,166	605,552	1,857,257
비율 (%)	28.9	0.6	0.7	2.2	14.1	43.2

※ 전체 할당할 수 있는 IP 수 : 4,294,967(천개)
※ 다른용도 : 멀티캐스트용(268,435천개(6.2%)) 등

상기 〈표 1〉에서 볼 수 있듯이 확률적으로 약 93.2%(100−0.6−6.2=93.2)의 패킷이 국제관문국을 경유하여 해외 Root DNS로 향하게 되므로, 국내의 주요 국제 관문국 라우터에서 심각한 병목현상이 발생되었으며, 이로 인해 외국으로의 인터넷 접속 장애 및 국내 DNS 서버 과부하가 발생하게 된 것이다.

이처럼 슬래머 웜이 확산됨에 따라 네트워크에 트래픽 폭주현상이 발생하게 되었고, 대부분의 ISP 국제 회선에 장애가 발생함에 따라 일반 이용자가 해외 사이트로 접속하는데 지장이 발생하였으며, 또한 ISP내 DNS 서버와 해외 루트 DNS 서버간 교신 장애를 유발하여 ISP내 DNS 서버의 CPU 부하를 높이는 결과를 초래하게 되어 결국은 국내 주요 네트워크의 마비 현상이 발생하게 된 것이다.

그러나, 슬래머 웜에 감염되지 않은 서버는 지속적으로 서비스를 제공할 수 있었으며, 일부 이용자의 경우에는 접속시 일부 지연되는 상황은 발생되었으나 접속 자체가 차단되는 경우는 아니였음이 조사결과 나타나고 있다.

이 외에도 1.25 인터넷 침해사고에 대한 몇가지 다른 의견도 있으나, 본 기고문에서는 다루지 않을 것이다.

3. 1.25 인터넷 침해사고의 특징

금번 1.25 인터넷 침해사고에는 지금까지 볼 수 없었던 몇 가지 특징을 가지고 있다. 먼저, 일반 바이러스와 달리 이용자에게 직접 피해를 주는 것보다는 네트워크 자체의 트래픽을 증가시켜 인터넷 접속에 장애를 유발케 하였다는 점이다. 즉, 지금까지의 일반적인 인터넷 침해사고는 소규모 네트워크 마비 공격이나 특정 서버 시스템에 대한 해킹 혹은 바이러스 공격이 주를 이루었다면, 금번 1.25 인터넷 침해사고는 광역 네트워크 전체를 마비시키는 대규모 공격이였다는 점이다. 이는 국가 전시 상황과 같은 비상시에 사회 혼란을 야기 시킬 수 있는 매우 심각한 문제가 될 소지가 있는 것이다.

또한, 사이버 공격의 패러다임이 핵티비즘(Hacktivism)의 영향으로 인하여 개인적 만족 혹은 이익을 위한 공격에서 정치 사회적인 이슈를 중심으로 한 대규모 공격으로 바뀌어지고 있는 상황에서 그러한 공격으로 인한 극적인 효과가 어떤 방식으로 나타나는지를 보여 주었다는 점이다.

이외에도 금번 1.25 침해사고는 슬래머 웜 감염 피해자가 자신도 모르게 자동적으로 가해자가 되는 현상을 보여주고 있으며, 부분의 문제가 전체의 문제로 급속히 확산되는 상황에서 일부 조직의 힘만으로는 사이버 공격을 방어할 수 없으며, 모든 국가 기관, ISP 업체 등이 신속히 총체적으로 공조해야 할 필요성이 매우 높다는 사실을 보여주고 있다.

또다른 특징으로는 해외의 경우에 비해 국내의 피해가 특히 컸다는 점이다. 이에 따른 원인은 여러 가지가 있을 수 있으며, 첫 번째로는 외국에

〈표 2〉 슬래머 웜 감염 현황(출처 : CAIDA)

국가	한국	일본	중국	미국
감염시스템수 (전세계 감염서버 대비 비율)	8,848 (11.82%)	1,288 (1.72%)	4,708 (6.29%)	32,091 (42.87)

※ 슬래머웜 발생 후 30분간 전 세계적으로 약 75,000대 감염

비해 상대적으로 훨씬 더 많은 MS SQL 서버가 슬래머 웜에 감염되었다는 사실을 들 수 있다. 〈표 2〉의 CAIDA 자료에 따르면, 감염된 MS SQL 2000 서버의 수가 국내는 일본의 약 7배, 중국의 약 2배 많음을 보여주고 있다. 이는 우리나라 일반 이용자들의 매우 낮은 정보보호 의식도 한 몫 하였음을 무시할 수 없을 것이다. 심지어는 1.25 인터넷 침해사고 이후에도 보안 패치를 실시하여야 함에도 불구하고 이를 무시한 사용자들이 많았다는 사실이 이를 증명하고 있다[4].

국내의 피해가 컸던 두 번째 이유로는 Root DNS 서버 부재에 따라 국내 DNS 서버 과부하 현상이 외국에 비해 상대적으로 심각하였다는 사실도 있다. 이는 외국 사이트 접속뿐만 아니라 국내 인터넷 소통을 위해서도 국내 DNS 서버들이 Root DNS에 접속하여야 하나, 슬래머웜에 의해 국제관문국에 병목현상이 발생하여 Root DNS에 접속할 수 없어 국내외 인터넷 소통에 심각한 지장을 초래하게 된 것이다. Root DNS 서버는 미국 10개, 유럽 2개, 일본이 1개를 보유하고 있다.

세 번째로, 국내의 피해가 컸던 이유로는 잘 정비되어 있는 초고속 통신망을 통해 슬래머웜이 손쉽게 확산될 수 있었다는 점과 정보보호가 취약한 일부 IDC를 통해서도 급격히 슬래머웜이 확산되었다는 점도 있다. 또한, 우리나라의 경우에는 장애가 발생되었던 당시가 인터넷 사용이 많은 낮 시간이었던 반면, 유럽이나 미국 등은 주말 연휴가 시작되는 새벽시간대였고, 중국은 춘절 연휴기간이어서 인터넷 이용률이 저조하였다는 점도 영향을 미쳤던 걸로 추측할 수 있다[4].

Ⅳ. 인터넷 침해사고에 대한 대책

금번 1.25 인터넷 침해사고를 계기로 하여 국내의 네트워크 환경이 사이버 공격에 매우 취약하다는 사실이 전세계에 공지된 결과를 초래하였다. 이는 추후 정보전/사이버전이 발생할 경우에 매우 큰 위협이 될 것이다. 또한, 국내의 경우 인터넷을 통하여 사적·공적인 업무를 수행하면서 매우 중요한 정보들이 유통되고 있음을 감안하면, 향후 이와 같은 인터넷 침해사고시 어떻게 대처할 것인지를 알아보는 것은 매우 중차대한 문제일 것이다. 따라서, 본 장에서는 향후 국가적 차원에서 정보보호 수준을 획기적으로 향상 시킬 수 있는 방안을 크게 개인적 측면의 대책과 제도·정책적 측면, 기술적 측면에서 살펴보도록 한다.

1. 개인적 측면의 대책

개인적 측면의 대책에 있어서 가장 중요한 사항은 정보보호에 대한 인식 제고일 것이다. 즉, 인터넷 사용에 있어서 정보보호가 얼마나 중요한지를 국민 개개인이 인식하면서 실제 생활에서 이를 실천하는 것이 매우 중요하다.

이를 위하여 각종 보안 취약점에 대한 패치를 적정한 시기에 수행한다던지, 백신을 사용하면서 최신의 자료로 업데이트 하는 것을 소홀히 하지 않으며, 또한 불필요한 불법 복제와 같은 행위를 하지 않는 것을 생활화 하여야 할 것이다. 특히, 불법 복제를 통하여 악성코드에 감염될 위험성이 매우 높다는 사실을 적시하여야 할 것이다.

2. 제도적·정책적 측면의 대책

- 정보보호 인식 제고를 위한 정책적 활동 : 서버 관리자 및 일반 PC 사용자들에 대한 인식을 제고하여 보안 패치 작업이나 백신 업데이트 등의 정보보호 활동을 생활화 시킬 수 있는 정책적 측면의 활동이 필요하다.
- 정보보호 예산 투자의 확대 : 각급 국가 기관이 우선적으로 정보보호 예산을 일정부분 확보하

여 적극적으로 투자할 수 있도록 유도하여야 하며, 이를 일반 기업체로 확대할 수 있는 정책적 측면의 활동이 필요할 것이다.

◦ 루트 DNS 서버의 국내 유치 필요 : 최근 루트 DNS 서버를 국내에 설치하기로 결정되었으며, 이는 1.25 인터넷 침해 사고처럼 네트워크 트래픽 폭주 공격과 같은 경우에도 정상적인 인터넷 서비스를 제공하기 위한 필수적인 조치일 것이다.

◦ 인터넷 트래픽 관리를 통한 조기 예·경보 체계의 수립 및 구축 : 최근 한국정보보호진흥원(KISA)을 통하여 국내에도 조기에 이상 트래픽의 발생을 모니터링하여 이를 예·경보할 수 있는 시스템을 개발하고, 이를 활용하여 수분 이내로 인터넷 전체에 트래픽을 차단할 수 있는 조기대응체계 구축을 시작하였으며, 이러한 시스템에 의해 금번과 같은 대규모 네트워크 침해사고를 예방할 수 있을 것으로 기대된다.

◦ 제도의 개선 : 침해사고 발생시 IDC가 입주한 업체 등의 서버에 대해 이상트래픽 차단 등의 긴급조치를 할 수 있도록 하고, IDC 안전기준을 강화할 수 있는 제도적 측면의 개선도 필요하며, 침해사고관련 정보통신서비스제공자에 대한 로그자료의 제출요구권 및 현장조사권 등을 도입할 필요가 있을 것이다. 또한, 대규모 네트워크 구축시 정보보호 영향 평가제도 등을 도입하여 최초 설계·구축 단계에서 침해사고에 대응할 수 있는 체계를 구축하도록 하여야 할 것이다.

◦ 침해사고 대응 전문가의 양성 : 일반 정보보호 인력의 양성과 동시에 침해사고 발생시 긴급히 대응할 수 있는 전문가의 양성도 필요할 것이다.

◦ 정보보호기술 개발의 투자 확대 : 정보보호 기술은 그 특성상 국가적 자주권 확립을 위한 필수적인 기술이다. 또한, 이러한 기술은 단기적으로 확보하기 힘든 측면이 있으므로 국가적 차원에서 정보보호 기술 개발에 대한 장기적 개발 계획을 수립하고 이를 추진하여야 할 것이다.

3. 기술적 측면의 대책

향후 1.25 인터넷 침해사고와 같은 대규모적인 사이버 공격을 사전에 미리 예방하고, 공격시 즉각적인 탐지와 대응이 되기 위해서는 국가적인 차원에서 아래와 같은 여러 가지 기술들이 신속히 개발되어 운영될 수 있어야 할 것이다.

◦ 단기적인 운영기술의 향상 기술 : 현재 제공되고 있는 방화벽, 침입탐지시스템과 같은 각종 정보보호 제품들을 효율적으로 활용할 수 있는 운영기술을 확보하고 이를 전파하여야 한다.

◦ 실시간 트래픽 모니터링 기술 개발 : 트래픽의 이상 징후 및 변화추이를 신속히 감지하기 위한 인터넷 트래픽 실시간 모니터링 시스템 기술이 필요하며, 여기에는 실시간으로 트래픽을 선택적으로 감시하고 이상 트래픽을 감지 및 전파, 다양한 인터페이스에 대한 접속 기능들이 개발되어야 한다.

◦ 전체 네트워크 차원의 정보수집 및 분석을 위한 통합 보안관리 기술 : 네트워크 전체 차원의 경보정보를 종합적으로 수집하고, 신속한 조치를 유도하는 통합 보안관리 시스템 기술을 개발하여야 한다. 여기에는 네트워크 상황 종합 모니터링, 이상 징후 시 즉각적인 알람 발생 기능, 이상 징후 유형 분석 및 보안장비간 표준 연동 규격 및 프로토콜 지원 기능 등이 있어야 할 것이다.

◦ 네트워크 단에서 이상 및 유해 트래픽 차단 기술 : 폭주 및 유해 트래픽 발생 시 조기에 이를 감지하여 해당 트래픽을 자동적으로 삭제 혹은 차단하는 시스템 기술을 개발하여야 한다. 여기에는 정책기반의 패킷 제거 기술, 트래픽 량에 따른 단계별 패킷 제거 기능, 우선 순위에 따른 대역폭 제어 기능, Sink Hole 및 Black Hole 등 필터링 기능 등이 포함된다.

◦ 네트워크 차원에서 이용자를 보호하기 위한 취약점 점검 툴 개발 : 정기적인 취약점 점검을 실시하거나, 많이 사용되는 장비나 소프트웨어에 대한 취약점 점검, 해킹/바이러스에 대한 사전 경보가 가능한 점검 툴을 개발하여야 한다.

◦ 이용자 차원에서 정보자원을 자체 보호하는 기

술 : 인터넷 이용자 관점에서 자신의 PC, PDA 등의 정보자산을 스스로 보호하기 위한 기본적인 정보보호 기능을 갖는 시스템 기술이 필요하며, 여기에는 PC 방화벽 등 최소한의 정보보호 기능, 부가적인 정보보호기능의 추가 가능성 지원, 이용자 차원의 취약점 점검 툴 지원 등의 기술개발이 요구된다.

◦ 중기적으로 요구되는 기술의 개발 : 모든 액세스 망의 인입점에 보안장비를 설치 및 운용하고, 이들간 보안정보의 송수신을 통해 망을 통합적으로 관리할 수 있는 기술이 개발되어야 한다. 여기에는 침입에 대한 탐지·차단·대응 기능 등을 수행하는 액세스망용 고성능 네트워크 보안장비, 보안장비로부터 보안정보를 수집하고, 이를 토대로 보안정책을 수립·실행하는 통합보안관리 시스템 등이 포함된다.

◦ 장기적으로 요구되는 기술의 개발 : 코어 망의 인입점에 보안장비를 설치 및 운용하고, 이들간 보안정보의 송수신을 통해 망을 통합적으로 관리할 수 있는 기술이 필요하다. 여기에는 100 기가비트 이상의 네트워트 보안장비가 필수적으로 소요되며, 이들을 통합 관리할 수 있는 통합보안관리 시스템도 필요로 할 것이다.

◦ 신뢰 정보보호 기술의 개발 : 향후의 정보보호 발전 방향은 자율적인 보호, 자체 복원, 능동 대응과 같은 특징을 지닌 차세대 정보보호 기술이 필수적으로 요구될 것이며, 이를 위한 기술 개발이 장기적인 관점에서 시작되어야 할 것이다[1].

이외에도 미국 I3P(Institute for Information Infrastructure Protection)에서 2003년 1월에 발표한 2003년도 정보보호 기술개발 방향에는 아래와 같은 8가지 기술 항목을 추천하고 있다[6,7].

- Enterprise Security Management(ESM)
- Trust Among Distributed Autonomous Parties
- Discovery and Analysis of Security Properties and Vulnerabilities-Secure System and Network Response and Recovery-Traceback, Identification, and Forensics
- Wireless Security
- Metrics and Models
- Law, Policy, and Economic Issues

V. 결론 및 시사점

본 기고문에서는 최근의 1.25 인터넷 침해사고의 원인인 웜 해킹기술에 대해 알아 보았으며, 구체적인 사고원인, 금번 사고의 특징, 국내의 피해가 컸던 이유 등을 살펴 보았다. 또한, 이러한 침해사고를 사전에 예방하고 사고 발생시 신속히 탐지하고 대응하기 위한 개인적 측면의 대책, 제도·정책적 측면의 대책, 그리고 기술적 측면의 대책을 알아 보았다.

향후 이러한 국내 네트워크의 마비를 가져올 수 있는 인터넷 침해사고를 예방하기 위해서는 국가적 차원에서 정보보호 수준을 획기적으로 제고할 수 있는 정보보호 강화 대책이 수립되고 이를 추진해 나가야 될 것이다. 여기에는 루트 DNS를 국내에 유치한다거나, 인터넷의 트래픽 관리를 통한 조기 예·경보 체계를 확립하고, 관련된 기술을 개발하는 활동, 제도적 정비를 통한 침해사고 예방 및 대응활동 지원 체계 확립, 정보보호 관련 인력의 양성 등이 포함될 것이다. 또한, 장기적인 관점에서의 정보보호 기술 개발 계획을 수립하고 이를 꾸준히 추진해 나가는 것도 매우 중요한 문제이다.

이러한 노력 이외에도 일반 PC 사용자들에 대한 정보보호 인식을 제고시킬 수 있는 국가적 차원의 대책도 별도로 수립되어 시행되는 것과, 국민 개개인이 정보보호에 대한 인식을 새롭게 인지하는 것이 무엇보다도 중요할 것이다.

참 고 문 헌

〔1〕 서동일, 손승원, 이상호, "미래 정보전 대비 차세대 정보보호 기술 전망", 사이버테러 사이버코리아(사이버테러정보전학회지), pp. 58-67, 2003년 3월

〔2〕 정태명, "인터넷 침해사고의 원인과 대책", 정보처리학회지 제10권 2호, pp.22-26, 2003년 3월

〔3〕 정관진, 이희조, "인터넷 웜과 바이러스의 진화와 전망", 정보처리학회지 제10권 2호, pp. 27-37, 2003년 3월

〔4〕 정보통신부 정보통신망 침해사고 합동 조사단, "정보통신망 침해사고 조사 결과", 2003년 2월

〔5〕 미국 White House, "The National Strategy to Secure Cyber space", 2003년 2월, http://www.whitehouse.gov/pcipb

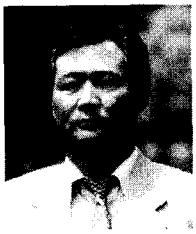
〔6〕 Dong-il Seo, H. S. Jo, S.W. Sohn and S.H. Lee, "Status & Trend of Information Security for Next Generation Network", PTR(Pacific Telecommunication Review), 4th Quarter 2002, Volume 24, Number 2, pp.9-17

〔7〕 I3P(Institute for Information Infrastructure Protection), "Cyber Security Research and Development Agenda", http://www.theI3P.org,2003년 1월

저 자 소 개

서 동 일

1998년 2월 : 경북대 전자공학과 졸업, 1994년 2월 : 포항공대 정보통신공학과 졸업, 2003년 2월 : 충북대 전자계산학과 박사과정 수료, 1989년 1월~1992년 2월 : 삼성전자(주) 종합연구소, 1994년 3월~현재 : 한국전자통신연구원 정보보호연구본부, 1994년 3월~현재 : ITU-T SG13 및 SG 17 표준 전문가 활동, 2001년 4월~현재 : ASTAP Forum 정보보호 전문가그룹 의장, 2001년 4월~현재 : 정보통신부지정 IT 국제 표준 전문가, 〈주관심 분야 : 인터넷 정보보호, 컴퓨터 통신, 네트워크〉



이 상 호

1976년 2월 숭실대학교 전자계산학과 졸업, 1981년 2월 숭실대학교 전자계산학과 석사, 1989년 2월 숭실대학교 전자계산학과 박사, 1981년~현재 : 충북대학교 컴퓨터과학과 교수, 〈주관심 분야 : 네트워크 보안, 망관리, 프로토콜〉