대규모 트래픽 폭주 공격에 대한 지능적 대응 방안

김 건 우* 김 환 국* 김 정 녀* 장 종 수*

◈ 목 차 ◈

1. 서 론

21세기 지식 정보화 사회의 기반은 전 세계적으로 수 백만대의 컴퓨터가 상호 연결되어 수억의 네티즌들이 사용하고 있는 인터넷이라는 데는 이론의 여지가 없다. 이러한 인터넷 망을 고도화 시키기 위한 선진 각국의 노력 또한 더 한층 치열해 지고 있다. 우리나라 역시 1998년 6월에 처음 서비스를 시작한 초고속 인터넷은 4년 만에 1000만 가입자 시대를 열었다. 이는 국내 전체 1430만 가구의 70%에 해당되며, 보급률도 캐나다의 약 2배, 미국의 4배, 일본의 8배 등으로 해외 선진국과 큰 차이를 보이고 있으며(OECD, 2001,12), 이로 인해 사회 전반에 정보화에 대한 인식이 보편화되고, IT기술의 생활화가 급격하게 진전되면서 산업발전에 기여하고, 시공간의 제약을 완화시켜 생활의 편의성을 높이는 등 국민들의 삶의 질 향상에 기여하고 있다.

그러나 인터넷은 누구나 쉽게 접근할 수 있는 개방망 환경으로 인한 해킹, 바이러스 유포, 지적 재산권의 침해, 사이버 범죄에의 이용 등과 같은 정보보호 역기능의 위협도 만만치 않은 것이 현실이다. 이에 각 기업 및 기관들은 해킹의 심각성을 자각하여 인터넷상의 정보를 보호하고, 자사의 시스템을 보호하기 위해 각종 보안 시스템을 도입하여 자사 네트워크 및 시스템을 보호하고자 했다.

이러한 사용자의 요구에 발맞추어 각종 보안 시스템들을 개발하여 도입하기 시작하였는데, 대표적인 보안 시스템으로는 방화벽, 침입탐지 시스템, VPN, Anti-Virus 시스템, 생체 인식 시스템 등이 있다. 이와 같은 시스템들은 주로 접근 제어 및 시스템 보안에 초점을 맞춘 제품들로 최근까지 각 시스템이 개별적으로 설치 운영되는 형태를 보여왔다. 그러나 점점 사이버 테러 공격 기술의 추세가 기존의 단위 기술에서 총체적이고 유기적으로 연동되는 통합 기술로 발전하고 있으며. 특히, 신속한 전파 능력을 지닌 웜 바이러스에 시스템 및 네트워크를 파괴할 수 있는 해킹 기술을 통합하는 시도가 최근 급격히 증가되고 있다. 제한된 네트워크와 호스트에 대한 서비스 거부 공격을 통한 국지적 네트워크 마비를 시도하던 방식에서, 다량의 네트워크 트래픽 발생과 네트워크 노드에 대한 공격을 동시에 시도하여 전역적 네트워크 마비를 일으키는 해킹이 시도되고 있으며, 이로 인해 개별적 보안 시스템으로 이를 막기에 한계에 이르게 되었다. 대표적인 예로 MS SQL 슬래머 웜 공격으로 인한 "1.25 인터넷 대란"에서 볼 수 있듯이 개별 보안 시스템의 설치가 분산 서비스 거부 공격 유형의 네트워크 트래픽 공격을 막기에는 한계를 드러내고 있다.

따라서, 본 원고에서는 이러한 대규모 네트워크 트래픽 공격에 대해서 능동적/지능적으로 대처하기 위한 다양한 대응 방안을 모색하고, 각 기술이 보장하는 다

* 한국전자통신연구원 네트워크보안그룹

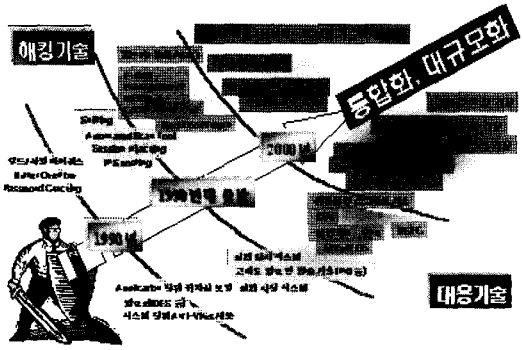
양한 보안 특성을 분석하고자 한다.

본 원고의 구성은 2장에서 최근의 해킹 기술 동향에 대해 살펴보고, 3장에서는 능동형 침입 대응 기술로 침입 방지 기술(IPS)에 대해 기술한다. 그리고, 4장에서는 최근 이슈가 되고 있는 침입 감내 기술(ITS)에 대해서 설명하고, 5장에서는 지능적 침입 대응 기술을 설명하며 마지막으로 6장에서는 결론을 맺는다.

2. 최근 해킹 기술 동향

최근 해킹 기술의 특징을 살펴보면, 단일 기법 중심의 해킹/바이러스 기술이 점차 통합화, 고도화되고 해킹 매체 및 목적이 다양화되고 있다.

다시 말해, 해킹의 공격 대상이 개별 시스템/서버 중심에서 개인 PC 공격을 활용하여 인터넷에 연결된 네트워크를 대상으로 변하고 있으며 해킹에 의한 피해 정도는 지엽적인 소규모 수준에서 광역적인 대규모 수준으로 커지고 있다. 또한, 공격의 목적이 개인적이 아닌 정치·사회, 군사·산업적 목적으로 악용되어 네트워크 또는 특정 서비스의 기능을 마비 및 파괴시키는 핵티비즘(Hacktivism)의 형태로 변하고 있다[1].



(그림 1) 최근 해킹 기술 동향

2.1 악성 코드(웜/바이러스)의 증가

초기 웜은 컴퓨터의 메모리에서 자기 복제를 통해 컴퓨터 부팅을 방해하는 프로그램으로서 피해범위는 개별 시스템으로 한정되며, 디스켓을 통한 느린 전파가 전부였다. 그러나, 네트워크 컴퓨팅 기술의 비약적인 발전으로 인하여 피해범위가 인터넷과 연결된 컴퓨터 전체의 영역으로 확장되고 악성코드의 전파 수단으로 e-mail 과 인터넷이 이용되면서 피해범위가 네트워크를 통해 동시 다발적으로 광범위하게 퍼지고 있다. 또한, 악성코드들이 해킹에 이용되는 기술들과 통합화가 이뤄지고 있다.

따라서, 앞으로 홈 네트워크, 이동통신과 인터넷의 결합 등 정보기술분야의 새로운 기술과 환경은 더욱 강력한 악성 코드의 증가를 예고하고 있다.

2.2 웹 어플리케이션 해킹의 증가

최근 주요기관이 침입 차단 시스템 설치 운영 등 보안관리 강화로 인하여 해커들이 직접 침투하기 어려운 환경이 되고 있다. 그러나 외부에 공개되는 웹 포트(TCP 80번)를 이용한 공격과 사고가 급증하고 있다. 즉, 기존의 침입 차단 시스템과 침입 탐지 시스템은 어플리케이션 계층에서 발생되는 해킹에 대응할 수 있는 보안 메커니즘이 취약하다. 따라서, 웹 어플리케이션에서의 버그나 CGI 프로그래밍 기법이 보안의 취약성을 낳게 되고 이러한 취약성을 이용한 웹 어플리케이션 해킹 공격이 증가하고 있다.

2.3 시스템 공격에서 대규모 네트워크 공격

해킹은 기존의 개인적인 호기심을 만족시키고 자신을 과시하기 위해 특정 시스템에 접근해 파괴하던 형태에서 정치, 사회, 군사, 경제적인 목적 달성을 위한 시스템, 네트워크의 주요자원을 악용하는 형태로 변화하고 있다. 특히 네트워크 또는 특정 서비스의 기능을 마비시킴으로써 인터넷 자체를 불가능하게 하고 있다.

지난 1.25 인터넷 대란의 원인인 슬래머 웜과 국내 ISP의 대형 백본 망에서 송수신되는 트래픽 중 약 10%가 정상적인 서비스와 무관한 트래픽이라는 사실을 통해 대규모 피해를 유발시키는 웜의 증가 및 개별 시스템 공격에서 네트워크 대역폭을 고갈시키는 유형의 네트워크 공격이 크게 증가되고 있음을 알 수 있다.

2.4 무선 랜 관련 취약점 공격 증가

무선 랜 환경이 확대되면서 무선 랜 프로토콜 아키텍처의 취약점을 이용한 무선 랜 해킹도 늘어나고 있다. 무선 랜 해킹의 대표적인 기법은 무선 액세스 포인트의 인증 구조를 이용하는 것으로서 이 기법은 무선 랜 사용자가 액세스 포인트에 접속할 때 가상의 액세스 포인트를 경유해 해커가 사용자 중요 정보를 모니터링 한다.

이 밖에도 인스턴트 메신저를 이용한 공격, Peer-to-Peer 응용 프로그램을 이용한 공격, PDA을 이용한 공격 등 고성능/고도화 해킹 기술이 출현하고 있으며, 해킹을 이용한 매체 및 목적이 다양화되고 있다.

3. 침입 방지 기술(IPS)

최근 해킹 기술 동향에서 살펴보듯이 다양하고 지능적인 침해사고가 날로 증가하고 있으나, 슬래머 웜이나 블래스터 웜 같은 복합 위협으로부터 기존의 IDS나 방화벽, 바이러스월 같은 기존 정보보호 기술로는 악의적인 위협을 모두 막아낼 수 없다는 기술적인 한계를 드러냈다. 이에 따라 유해 트래픽으로 인한 네트워크 전반의 가용성 침해를 방지하기 위해 방화벽과 IDS의 기능 보강에 대한 요구가 높아졌고, 네트워크 트래픽의 폭증으로 보다 능동적이고 진보된 보안기술이 요구되고 있다.

능동형 보안 기술은 외부의 침입을 지능적으로 탐지하고 자동으로 차단하는 기능과 함께 각종 정보보호 솔루션들과 유기적으로 연동해 네트워크를 안전하게 보호할 수 있도록 하는 일련의 기술을 포함하고 있다. 이 기술은 특히 기존의 통합보안 추세에 이어 보안 솔루션의 고속화, 고성능화와 함께 인텔리전트 기술을 수용하며 빠르게 발전하고 있다.

이와 같은 시장의 요구에 따라 출현한 개념이 사이버상의 어떠한 위협에 대해서도 사전에 방지한다는 침입방지(Intrusion Prevention) 기술이다. 이러한 능동형 보안 기술은 가장 먼저 기존 방화벽과 IDS를 보완한 침입 방지 시스템(IPS)의 형태로 제품화되고 있다.

3.1 IPS 기술

침입 방지 시스템(IPS)과 IDS의 차이점은 IDS는 침입이 발생했을 때 문제를 즉각적으로 처리하지는 못하지만, IPS는 공격 시그너처를 찾아내고 네트워크의 트래픽을 관찰해, 수상한 활동을 하는 패킷에 조치를 취한다는 것이다. 또한, IPS는 서버가 비정상적인 행동을 할 경우 자동으로 실행을 중단할 수도 있다. 이러한 IPS 시스템은 IDS와 마찬가지로 호스트 기반과 네트워크 기반의 시스템으로 나누어진다[2][3].

3.1.1 호스트 기반 IPS

호스트 기반 IPS의 기술적인 특징은 크게 커널과 함께 동작해 커널 이벤트를 가로채 처리하는 방식과 커널과 독립적으로 작동하는 방식으로 구분되며, 전자는 대부분 접근제어 기능을 가진 트러스트 운영체제(Trust Operating System) 제품들로 분류할 수 있고 후자는 시그너처와 행동 기반 분석 알고리즘을 이용하여 특정 규칙에 위배되는 이벤트를 필터링하는 제품들로 분류할 수 있다.

시장조사 전문업체인 가트너에 따르면 호스트 IPS는 우선 소프트웨어 제품이어야 하며, 방화벽 룰 셋(rule set)과 같은 정책이나 정상/비정상 접근에 대한 학습을 통해 취약한 응용 프로그램을 보호할 수 있어야 한다.

3.1.2 네트워크 기반 IPS

네트워크 기반 IPS의 기술적인 특징은 실시간 패킷 처리, 오탐지를 최소화하는 기술, 변형 공격과 오용공격의 탐지기술, 그리고 각 상황에 맞는 실시간 반응 기술이라고 말할 수 있다.

가트너에 따르면 침입 방지 능력과 빠른 반응 속도를 위해 네트워크 라인상에 위치한 제품이어야 하며, 세션 기반 탐지(session aware inspection)를 지원할 수 있는 시스템을 말한다. 또한 다양한 종류의 방지 방법 및 방식(signature, 프로토콜적인 비정상 행위 탐지)을 통해 악의적인 세션을 차단하는 것도 필수적이다. 현재 시장에서는 기가비트 트래픽을 지원하며 ASIC 기반의 제품 등과 같이 다양한 국내/외 제품이 출시 및

개발되고 있다. (표 1)은 시장에서 출시되고 있는 IPS 제품들을 3가지 유형으로 분류한 것이다[4].

(표 1) IPS 제품 분류

종 류	내 용
스위치 기반의 IPS	백본 스위치로 연결되는 경로에 설치된 스위치에서 실시간 공격이나 유해 트래픽을 차단하는 제품
IDS 기반의 IPS	서버 기반의 소프트웨어 형태의 IDS 기술을 전제로 침입 차단 시스템의 패킷 필터링 기능을 추가한 제품
Firewall 기반의 IPS	하드웨어 기반의 IPS를 구현하기 위해 ASIC 기반의 어플라이언스 형태의 침입 차단 시스템을 이용한 제품

3.2 IPS 문제점

IPS는 IDS와 방화벽의 기반 기술을 이용한다. IDS가 불법 패킷을 탐지하고 이에 따라 자동으로 방화벽에서 차단한다는 원리를 내포하고 있다. 따라서 IPS는 IDS에서 발생하는 공격인 아닌 것을 공격으로 오인, 전달하는 잘못된 경고 메시지 False Positives와 공격을 정상으로 오인하여 탐지를 해내지 못하는 False Negative를 완벽히 제거해야 한다. 이러한 False Positive가 발생할 경우 자동적으로 패킷이 차단되어 정상적인 정보나 서비스를 차단하는 문제점을 가져오게 된다. 또한 False Negative가 발생하는 경우에는 IPS는 방지 자체를 못하게 되며 침입이 발생한 후에 대한 방지는 의미를 잃게 된다[2].

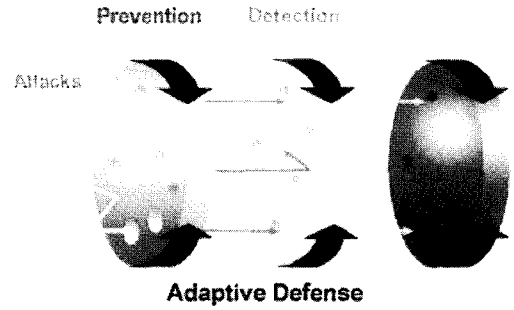
지금까지 살펴본 IPS는 IDS를 기반으로 출발했지만, 침입방지 기술의 핵심은 실시간 패킷 처리 속도, 오탐지를 최소화하는 기술, 변형 공격과 오용 공격의 탐지 기술, 그리고 각 상황에 맞는 실시간 반응 기술 등이다.

앞으로 다양한 공격에 대해 실시간 탐지 및 차단 기능을 제공하는 침입 방지 시스템에 대한 필요성이 더욱 증가할 것으로 예상된다. 최근 가트너 발표자료에 의하면 2004년에는 네트워크 기반 침입방지 시스템이 이미 설치된 침입 탐지 시스템의 50%를 대체하고, 새롭게 도입하고자 하는 고객의 75%가 네트워크 기반 침입 방지 시스템을 선택할 전망이라고 한다. 따라서, IPS 가 방화벽과 IDS를 하나로 구현한 통합보안 솔루션으로 한 축을 이룰 것으로 보인다[4].

4. 침입 감내 기술 (Intrusion Tolerance Technology)

과거에는 정보시스템의 보안을 위해 침입자와 데이터의 격리를 통한 기밀성과 무결성을 강조하였으며, 이를 위해 중요한 정보를 암호화하는 방법과 인증된 사용자에게만 권한을 부여하는 접근 제어 방법이 많이 사용되었다. 그러나 이러한 방법은 성능과 기능성이 저하되고 암호화와 인증을 위한 추가 비용이 발생하는 점과, 특정 소프트웨어나 하드웨어가 필요하다는 단점이 있다. 따라서 이러한 문제점을 해결하기 위해서, 침입이 성공하더라도 시스템의 중요 서비스를 지속적으로 제공하는 것을 목표로 무결성과 가용성을 강조하는 침입 감내 시스템이 제안되었다[5].

침입은 성공 단계에 따라 침입(Intrusion), 접근(Access), 충격(Impact) 및 손상(Failure)으로 구분될 수 있으며, 접근, 충격 상태에서 손상 상태로 단계가 진행되지 않도록 침입 감내 체계가 필요하다.



(그림 2) 침입 감내 기술 계층 구조

(그림 2)는 외부 공격에 효율적으로 대처하기 위한 침입 감내 시스템의 계층 구조를 보여준다. 첫 번째 계층은 예방(Prevention) 계층으로서, 시스템이 가지는 취약성 분석, 방화벽 기술 등과 같이 공격 예방을 위한 기술들을 포함한다. 두 번째 계층은 탐지(Detection)

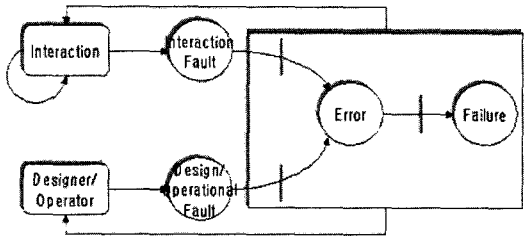
계층으로, 예방 계층에서 미처 방어하지 못한 취약점을 뚫고 침입하는 공격을 탐지하고 이에 대한 대응책을 마련하는 기술들을 나타낸다. 현재 대부분의 정보보호 기술들은 이 두 계층을 구현하고 있다. 하지만 예방 계층, 탐지 계층의 정보보호 기술들만으로는 알려지지 않은 취약점 공격에 효율적으로 대처할 수 없다. 마지막 세 번째 감내(Tolerance) 계층은 복제 시스템을 이용하여 침입에 감내하는 기술이며 알려지지 않은 취약점으로 인한 침해사고에 대한 대책을 포함한다.

대표적인 감내 기능은 보안자원 관리기술, 동적 네트워킹 기술, 시스템 적용력 기술 등이 있다. 보안자원 관리기술은 위험 상황 시에 보안 서비스를 신뢰성 있게 지원하기 위하여 보안 자원을 관리하고 보안 서비스가 적합한 수준으로 제공될 수 있도록 지원한다.

동적 네트워킹 기술은 위험 상황에 대처하기 위한 전체 네트워크 차원의 기술이며, 동적 라우팅 설정을 통하여 논리적인 보안 네트워크를 생성 관리하며, 이를 통하여 네트워크의 신뢰성을 보장한다. 즉, 네트워크 서비스의 복제를 통하여 위험 상황에 대처하기 위한 예비 자원을 할당하고, 네트워크 침입의 영향이 전체 네트워크 서비스의 안전성에 영향을 미치지 않도록 네트워크 서비스를 분할하는 것이다. 시스템 적응력 기술은 보안 시스템의 신뢰성을 지원하기 위한 시스템 자체의 동적 적응 기술을 의미하며, 보안 기능의 성능이 저하될 경우 제한된 보안 자원을 최대한 활용하여 보장된 보안 기능을 수행할 수 있도록 하는 것이다[6].

4.1 결함 허용 기술(Fault Tolerance Technology)

결함 허용 기술이란 하드웨어 혹은 소프트웨어에 결함이 존재하더라도 계속 주어진 임무를 수행하도록 하는 기술이다. 시스템의 손상은 결함으로부터 시작되며 이러한 결함은 우발적, 혹은 의도적으로 발생할 수 있고, 발생 요인 또한 내부적 결함 혹은 외부 환경에 의한 결함, 설계의 결함 등 매우 다양한 원인으로부터 발생할 수 있다. 결함은 시스템의 다른 부분으로 전파되어 시스템이 정상적인 결과물을 산출하지 못하는 오류(Error) 상태로 전이되고 오류 상태를 결국 시스템의 고장(Failure) 상태로 전이되게 된다.



(그림 3) 상태 개념 및 전이

(그림 3)은 각 상태의 개념과 전이 과정을 보여준다. 따라서, 결함 허용 기술은 시스템의 결함이 오류, 혹은 고장 상태로 전이되어 정상적인 서비스가 불가능하게 되는 것을 방지하기 위한 기술로 볼 수 있다.

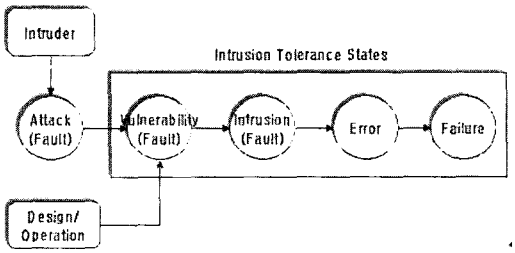
기존 결함 허용 기법은 결함 허용성을 부여하는 방법에 따라 크게 소프트웨어 기법, 하드웨어 기법, 및 혼합 기법으로 구분할 수 있다.

4.2 침입 감내 기술(Intrusion Tolerance Technology)

침입 감내 기술에서의 결함은 결함 허용 기술에서의 결함과 다르다. 결함 허용 기술에서는 주로 시스템 내부적으로 유발되거나 악의가 없는 우발적 실수에 의하여 발생하는 결함이 대부분인데 반해, 침임 감내 기술은 외부의 악의적인 공격은 물론 공격이 발생한 시스템의 취약점을 방지하고 제거함으로써, 시스템의 의존성 및 신뢰성을 확보할 수 있고 시스템이 제공하는 정상적인 서비스를 지속적으로 제공하기 위한 기술이다.

침입 감내 기술이 가지는 특징은 가용성과 신뢰성, 그리고 보안성으로 대표되는 의존성의 확보이다. 보안 시스템의 통합적 사용을 위한 ESM 기술의 확장된 사용, 침입대응 및 복구기술의 사용 등을 통하여 부분적으로 이루어질 수 있다. 그러나 침입 감내 시스템은 서비스의 가용성 제공과 더불어 제공되는 정보의 신

뢰성과 보안성, 그리고 적시성이 동시에 만족되어야 하는 특징이 있다. 그러므로 부분적인 문제 해결을 제공하는 기존의 기술들과 많은 부분에서 차이를 보인다[7].



(그림 4) 침입 감내의 결함 모델

시스템의 취약점이 있을 경우 외부의 악의적인 공격으로 시작되어 시스템이 결함이 발생하고, 결함은 오류로 전파되어 오류는 다시 시스템의 고장을 유발시킨다.

오류처리는 결함 탐지(fault detection)와 복구(recovery)에 의해 이루어진다. 오류 탐지(error detection)는 시스템의 결함이나 공격이 발생하였는지 알기 위한 방법이며, 복구는 결함이나 공격이 발견되는 경우 시스템이 정상적인 상태를 유지할 수 있도록 하기 위한 방법이다.

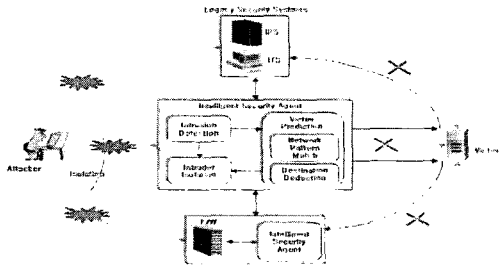
결함이 탐지되면 오류가 발생한 부분을 시스템에서 분리하고 오류가 없는 새로운 부분으로 대치(복구)해야 하며, 회복 방법에는 후방 회복(backward recovery), 전방 회복(forward recovery), 오류 마스킹(error masking)이 있다

결함이 발생한 부분을 시스템에서 분리하는 과정이 수행된 후에는 발생한 결함에 대한 치료가 필요하다. 이 부분에서는 어떠한 결함 혹은 침입이 발생하였고 어떤 오류를 발생하게 하였는지 식별하고 예방 조치를 취하는 기능이 필요하며, 진단(Diagnosis), 격리(Isolation), 재구성(Reconfiguration)이 등의 방법이 있다.

5. 지능적 침입 대응 기술

침입 방지 기술이나 침입 감내 기술 등이 외부의 불법 공격으로부터 시스템이나 로컬 네트워크를 보호하는데 중점을 두는데 반해, 본 절에서 설명하는 지능적 보안 에이전트(ISA: Intelligent Security Agent)를 이용한 침입 대응 기술은 DDoS와 같은 대규모 네트워크 기반 트래픽 폭주 공격을 효과적으로 탐지, 대응 및 예방함으로써, 공격에 의한 영향을 최소화하고 침입자를 격리시키는 효과를 통해 추후의 2차적인 공격을 차단하는 방안을 제시한다.

다중 네트워크 경로를 통한 단일 시스템으로의 공격에 효과적으로 대응하기 위해서는 네트워크간의 연동이 무엇보다도 중요하다. 또한 다양한 침입 패턴 및 세션 정보 등의 분석을 통해 침입자를 고립/격리시켜 근본적인 침입 경로를 차단하고, 최종 타켓 시스템은 물론 전체 인터넷에 미칠 수 있는 영향을 최소화해야 한다.

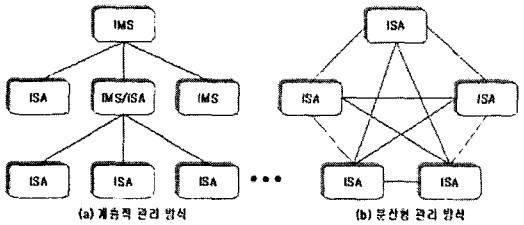


(그림 5) ISA 침입 대응 모델

ISA는 크게 네트워크 침입 탐지 기능(NIDS), 탐지된 네트워크 패턴을 통한 Victim 예상 기능(Victim Prediction) 및 침입자 고립 기능(Intruder Isolation) 등으로 구성된다. 또한, 임의의 네트워크 경로에 위치할 수 있으며, ISA간의 연동은 물론 IDS, IPS, ITS 및 방화벽과 같은 기존 네트워크 보안 시스템과의 인터페이스를 제공할 수 있어야 한다. 다중 ISA를 관리하는 방식에는 IMS(ISA Management System)를 통한 계층적 관리 방식과 ISA간 제어 정보 교환을 통한 분산형 관리 방식이 있으며, 이들간의 통신은 IPsec이나 SSL과 같은 보안 프로토콜에 의해서 보호되어야 한다.

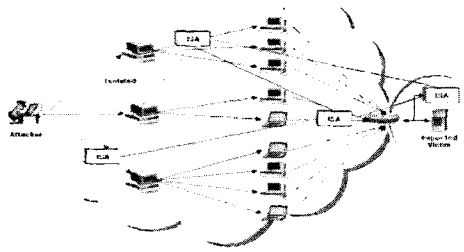
계층적 관리 방식은 높은 확장성과 이식성을 가지며, 효율적인 제어와 관리 기능을 제공하지만 중복되는 세션 생성에 의한 네트워크 성능이 저하될 우려가

있다. 반면, 분산형 관리 방식은 구현이 용이하고 최소한의 성능 저하를 초래하지만, 낮은 확장성을 가지는 단점을 내포한다.



(그림 6) ISA 관리 방식

ISA내의 침입 탐지 모듈이 네트워크 공격을 탐지하면, 우선 해당 세션을 차단하거나 침입자 역추적 모듈을 구동하는 등 정의되어 있는 침입 대응 방식을 수행할 수 있다. 더불어, 탐지된 침입 패턴, 세션 정보, 및 다른 ISA에서 수집한 정보를 기반으로 최종적으로 예측되는 victim을 추론하여, 해당 victim을 관장하는 ISA에 통보한다. 또한 해당 공격으로부터 victim 네트워크를 보호하는 것은 물론, 모든 침입 루틴을 분석해서 침입자로 추정되는 노드로부터 발생되는 모든 패킷의 경로를 실시간으로 차단한다.

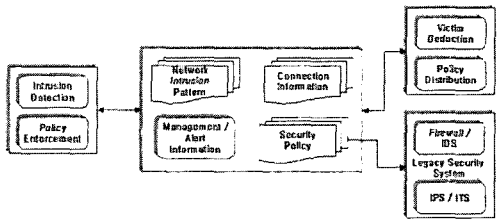


(그림 7) ISA 네트워크 모델

DDoS와 같은 대규모 네트워크 트래픽 공격은 다중 세션을 통해 대형 트래픽을 발생시켜 단일 네트워크나 노드에 집중시키기 때문에, 하나의 침입 루틴만을 차단하는 소극적인 대응 방식으로는 공격의 영향을 최소화하기 어렵다. 또한, 최종 victim 레벨에서의 공격 차단은 해당 네트워크를 보호할 수는 있지만 인터넷 상에서의 불필요한 트래픽 폭주로 인한 성능 저하를 효과적으로 방지할 수는 없다.

따라서, 이러한 수동적인 대응 방안에서 벗어나, 예상되는 피해를 최소화하고 침입자를 고립시켜 침입을 원천봉쇄하고 역추적하여, 추후의 2차 공격을 예방하는 지능적 대응 방안이 필요하다.

한편, 중복된 ISA간의 연동은 오히려 네트워크 트래픽을 증가시켜 성능 저하를 초래할 수 있다. 즉, 불필요한 ISA간의 연동을 배제하기 위해서는 교환되는 정보에 대한 효과적인 상태 기반 세션 관리가 요구됨에 따라 계층적 관리 방식이 효율적인 솔루션이 될 수 있다.



(그림 8) ISA 연동을 위한 정보

네트워크 침입 탐지 모듈은 탐지된 침입 패턴과 연결 정보를 다른 ISA와 교환하고 분석해서 최종 victim을 추론한다. 또한 해당 공격을 원천봉쇄하기 위해서는 대응 방안을 포함하는 보안 정책이 필요하며, 이는 ISA에서 실시간으로 적용될 뿐 아니라, 기존의 보안 시스템과의 호환성을 보장할 수 있어야 한다.

6. 결 론

대규모 인프라 공격에 대한 기술 연구는 최근에 들어서야 집중적으로 이루어지고 있는데, 공격 방법에 대한 원천적인 연구보다는 실제의 공격 경험을 토대로 한 탐지 및 대응 방법의 연구가 주류였다. 탐지 및 대응 방법에 관련된 대부분의 연구들에서는 공격 탐지와 대응 시점이 공격이 대부분 진행된 시점에 이루어지고, 이를 위해 단시간에 수집된 소량의 패킷 정보를 이용하고 있다. 또한 네트워크 전체적인 관점에서보다는 특정 위치에 국한된 탐지와 대응 방법들이 연구되어 왔다[8].

하지만, 정보보호에 대한 개념이 수동적 대응에서 능동적 대응으로 변함에 따라, 외부 침입에 대해 수동적으로 대응해온 기존 정보보안 솔루션의 개념도 네트워크와 시스템 구성의 기본 인프라로서 침입을 원천봉쇄하고 침입의 영향을 최소화하는 능동적 개념으로 진화하고 있다.

현재 개별 호스트나 지역 망에서 적용되고 있는 방화벽, 침입 차단 시스템, 침입 탐지 시스템, 취약성 분석 시스템 및 바이러스 백신 등의 보안 시스템들은 DDoS와 같이 분산 협력 방식으로 다양하고 복잡하게 진화하는 공격과 인터넷 웜의 빠른 확산에 적절히 대처하지 못하고 있다. 이러한 주요 원인은 기존의 정보보호 시스템들이 네트워크 차원에서 효율적이고 적극적인 대응이 불가능하며, 새로운 공격 패턴이나 보안 정책 등의 변환에 적응이 어려운데 기인한다. 따라서 이러한 문제점을 해결하기 위하여 다양한 공격에 대해 능동적 대응이 가능하며, 보안 시스템들간의 협력을 통한 광역망 차원의 보안 기능을 제공하고, 사용자의 요구에 따라 보안 정책의 다변화가 용이한 새로운 구조가 필요하다[9].

침입 방지 시스템은 다양하고 지능적인 침입 기술에 대해 다양한 방법의 보안 기술을 이용해, 침입이 일어나기 전에 실시간으로 침입을 막고 알려지지 않은 방식의 침입으로부터 네트워크와 호스트를 보호할 수 있는 시스템을 말한다. 즉, 방화벽과 IDS, Secure OS 등의 보안 기술에 기반을 둔 IPS는 공격을 탐지하는 것 뿐만 아니라 공격이 일어나는 것을 근본적으로 방어하는 것을 목적으로 한다.

침입 탐지 시스템이 탐지할 수 있는 공격 또는 비율은 전체의 일부분에 지나지 않으며, 차단이 어려운 내부 공격자들에 의한 보안 사고 등, 기존 보안 기술로는 어려움이 있어 치명적인 약점을 노출하고 있다. 침입 감내 시스템은 이러한 문제를 해결하기 위한 기술이며, 미처 발견하지 못한 공격이나, 침입이 있는 경우에도 서비스를 정상적으로 제공하기 위한 새로운 분야의 정보보호 기술이다. 침입 감내 시스템이 가지는 특징은 가용성, 신뢰성, 및 보안성으로 대표되는 의존성의 확보이며, 대표적인 감내 기능으로는 보안자원 관리기술, 동적 네트워킹 기술, 시스템 적용력 기술 등이 있다.

침입 방지 기술이나 침입 감내 기술 등이 불법 공격으로부터 시스템이나 로컬 네트워크를 보호하는데 중점을 두는데 반해, 지능적 보안 에이전트(ISA: Intelligent Security Agent)를 이용한 침입 대응 기술은 DDoS와 같은 대규모 네트워크 기반 트래픽 폭주 공격에 대한 실시간 탐지 기능과 능동적이고 지능적인 대응 방안을 제공한다.

다중 네트워크 경로를 통한 단일 시스템으로의 공격에 능동적으로 대처하기 위해서, ISA간 트래픽 패턴 및 세션 정보 등의 분석을 통해 최종 victim 네트워크를 예측하여 보호할 뿐 아니라, 침입자의 근본적인 공격 경로를 원천 봉쇄하여 불필요한 트래픽 폭주로 인한 인터넷 성능 저하를 방지하고 침입자를 고립시키는 방안을 제공한다.

참고문헌

[1] 서동일, "차세대 해킹대응 기술", 제8회 정보보호 심포지움, 2003.7.

[2] 정보홍, 김정녀, 손승원, "침입방지 시스템 기술 현황 및 전망", 한국정보보호산업협회, 2003.6.

[3] J. Pescatore, R. Stiennon, "Defining Intrusion Prevention", Gartner Research, May. 2003.

[4] 심상현, "IPS, 허구인가 진실인가", 정보보호21세기, 2003.8.

[5] 김기환, 이경환, 최명렬, "Information Security : Classification of the Intrusion Tolerant Systems and Integrated Framework for Survivability", 한국정보처리학회지, 2003.

[6] 서동일, "최근 사이버 공격기술 및 정보보호 기술전망", Digital Administration, 통권 제 92호, 2003. 6.

[7] "기반보호기술(침입감내기술개발)", 한국정보보호진흥원, 2004. 02.

[8] 정유석, 홍만표, "대규모 인프라 공격에 대한 방어 기술의 발전 동향", 정보과학회지, 2003. 12.

[9] 구자범, 박세현, "차세대 네트워크 환경에서의 보안 인프라 구축을 위한 새로운 전략", 정보과학회지, 2003. 12.

◐ 저 자 소 개 ◑

김 건 우

1998년 경북대학교 컴퓨터과학과 학사
2000년 경북대학교 대학원 컴퓨터과학과 석사
2000년~현재 한국전자통신연구원 연구원
관심분야 : 네트워크 보안, 이동 네트워크, IPv6

김 환 국

1998년 한국항공대학교 전자계산학과 학사
2000년 한국항공대학교 대학원 컴퓨터공학과 석사
2000년~2002년 이레스페이스 연구원
관심분야 : 네트워크 보안, 해킹/바이러스

김 정 녀

1987년 전남대학교 전산통계학과 졸업
2000년 충남대학교 컴퓨터공학과 석사
2004년 충남대학교 컴퓨터공학과 박사
1988년~현재 한국전자통신연구원 선임연구원(팀장)
관심분야 : 인터넷 정보보호, Secure OS, 네트워크 보안

장 종 수

1984년 경북대학교 전자공학과 졸업
1986년 경북대학교 전자공학과 석사
2000년 충북대학교 컴퓨터공학과 박사
1989년~현재 한국전자통신연구원 책임연구원, 정보보호연구단 네트워크보안그룹 그룹장
관심분야 : 네트워크 보안, 보안관리기술, 개인정보보호기술 등