제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

인터넷 웜 확산방지 시스템의 설계 및 구현

최 양 서*, 서 동 일*
* 한국전자통신연구원 네트워크보안구조연구팀

요 약

급속도로 발전한 인터넷으로 인해 새로운 사이버 세상이 실현되었으나, 인터넷의 발전으로 인한 각종 침해사고 역시 크게 증가하고 있다. 과거에는 다양한 형태의 침해 사건들이 발생하더라도 피해 범위가 국지적이었다. 그러나, 최근에는 그 피해 범위가 광범위해 지고 있다. 특히, 지난 2003년에 발생한 1.25 인터넷 대란으로 인해 전국의 인터넷 망이 마비되었다. 이는 바이러스와 해킹의 기술이 통합되어 윈도우 시스템의 취약점을 이용해 자동화된 복제 및 확산을 수행함으로써 발생한 결과였다. 이와 같이, 최근 빈번하게 발생하는 각종 인터넷 웜은 주로 개인용 PC에 설치된 MS-Window 운영체제를 주 공격 대상으로 하고 있다. 즉, 개인용 PC의 문제로 인해 인터넷 전체가 마비될 수 있는 문제가 1.25 인터넷 대란을 통해 발견된 것이다. 이에, 본 논문에서는 개인용 PC에 설치하여 다양한 형태의 인터넷 웜이 더 이상 확산되지 않도록 하는 "인터넷 웜 확산 방지 시스템"을 설계하고 구현한 결과를 논의하도록 한다.

Design and Implementation of Internet Worm Spreading Prevention System

Yang Seo Choi, Seo Dong Il*

ABSTRACT

The new cyber world has created by Internet that is prosperous rapidly. But with the expansion of Internet the hacking and intrusion are also increased very much. Actually there were many incidents in Internet, but the damage was restricted within a local area and local system. However, the Great 1.25 Internet Disturbance has paralyzed the national wide Internet environment. It because the Slammer Worm. The worm is a malformed program that uses both of the hacking and computer virus techniques. It autonomously attacks the vulnerability of Windows system, duplicates and spreads by itself. Jus like the Slammer Worm, almost every worms attack the vulnerability of Windows systems that installed in personal PC. Therefore, the vulnerability in personal PC could destroy the whole Internet world. So, in this paper we propose a Internet Worm Expanding Prevention System that could be installed in personal PC to prevent from expanding the Internet Worm. And we will introduce the results of developed system.

1. 서 론

2003년 1월 25일, 한국의 인터넷 망이 하루아침에 기능을 상실하는 사건이 발생 했다. '인터넷 대란'이 일어난 것이다. 인터넷 대란은, 2003년 1월 25일 오후 2시경부터 마이크로소프트사의 SQL 서버의 보안 취약점을 이용한 슬래머 웜이 국내로 유입되면서 시작 되었다. 그로부터 전국의 인터넷 망은 최소 9시간부터 최장 2-3일간 마비되었다. 이로 인해 최소한 수백 억 원의 경제적인 피해를 입은 것으로 보고 되고 있다[1]. 경제적 피해 외에도, 인터넷이 마비되면서 많은 공적, 사적 생활을 영위할 수 없게 되어 그로 인한 사회적 충격 역시 컸으며 한국이 세계 최고의 바이러스 피해국이라는 오명을 얻게 됐다. '1.25인터넷 대란'후에도 블래스터, 소빅, 웰치아, 마이둠과 같은 웜 바이러스들이 끊임없이 인터넷으로 유입되어 그 피해는 날로 커 저만 가는 상황이다.

이에 인터넷대란을 계기로 한국 정보화 사회에 대해서 깊은 반성과 성찰이 필요하다는 주장이 강하게 제기되었다. 이것은 정보화 사회로 사회가 재조직되고 있는데, 그 하부 구조라 할 인터넷의 안전을 신뢰할 수 없는 것이 아니냐는 회의와도 연결되어 있다. 게다가 지난 인터넷대란을 야기한 '슬래머 웜'이 한국만을 공격한 것이 아니라 전 세계를 대상으로 한 것임에도, 유독 한국만이 전국적인 인터넷 마비를 겪었다는 점에서 한국의 정보화가 초고속통신망을 설치하고 정보통신기술 연구개발에만 치중하면서 성장위주의 정책을 추구해왔을 뿐, 정보화 사회의 안정적 운영을 위해서 필요한 보안문제를 외면하고는 있지 않나 생각 하게 된다.

이에 본 논문에서는 인터넷을 통하여 발생하고 있는 웜 바이러스의 확산을 막고 인가되지 않은 네트워크 사용을 차단하여 이로 이해 발생하는 경제, 사회적인 피해를 최소화 하기위한 "인터넷 웜 확산 방지 도구"를 제안한다.

2. 인터넷 웜의 특성

인터넷 웜은 해킹과 바이러스의 기술이 통합된 형태의 기술로서 지난 1988년 솔라리스의 finger데몬의 취약점을 이용한 모리스 웜이 최초의 웜이었다[2]. 당시에도 큰 사회적 문제를 일으켰으나, 그 공격 대상이 한정적이었기 때문에 피해는 크지 않았다. 그러나, 최근 발생하고 있는 인터넷 웜은 개인용 PC를 대상으로 확산 전파하기 때문에 그 전파력은 가히 상상할 수 없을 정도이다. 인터넷 웜은 그림 1과 같은 공격 패턴을 갖는다.

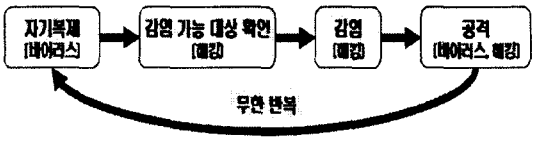


그림 1 인터넷 웜 공격 패턴

즉, 바이러스 유포가 시작되면, 공격 가능한 대상을 찾아내어 감염을 시키고 지속적으로 자기 복제를 해나감으로써 빠르게 확산해 나가는 것이다. 여기서 취약점을 가지고 있는 시스템을 찾아내고 실제 공격을 수행하는 것은 해킹의 특성이며, 시스템 파괴 등과 같은 공격과 자기 복제는 바이러스의 특성이다. 그림 2는 지난 1.25 대란의 주범인 슬래머 웜이 발생하고 30분 후의 감염지역의 분포를 나타낸 것이다.

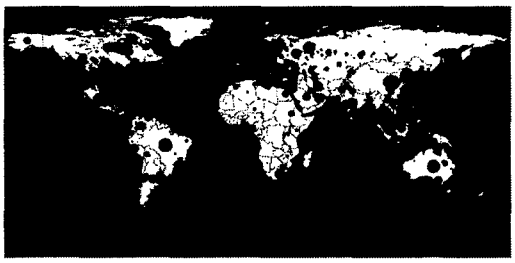


그림 2 슬래머웜 발생 30분 후 감염지역

인터넷 웜은 일반적으로 다음과 같은 3가지 방법을 통해 확산된다.

- E-mail을 통한 확산

최초 E-mail에 첨부된 형태로 전송이 이루어지고 수신자가 첨부파일을 실행 혹은 읽는 동작만으로 감염되는 방식으로, 감염 후 등록된 E-mail 리스트를 기반으로 또 다시 확산을 시도. SMTP 트래픽이 현저하게 증가하는 것이 특징이다[3].

- 윈도우 OS의 공유 자원을 통한 확산

NBT(NetBIOS over TCP/IP)를 이용하여 관리자 패스워드가 설치되지 않은 공유폴더에 접근하고 자신을 복제하는 방식으로, NBT 포트(137, 138, 139, 445)에 대한 트래픽이 증가하며 네트워크의 성능을 저하시키는 것이 특징이다.

- 윈도우 OS의 보안적 결함을 통한 확산

Buffer Overflow와 같은 보안 취약점을 이용하여 전파되는 방식으로, 상당수의 웜 바이러스가 채택하고 있는 방식이며 네트워크에 치명적인 문제를 야기 시킨다. 대상 호스트를 찾기 위한 ICMP 패킷이나 스캔 패킷이 증가하며 단 하나의 호스트가 전체 시스템에 영향을 줄 수도 있으며, 경우에 따라서 DDoS 공격의 Agent로써 동작한다[7].

3. 인터넷 웜 확산방지 시스템

1. 시스템 구성

본 인터넷 웜 확산방지 시스템은 운영체제의 커널과 응용 프로그램 사이에서 네트워크 패킷을 감지하여 다양한 기법을 통해 웜 확산을 방지하게 된다.

즉, 커널모드에서 유저모드로 혹은 유저모드에서 커널모드로의 전환시 필터링 드라이버를 경유하게 되고 필터링 드라이버 내부에서 사용자의 정책에 따라 제어가 가능하도록 개발되었다.

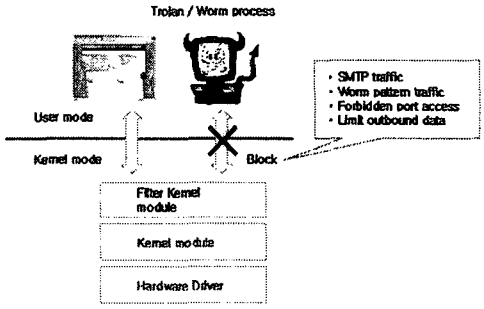


그림 3 웜 확산방지 시스템 구성도

2. 시스템 기능

본 인터넷 웜 확산방지 시스템은 다음과 같은 기능을 포함하고 있다.

- 프로세스 단위의 인터넷 접근 감시 및 제어
  . 응용 프로그램의 인터넷 접근 제한 기능
  . 허용된 프로세스의 무결성을 확인 기능

- 인터넷접근 허용 프로세스에 대한 정책적용
  . Outbound 트래픽의 양 제한 기능
  . 한 프로세스의 동시 접속 세션 제한 기능
  . 특정 포트의 외부 개방을 제한하는 기능

- 특정 포트에 대한 Outbound 트래픽 차단
  . 접근 가능한 외부 포트의 제한

- 패턴에 근거한 Outbound 트래픽 차단
  . 특정 패턴의 외부 전송차단 기능

- SMTP를 이용한 E-mail 발송 제한
  . E-mail 발송 가능 프로세스 지정 기능

이와 같은 기능들은 인터넷 웜이 확산을 위해 사용하는 방법을 차단하는 방법으로 동시에 같은 특징을 갖는 세션이 다수 발생하는 것을 방

지하는데 초점을 맞춘 것이다.

3. 구현 결과

앞서 설명한 기능을 포함하는 인터넷 웜 확산 방지 시스템의 구현을 통해 인터넷 웜에 감염된 시스템이 웜 확산을 하지 못하게 됨을 확인하였다. 그림 4에서 보면 인터넷 접근이 차단된 프로세스를 볼 수 있다.

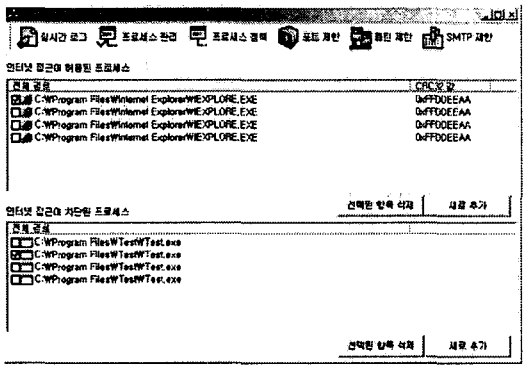


그림 4 인터넷 웜 확산방지 시스템

4. 결론

인터넷의 발전으로 인해 새로운 사이버 세상이 발현되었으나, 이와 함께 그 역기능 또한 크게 증가하고 있다. 다양한 역기능 중 해킹과 바이러스 기술이 통합된 인터넷 웜은 빠른 확산으로 인해 인터넷 전체가 마비되는 등의 큰 문제를 야기 시키고 있다. 이에 본 논문에서는 이와 같은 인터넷 웜의 확산을 방지하고자 개발한 "인터넷 웜 확산 방지 시스템"의 구성과 구현 결과에 대해 논의하였다.

본 개발 결과를 통해 네트워크를 통해 유포되는 웜 바이러스의 활동 무대인 개인 PC를 웜 확산으로부터 원천 봉쇄함으로서 보다 안전한 인터넷 환경을 기대할 수 있을 것으로 예상되며, 또한 내부 사용자 개인의 정보 보호와 개인 PC 자원의 남용을 방지할 수 있을 것으로 예상된다.

참고문헌

[1] 정관진, 이희조, "인터넷 웜과 바이러스의 진화와 전망", 정보처리학회지, 10권 2호, 27-37쪽, 한국정보처리학회, 2003

[2] Zesheng Chen, Lixin Gao and Kevin Kwiat, "Modeling the spread of Active Worms," Proc. of IEEE INFOCOM, 2003 .

[3] Nicholas Weaver, "A Brief History of The worm," Nov. 1997,

[4] David Moore, Colleen Shannon, Jeff Brown, "Code-Red: a case study on the spread and victims of an internet worm," Proc. of SIGCOMM IMW 2002, Nov. 2002 .

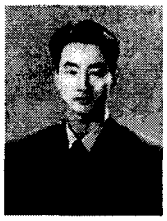
[5] Ahnlab, Inc, "Win32/Nimda, " sep. 2001.

[7] CAIDA, "Analysis of the Sapphire worm, " Jan. 2003.

[8] Stuart Staniford, Vern Paxson and Nicholas Weaver, "How to Own the Internet in Your Spare Time, " USENIX security Symposium, Aug. 2002 .

[9] Jose Nazario, with Jeremy Anderson, Rick wash and Chris Connelly, "The Future of Internet Worms " . Crimelabs research, July 20, 2001.

최 양 서



1996년 : 강원대학교 전자계산학과 이학사

2000년 : 서강대학교 컴퓨터공학과 공학석사

2000. 6.~현재 한국전자통신연구원 네트워크보안구조연구팀 연구원

서 동 일

1989년 : 경북대학교 전자공학과 공학사

제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

1994년 : 포항공과대학교 정보통신학과 공학석사
2002년 : 충북대학교 전자계산학과 (박사과정 수료)
1989. 1.~1992. 2. : 삼성전자종합연구소
1994. 3.~현재 한국전자통신연구원 네트워크보안구조연구팀장