분산 침입탐지시스템을 위한 Dynamic Screened Zone

이정석[0] 유기영
경북대학교 대학원 컴퓨터공학과 정보보호연구실
(kit92[0], yook)@purple.knu.ac.kr

Dynamic Screened Zone for Distributed Intrusion Detection System

Jung-Seuk Lee[0] Kee-young Yoo

Dept. of Computer Engineering, Kyung-Pook National University

요 약

인터넷의 발달과 함께, 인터넷을 이용한 전자상거래, 홈 뱅킹, 온라인 교육 등 정보통신 관련 서비스가 급격히 발전하게 되었다. 그러나 이러한 확장으로 인한 긍정적 효과도 있으나, 시스템의 불법 침입, 중요 정보의 유출 및 훼손, 불법적인 사용, 악성 바이러스 등 역기능 역시 심각한 피해를 주고 있다. 이러한 피해를 막기 위한 기술로 다양한 침입탐지 시스템과 방화벽이 활용되고 있으나, 아직 한계와 문제점들이 존재하고 있다. 본 논문에서는 이러한 악의적인 공격들로부터 대처 하기 위해 현재 개발 중인 분산 침입 탐지 시스템과 함께 동작 하게 될 Dynamic Screened Zone을 구성하였다.

1. 서 론

인터넷의 발달과 함께, 인터넷을 이용한 전자상거래, 홈 뱅킹, 온라인 교육 등 정보 통신 관련 서비스가 급격히 발전하게 되었다. 이러한 발전에 힘입어 사용자의 편리성을 증대 시키고, 업무 처리의 효율성을 강화 시키는 등 긍정적인 효과도 있으나, 악의적인 사용자의 불법 침입, 중요 정보 유출 및 훼손, 악성 바이러스 등 역기능 역시 심각한 피해를 주고 있다. 따라서 이러한 피해를 막기 위한 기술로 다양한 연구가 이루어 지고 있으며, 대표적인 것이 침입탐지 시스템과 방화벽이다.

지금까지 침입탐지 시스템과 방화벽 같은 보안 기술에 대한 많은 연구가 이루어졌으나, 상대적으로 공격 기술 또한 발전하여 새로운 공격 형태들이 나타나고 있다. 이러한 새로운 공격 기술들은 더욱 고도화되고 지능화되는 추세이다. 본 연구팀이 이러한 악의적인 공격으로부터 대처하기 위한 보안 시스템으로 연구/개발 중인 것이 분산형 침입 탐지 시스템과 Dynamic Screened Zone이다. 본 논문에서는 그 중에서 분산 침입탐지 시스템과 함께 동작하게 될 Dynamic Screened Zone영역만 설명하려고 한다.

본 논문의 구성은 2장과 3장에서 침입탐지 시스템과 방화벽에 대해 알아보고, 이를 효율적으로 구성하기 위한 고려 사항과 문제점들을 알아본다. 4장에서 본 논문에서 설계한 Dynamic Screened Zone에 대한 구조를 설명한다. 마지막으로 5장에서 결론을 짓는다.

2. 침입탐지 시스템과 방화벽

2.1 침입탐지 시스템

침입탐지 시스템이란 네트워크 또는 컴퓨터 시스템에서 발생하는 이벤트를 모니터링하여 보안 위협에 대한 징후를 분석하는 과정을 자동화한 시스템을 뜻한다. 침입탐지 시스템의 종류에는 크게 탐지 방법에 따라 비정상 행위 탐지(anomaly detection)와 오용 탐지(misused detection)로 나뉘며, 데이터 소스 자원에 따라 네트워크 기반 시스템과 호스트 기반 시스템으로 나뉘게 된다 [1][2][3].

1) 비정상 탐지 : 주로 대학이나 연구소에서 연구되고 있는 방식으로 정상적인 사용자 조작 또는 시스템의 예상되는 행위에 대한 정보를 이용하여 탐지하며, 이를 위하여 통계적 방법을 주로 이용한다. 가장 큰 장점은 현재 알려지지 않은 공격 방식에 대해서도 탐지가 가능하다는 점이다. 하지만 비정상 패킷을 탐지하기 위한 임계값 설정이 모호하며, 설정에 따른 잘못된 결과를 출력하기도 한다.

2) 오용 탐지 : 기존에 알려진 공격 방식들을 데이터베이스로 미리 구성하여, 이 정보들과 비교해서 침입을 탐지하는 방식이다. 구현 방법이 용이하고 정확도가 높고 효율적이기 때문에 현재까지 많이 개발되고 있으며 오경고율이 낮다. 반면에 특정 침입에 대한 탐지만 가능하기 때문에 새로운 공격유형은 탐지하기 어렵다는 단점이 있다.

3) 네트워크 기반 탐지 : 네트워크 패킷을 사용하여 침입을 탐지하는 시스템으로 네트워크를 통과하는 패킷 정보를 분석하여 공격을 탐지하고 관리자에게 보고 및 실시간 대응을 한다. 또한 트래픽 상황 및 TCP 연결 세션에 대한 감사를 통해 잠재적으로 발생할 수 있는 침입에 대한 대비를 할 수 있다.

4) 호스트 기반 탐지 : 내부 사용자나 외부 공격자의 악의적인 공격이나 데이터의 불법적인 변경으로부터 시스템을 안전하게 보호하는 기능을 수행하는 시스템으로, 침입 여부를 감시하고자 하는 호스트들에게 보안 에이전트를 파견하여 실시간으로 감사 자료를 바탕으로 탐지하는 시스템이다. 각 호스트들을 개별적으로 감시할 수 있기 때문에 정확한 탐지가 가능하지만 호스트의 성능에 영향을 미친다.

2.2 방화벽

방화벽이란 내부 망과 외부 망을 논리적, 물리적으로 분리하여 내부 자원에 대한 사용자의 접근을 제어하고, 침입 및 내부 사용자의 불법적인 정보 유출을 방지하기 위한 시스템이다. 방화벽은 내부 네트워크상의 모든 네트워크 요소를 외부에 공개하지 않는 것을 원칙으로 하며, 네트워크 상의 모든 트래픽을 기록할 수 있다 [3][4][5][6].

1) 패킷 필터링 방식 : 내부 호스트와 외부 호스트 사이에 통신하고 있는 패킷을 선택적으로 처리하며, 처리되는 패킷의 정보는 출발지 IP주소, 목적지 IP주소, 프로토콜(TCP, UDP, ICMP), 출발지 포트, 목적지 포트, ICMP 메시지 등이 있다. 패킷 필터링 방식은 하드웨어 방식의 방화벽을 구현하기 쉬우며, 처리속도가 빠른 장점이 있으나, 보안 규칙을 적용하기 때문에 오류를 발생 시킬 가능성이 높다.

2) 응용 게이트웨이 방식 : 방화벽에서 제공되는 보안 기능 및 서비스들을 모두 응용 소프트웨어로 구현하게 되며, 서비스마다 각각의 해당 응용 게이트웨이로 구현하기 때문에 패킷 필터링 방식보다 안전하다. 또한 접근 제어 및 기록, 인증 등의 추가적인 기능 구현이 용이한 장점이 있으나, 각각의 서비스에 대한 응용 게이트웨이가 반드시 존재하여야 되기 때문에 서비스 종류가 많아지면 오버헤드가 높아지는 단점이 있다.

3. 문제점 및 한계

3.1 침입탐지 시스템

불법적인 공격 유형이 발전하면서 침입탐지 시스템 역시 많은 발전을 하였으나, 서로 다른 보안 메커니즘과의 협력이 필요하다[1][3][4][7].

1) 네트워크 환경이 대형화 되면서 모든 패킷에 대한 검사가 불가능하며, 엔터프라이즈 환경에서는 탐지의 한계가 있다.
2) 새로운 공격 유형에 따른 정책 변경 및 대응이 어렵다.
3) 외부 침입자의 정확한 정보를 찾아내기가 어렵다.
4) 내부 공격자는 찾아 낼 수 없다.
5) 침입탐지 시스템에 피해가 발생하였을 경우 대처방법이 없다.
6) 스위칭 상에서는 정확한 탐지가 어렵다.

3.2 방화벽

방화벽 시스템은 보호하고자 하는 네트워크 자원이나 정보를 완벽하게 차단 할 수 없으며, 다만 외부 네트워크와 내부 네트워크사이를 1차적으로 방어해 주는 역할을 한다[1][3][5][6].

1) 패킷을 필터링 할 때 네트워크 접근정책이 적용이 되기 때문에 정상 패킷으로 침입을 하면 탐지 할 수 없다.
2) 접근정책이 적용되는 순서에 의해 점검하기 때문에 규칙이 적용되는 순서가 변경되었을 경우 통신장애가 발생한다.
3) 데이터 자체에 암호화가 이루어 지면 데이터 내부를 확인 할 수 없다.
4) 방화벽 또는 라우터에 저장된 로그파일, 라우팅 테이블 등 직접적 공격을 당하거나 변경이 되면 대처방안이 없다.

4. Dynamic Screened Zone

본 논문에서 연구중인 보안제어 메커니즘은 크게 3단계로 분산되어 처리하고 있으며, 관리 모델은 [8]에 정의한 형태를 기준으로 구성한다. 또한 전체 분산형 침입탐지 시스템 중에서 Screened Zone을 중심으로 설명하였다.

1) 침입 방지 : 침입을 방지 하기위한 1차적 방어를 위해 Screened Zone 영역을 구성하였다. 가장 많이 사용되는 기존 방화벽인 Screened Zone은 Dual-homed 게이트웨이와 스크린 라우터를 혼합하여 사용되고 있다 [3][5][6]. 이 영역에서 Dual-home 게이트웨이에 있는 Bastion호스트의 Configuration정보를 침입탐지 시스템이 직접 개입하여 침입탐지 시스템의 보안 정책에 따라 자동으로 변경하도록 하는 것이 Dynamic Screened Zone의 기능이다.

침입탐지 시스템에서 Screened zone영역을 변경 시켜줌으로써 침입에 대한 능동적 대응으로 공격자의 위치 및 경로를 역추적하거나 공격자의 컴퓨터를 네트워크상에서 교란 시키는 메커니즘을 만들수 있도록 하였다. 또한 Screened Zone 영역에 한정하여 보안설정을 구성하지 않고, 내부 네트워크에 존재하는 모든 호스트들에게 각각 클라이언트용 Agent를 도메인 레벨의 침입탐지 시스템이 배포하여 사용하도록 하였다. 이때 각 호스트에 전달된 에이전트는 도메인 레벨의 침입탐지 시스템의 정책을 따른다.

2) 침입 탐지 : 기존의 침입 탐지 시스템에 적용된 보안정책은 고정되어있어서 정책 변경이 쉽지 않으며, 관리자의 직접 개입을 필요로 한다. 본 논문에서는 최상위에 도메인 기반 침입탐지 시스템을 중심으로, 관리 시스템, 보안 시스템, 모니터링 시스템, 정책 시스템를 두었다. 각각의 시스템은 이동 에이젼트로 구현 및 통신을 하도록 하였다. 이동 에이젼트는 독립적으로 수행 가능하고 응용프로그램에 의해 제공되는 기능을 확장 할 수 있으며, 이동성을 충족 시켜 주기 때문에 프로그램의 경량화와 오버헤드를 줄 일 수 있다.

3) 침입 대응 : 기존의 침입탐지 시스템에서는 침입이 확인되면 관리자에게 경고를 하거나, 로그파일의 작성 등 수동적인 대응방법만 취하여 왔다. 본 시스템에서는 대응 방법을 각 단계별로 수행하여, 최종적으로 역추적까지 가능하도록 하였다. 이러한 단계를 결정하는 것과 적용하는 것은 각각의 정책 시스템내에서 이루어지며, 최상위 결정권은 도메인 기반 침입탐지 시스템의 정책에 따른다.

우선 모니터링 시스템의 모니터링 정책에 따라 각 호스트와 Dynamic Screened Zone에서 호스트 및 네트워크의 활동 상황을 모니터링하며, 보안 정책에 위배되는 처리나 이벤트가 발생을 하면, 보안 시스템의 정책이 적용된다. 또한 각 레벨의 변경된 상황이 도메인 기반 침입탐지 시스템으로 알려지게 된다.
침입 사실이 확인되면, 도메인 기반 침입 탐지 시스템에서 모니터링 시스템의 모니터링 레벨과 보안 시스템의 보안 레벨을 상향 조절한다. 위협정도가 일정 수준 이상이 되면, Dynamic Screened Zone 영역의 관리 시스템에게 보안 레벨과 모니터링 레벨을 변경하도록 하며, Bastion호스트의 Configuration의 변경을 지시하여 침입에 대한 대응을 할 수 있도록 한다.

침입 대응의 최상위 단계에서 공격자의 근원지를 찾는 역추적을 실시하여 관련 정보를 수집하고, 관리자의 개입을 기다리게 한다.

4) Dynamic Screened Zone Configuration : 최근 해킹 동향들을 확인하여 보면 IP 주소를 조작하여(IP spoofing, LAND Attack 등) 공격하는 기법들이 소개되고 있다[1][3]. 이 경우 공격자의 네트워크 정보나 위치 등을 정확히 찾을 수 없기 때문에 원천적으로 역추적이 불가능하게 된다. 따라서 네트워크 상의 데이터 통신 특성상 Bastion호스트의 Configuration을 재설정 시켜 주고 변경된 정보가 각 노드의 라우팅 테이블로 전파되는 과정에서 역추적을 시도하려고 한다. 또한 Configuration설정은 관리 시스템에 레벨별로 구성하여 외부 또는 내부 공격자가 감시 당하고 있다는 사실을 알아차리지 못하도록 한다.
5) 정책 Level : 각각의 영역마다 모니터링 정책 (12단계), 보안 정책 (12단계), 역추적 정책(4단계) Dynamic Screened Zone Configuration 정책(4단계)을 적용하며, 모니터링 정책과 보안 정책에서 위험 수준에 따라 역추적 정책이 적용된다.

5. 결 론

지금까지 다양한 침입 탐지 시스템이 연구되어 지고 있으나, 불법적인 공격으로부터 충분한 대응이 되지 못하고있다. 본 논문에서는 다음과 같은 장점이 있다.

1) 단일 시스템으로 호스트와 네트워크 두 영역 모두 침입 차단,탐지,대응을 수행할 수 있다.
2) 대부분의 시스템이 이동 에이젼트로 구현을 하기 때문에 시스템 및 네트워크 자원의 소모를 줄일 수 있고, 오버헤드를 최소화할 수 있다.
3) 각각의 정책 단위로 단계별로 해당 작업이 수행이 되며, 도메인 기반 침입탐지 시스템, 관리 시스템, 클라이언트용 Agent가 서로 협력하여 침입 차단, 탐지, 대응 작업 및 역추적을 수행한다.
4) 네트워크 상에서 방화벽의 위치에 Dynamic Screened Zone 기능을 추가함으로써 침입탐지 시스템과 방화벽의 통합을 시도하였다.
5) 도메인 기반 침입탐지 시스템에서 각각의 클라이언트에게 특정 보안 프로그램을 실행시키거나, 각 호스트 단위로 개인 침입 탐지 및 방지 기능을 수행 할 수 있도록 하였다.

참 고 문 헌

[1] Rebecca Bace, Peter Mell " Intrusion Detection Systems" , NIST Secial Publication on IDS.
[2] Ran Zhang, Depei Qian, Chongming Bao, Weiguo Wu, Xiaobing Guo, " Multi-agent Based Intrusion Detecton Architecture" , IEEE 2001
[3] 이정석, " Windows 해킹동향과 보안 대책" , 마이크로소프트 대구/경북 세미나, 2001.
[4] Kai Hwang, Muralidaran Gangadharan, " Micro-Firewalls for Dynamic Network Security with Distributed Intrusion Detection" , IEEE 2001.
[5] " 방화벽 FAQ" , 한국정보보호진흥원, 1996.
[6] D.Brent Chapman, Elizabeth D. Zwichy, " Building Internet Firewall" , O' reilly, 1995
[7] Eugene H.Spafford, Diego Zamboni, " Intrusion Detection using automous agents" , Computer Network, Elsevier Science, 2000.
[8] 이정석, 이성운, 유기영, " Designing a Active Network Infrastructore" , 정보처리학회, 2001.