특

Secure OS 기반의 지능형 다단계 정보보호시스템

홍기융[1] 은유진[2] 김재명[3] 이규호[4]

목 차

- 요 약 -

본 고에서는 1.25 인터넷 대란과 같은 버퍼오버플로우를 이용해 침투하는 인터넷 웜 및 DOS (Denial of Service) 공격을 Secure OS(보안운영체제), IDS(Intrusion Detection System : 침입탐지시스템), Scanner(취약성진단도구), Firewall(침입차단시스템)의 지능형 상호연동 스킴을 이용해, 근본적인 대응이 가능한 지능형 다단계 정보보호체계를 제시하였다. 본 고에서 제시한 정보보호대응책은 고도로 지능화하고 있는 인터넷 웜 및 DoS(Denial of Service : 서비스거부)공격을 미연에 예방하고, 실시간으로 대응할 수 있는 시스템이 될 것이다.

1. 서 론

2003년 1월에 발생한 국내 사상 초유의 인터넷 마비 사건은 Slammer/Sapphire (국내엔 Slammer로 알려져 있으나, 국외에는 Sapphire로도 알려져 있음)로 알려진 인터넷 웜이 MS-SQL 서버 Resolution Service의 버퍼오버런 취약성을 이용해 전파되면서 네트워크 트래픽의 급격한 증가를 유발시키며 DDoS(Distributed Denial of Service:분산서비스거부) 공격을 일으킨 것으로 알려져 있다.

위의 DDoS 공격 형태를 좀 더 유심히 살펴보면 기존의 DDoS 공격과는 다른 특징을 발견할 수 있다. 기존 DDoS 공격은 일종의 공격도구인 에이전트를 설치해 공격을 수행하나 이번 사건의 경우 정상적인 서비스인 Windows 시스템의 DNS lookup 과정이 마치 DDoS의 에이전트가 공격하는 것과 같은 역할을 수행했다는 것이다.

이와 같은 공격 형태는 2002년 1월 미국에서 처음 발견된 DRDoS와 유사한 형태로 DRDoS 공격은 별도의 에이전트 없이 네트워크 통신 프로토콜 구조의 취약성을 이용해 정상적인 서비스를 운영하고 있는 시스템을 DDoS 공격의 에이전트와 유사하게 사용할 수 있다. 이는 기존 DDoS 공격에 비해 악의적인 사용자들이 사용하기 쉽고, 공격 당한 사이트는 그 원인을 쉽게 밝혀내기 어렵다는 점에서 그 심각성이 높다고 할 수 있다[1].

1) (주)시큐브/(주)케이사인 대표이사
2) (주)시큐브 부사장
3) (주)시큐브 상무이사
4) (주)시큐브 보안취약성도구 개발팀장

2. 기존 보안 솔루션의 한계

2.1공격방법의 변화

2.1.1 기존 공격 형태

기존 DoS, DDoS 공격의 가장 큰 특징은 특정 시스템의 서비스거부를 일으키기 위해서는 대량의 에이전트 역할을 수행하는 객체가 필요했다는 점이다. 따라서 대량의 에이전트를 확보하기 위해 해커는 운영체제 및 응용프로그램의 알려진 취약성을 이용해 해당 시스템에 접근하여, 에이전트를 직접 설치 하거나, 바이러스, 웜 및 악성코드를 이용하여 운영체제 및 응용프로그램의 알려진 취약성을 통해 자동으로 전파되도록 하는 방법을 사용하였다.

그러나, 이러한 방법은 특정 에이전트를 이용해야만 하고, 에이전트의 이용을 위해서는 에이전트를 제어해야만 한다. 이러한 부분에서 통신 트래픽 상에 에이전트 제어를 위한 패킷 혹은 공격의 특성을 나타내는 패킷들이 노출되어 이를 이용한 탐지 및 방어가 가능하도록 하였다.

과거 DoS, DDoS로 알려졌던 공격들은 아래 표와 같다[2].

〈표 1〉 기존 DoS, DDoS 공격 예

순위	공 격 이 름
1	FUNLOVE.4099
2	KLEZ.H
3	NOCLOSE.E
4	NIMDA.E
5	ELKERN.D
6	SOBIG.A
7	YAHA.K
8	IFRMEXP.GEN
9	YAHA.G
10	CODE RED

2.1.2 새로운 공격 형태

이에 반에 새로운 공격은 DRDoS 형태를 취하는 방법으로 특정 시스템에 대한 서비스거부공격을 위해 중간 매개체인 에이전트 역할을 수행하는 객체뿐만 아니라, 인터넷 환경의 일반적인 시스템 및 서비스를 객체로 활용한다.

따라서, 공격자는 중간 매개체인 에이전트 확보를 위해 바이러스, 웜 및 악성코드를 이용할 뿐 아니라, 인터넷 환경에서 정상적으로 이용할 수 있는 시스템 및 서비스(예 : DNS, WEB, FTP, Telnet 등)를 에이전트로 이용한다.

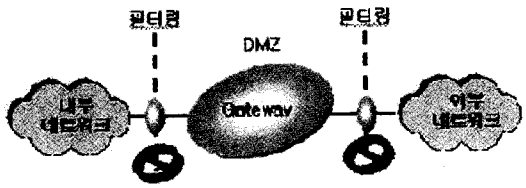
공격행태가 특정 에이전트를 이용하기도 하고, 또한 정상적인 인터넷 서비스를 이용하기도 하므로 통신 트래픽 상에 공격을 나타내는 일부 정보가 노출되기도 하나, 정상적인 트래픽으로 위장이 가능하다.

새롭게 출현한 공격으로는 Slammer와 SYN/ACK DRDoS [1] 등이 있다.

2.2 기존 보안 솔루션의 한계

2.2.1 침입차단시스템

침입차단시스템은 아래 그림과 같이 내부 네트워크와 외부 네트워크 사이의 모든 트래픽이 통과하는 곳에 위치하여, 보안관리자에 의해 정의되고 허가된 패킷만 통과하도록 하는 것을 기본 기능으로 한다.



(그림 1) 침입차단시스템 기본동작원리

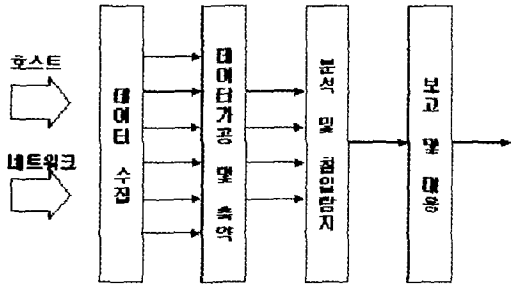
침입차단시스템은 위와 같은 기본 기능을 가지고 있기 때문에, 근본적으로 허가된 서비스의 취

약성을 이용한 공격과 내부자에 의한 공격에 취약하다.

특히 이 중 허가된 서비스의 취약성을 이용하는 경우가 DRDoS의 특성에 취약하다 할 수 있다. DRDoS는 정상적으로 운영되고 있는 인터넷 서비스를 중간매개체로 사용하는 특성을 가지고 있으므로 침입차단시스템 단독으로 이러한 공격에 적절히 대응할 수 없는 한계점을 가지고 있다.

2.2.2 침입탐지시스템

침입탐지시스템의 경우 아래 그림과 같은 기술적인 구성요소를 가지고 있다.



(그림 2) 침입탐지시스템 기술적 구성요소

호스트 또는 네트워크에서 감사 데이터를 수집하여 이를 가공 및 축약한 후 침입 여부를 분석 및 탐지하고 이에 대한 보고 및 대응을 수행한다.

S. Kumar와 COAST의 분류에 따르면[3][4], 데이터 수집 과정에서 호스트에서 감사 데이터를 수집하는 경우를 호스트 기반 침입탐지 시스템이라 하고, 네트워크 패킷을 감사 데이터로 수집하는 경우를 네트워크 기반 침입탐지 시스템이라 한다.

또한 침입 여부를 분석 및 탐지하는 과정에서 기존에 존재하는 악의적인 침입 패턴을 가지고 이와 일치하는 패턴일 경우 침입으로 판단하는 경우를 오용탐지 기반 침입탐지시스템이라 하고, 정상적인 행위에 대한 프로파일을 만들고, 이에서 벗어나는 경우를 침입으로 판단하는 경우를 비정상 행위탐지 기반 침입탐지시스템이라 한다.

그러나, 비정상행위기반 침입탐지시스템은 실제 네트워크 및 시스템에 적용하기 어려움이 많아 실제 상용으로 개발되어 있는 시스템은 호스트 혹은 네트워크 기반 오용탐지 침입탐지시스템이다.

따라서, 침입탐지시스템은 기존에 발생한 침입탐지패턴의 소유 여부에 따라 침입탐지 가능 여부가 결정된다고 볼 수 있다.

그러나 DRDoS의 경우, 정상적인 서비스를 이용해 공격하는 특성이 있으며, 특정 에이전트를 이용해 공격하는 경우도, 침입탐지시스템의 침입패턴 데이터베이스에 있지 않은 새로운 공격일 경우 탐지할 수 없는 한계점이 있다.

3. Secure OS기반의 지능형 다단계 정보보호시스템

3.1 시스템 개요

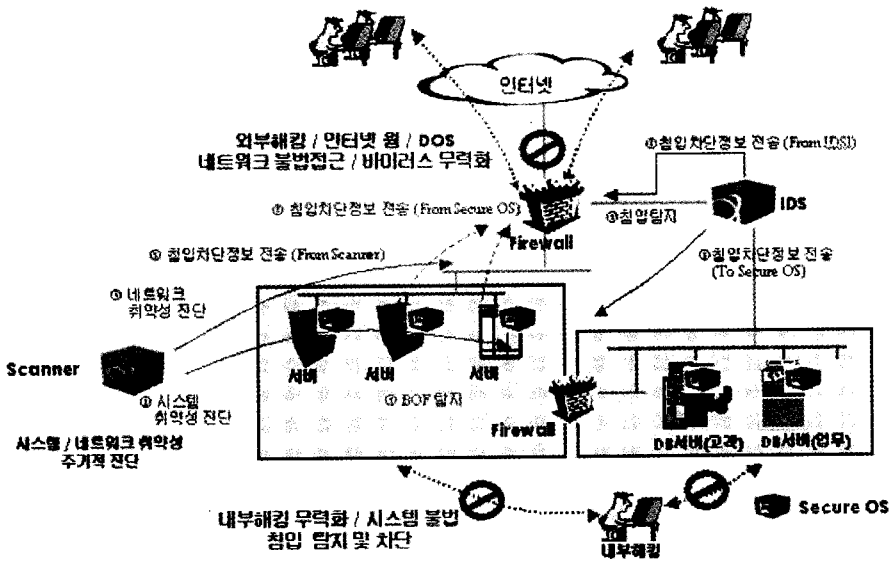
이제까지 살펴본 바와 같이 기존 보안 시스템들은 각자 독자적인 보안 기능은 충실히 수행하지만, 각자의 한계를 가지고 있어, 웜 바이러스/DRDoS 공격에는 적절히 대응할 수 없는 한계를 가지고 있다. 따라서 본 고에서는 Secure OS, 침입탐지시스템(IDS), 침입차단시스템(Firewall), 취약성진단도구(Scanner) 등을 이용해 이들 보안 솔루션 간의 상호 연동 및 보완을 통하여 이러한 한계를 극복할 수 있는 지능형 다단계 정보보호시스템을 제안한다.

3.2 시스템 구성 요소 및 기능

Secure OS를 이용한 다단계 지능형 보안 시스템의 전체 구성은 다음 (그림 3)과 같다.

3.2.1 Secure OS

Secure OS는 전체 시스템에서 다음과 같은 기능을 수행한다.



(그림 3) 지능형 다단계 정보보호체계

- 시스템 커널레벨 접근제어
- 알려지지 않은 BOF 공격 탐지 및 차단
- 알려지지 않은 BOF 공격 차단 정보 침입차단 시스템에 전송
- 침입탐지시스템 탐지 정보 수신 및 해당 IP, 포트에 대한 차단
- 취약성진단도구 취약성 정보 수신 및 해당 IP, 포트에 대한 차단

3.2.2 침입탐지시스템

침입탐지시스템은 전체 시스템에서 다음과 같은 기능을 수행한다.

- 네트워크 침입탐지 기능 수행
- 공격 차단 정보 침입차단시스템에 전송
- 공격 차단 정보 Secure OS에 전송
- 침입 탐지 사실 관리자 통보

3.2.3 취약성진단도구

취약성진단도구는 전체 시스템에서 다음과 같은 기능을 수행한다.

- 알려진 취약성 진단 기능 수행
- 취약성 차단 정보 침입차단시스템에 전송
- 취약성 차단 정보 Secure OS에 전송
- 취약성 진단 결과 관리자 통보

3.2.4 침입차단시스템

침입차단시스템은 전체 시스템에서 다음과 같은 기능을 수행한다.

- Secure OS의 알려지지 않은 BOF 공격 탐지 정보 수신 및 해당 IP, 포트에 대한 차단 기능 수행
- 침입탐지시스템의 탐지 정보 수신 및 해당 IP, 포트에 대한 차단
- 취약성 진단시스템의 취약성 정보 수신 및 해당 IP, 포트에 대한 차단

3.3 지능형 다단계 정보보호체계

지능형 다단계 정보보호체계의 구축을 위해서는

정보보호의 세가지 측면을 고려해야 하며, 이에 대한 절차는 다음과 같다.

먼저, Secure OS및 침입차단시스템 연동기반의 시스템 정보보호체계를 구축하며, 다음에는 Secure OS, 침입탐지시스템과 침입차단시스템 연동기반의 네트워크 정보보호체계를 구축한다.

마지막으로, Secure OS, 취약성진단도구 및 침입차단시스템 연동기반의 사전예방 정보보호체계를 구축한다.

이러한 지능형 다단계 정보보호체계에 대한 상세설명은 다음과 같다(그림 3 참고).

3.3.1 1단계 - 시스템 정보보호체계(Secure OS와 침입차단시스템 연동을 이용한 대응체계)

웜 바이러스가 방화벽을 통과하여 서버 시스템에 유입되면 Secure OS가 서버 수준에서 버퍼오버플로우를 탐지 및 차단하여 웜 바이러스가 더 이상 악의적인 행위를 하지 못하도록 원천적으로 차단 및 방지함과 동시에 이 사실을 관리자에게 통보하고 방화벽에 해당 IP와 Port를 알려서 웜 바이러스의 네트워크 유입을 차단

3.3.2 2단계 - 네트워크 정보보호체계(Secure OS와 침입차단시스템 및 침입탐지시스템 연동을 이용한 대응체계)

웜 바이러스가 네트워크로 유입되게 되면 IDS가 이를 탐지하여 이 사실을 관리자에게 통보함과 동시에 방화벽과 Secure OS에 해당 IP와 Port를 알리면, 이후 악성 패킷의 네트워크 및 서버 시스템에 대한 접근을 동시에 차단

3.3.3 3단계 - 사전예방 정보보호체계(Secure OS, 취약성진단도구와 침입차단시스템 연동을 이용한 대응체계)

Scanner가 주기적인 취약성 점검을 통해서 웜 바이러스 취약성을 발견하게 되면 이 사실을 관리자에게 통보함과 동시에 방화벽과 Secure OS에 해당 IP와 Port를 알리고 악성 패킷의 네트워크 및 서버 시스템에 대한 접근을 동시에 차단

4. 결 론

이제까지 살펴본 바와 같이 침입탐지시스템, 침입차단시스템과 같은 단일 보안 솔루션의 운용으로는 웜 바이러스나 DRDoS와 같이 새로운 취약성을 이용한 공격, 또는 정상적인 서비스를 이용한 공격 기법에는 그 한계를 드러내고 있음을 살펴보았다.

본 고에서는 이와 같은 한계점을 극복하기 위해, Secure OS, 침입탐지시스템, 침입차단시스템, 취약성분석도구 등을 적용하여, 각 솔루션 간의 상호 보완적인 연동을 통해 이러한 공격 기법에 대한 근본적인 대응을 수행할 수 있는 Secure OS를 이용한 지능형 다단계 정보보호시스템을 제안하였다.

이러한 보안 솔루션간의 상호연동을 통한 지능형 다단계 정보보호시스템은 인터넷 웜 및 DOS 등의 공격을 원천적으로 방어할 수 있으며, 또한 기존의 보안솔루션(Legacy Security Solution)을 그대로 활용하여 손쉽게 구현이 가능한 장점을 가지고 있다.

참고문헌

[1] http://grc.com/dos/drdos.htm
[2] Annual Report 2002, Trend Micro
[3] S. Kumar, Classification and Detection of Computer Intrusions, Purdue University, Aug, 1995
[4] http://www.cs.purdue.edu/coast/intrusion -detection/welcome.html

저자약력

홍 기 웅

1985년 2월 전남대 전자계산학과 졸업(학사)
1990년 2월 중앙대 대학원 전자계산학과 졸업(석사)
1996년 2월 아주대 대학원 컴퓨터공학과 졸업(박사)
1985년 9월~1995년 10월 한국전자통신연구원 선임연구원
1995년 10월~1996년 4월 한국전산원 선임연구원
1996년 4월~2000년 2월 한국정보보호센터 (응용기술팀장, 평가체계팀장, 인증관리팀장)
1998년 3월 - 현재 동국대학교 국제정보대학원 겸임교수
2000년 3월 - 현재 (주)시큐브/(주)케이사인 대표이사
이 메 일 : kyhong@secuve.com

김 재 명

1997년 2월 충남대 컴퓨터과학과 졸업(학사)
1999년 2월 충남대 대학원 컴퓨터과학과 졸업(석사)
2003년- 현재 경기대 정보보호기술공학과 박사과정 재학 중
1996년 7월~1997년 12월 한국전자통신연구원 위촉연구원
1998년 12월~2000년 2월 한국정보보호센터 기술개발부 연구원
1999년 1월~2000년 2월 공인인증기관 실질심사 위원
2001년 3월-현재 (주)시큐브 상무이사
이 메 일 : cosmos@secuve.com

은 유 진

1995년 2월 아주대 컴퓨터공학과 졸업(학사)
1997년 2월 아주대 대학원 컴퓨터공학과 졸업(석사)
2002년 아주대 대학원 컴퓨터공학과 박사과정 수료
1996년 12월~2000년 2월 : 한국정보보호센터 기술개발부 주임연구원
1997년 10월~2000년 2월 : 한국정보통신기술협회(TTA) 정보보호 기술연구위원회 연구위원
2000년 3월 - 현재 (주)시큐브 부사장
이 메 일 : silver@secuve.com

이 규 호

1999년 2월 아주대 컴퓨터공학과 졸업(학사)
2001년 2월 아주대 대학원 컴퓨터공학과 졸업(석사)
2003년 - 현재 경기대 대학원 정보보호기술공학과 재학중(박사)
2000년 4월 - 현재 (주)시큐브 보안취약성도구 개발팀장
이 메 일 : perry@secuve.com