분산 면역 시스템을 적용한 침입 탐지 시스템의 설계

정종근*, 김원필, 박상철, 김용호, 김판구, 이윤배
조선대학교 대학원 전자계산학과 멀티미디어시스템 연구실
e-mail:jkjeong@infoman.chosun.ac.kr

Design of Intrusion Detection System Distributed Immunity System

Jong-Kun Jeong*, Won-Pil Kim, Sang-Chul Park,
Yong-Ho Kim, Pan-Koo Kim, Yun-Bae Lee
Multimedia-System Lab., Dept. of Computer Science,
Graduate School, Chosun University

요 약

인터넷의 급속한 발전으로 빠른 데이터 전송이나 대용량의 데이터 전송이 현실화 되고 있다. 또한 신속한 정보 획득으로 인한 생활의 질적 향상은 물론 국가 경쟁력의 확보등을 이룰 수 있다는 긍정적인 효과가 있는 반면 인터넷의 확장으로 인한 시스템의 불법침입, 중요 정보 유출, 시스템 파괴·변경 등의 부정적인 사례들이 계속 증가하고 있다. 특히, 최근에 컴퓨터 시스템의 침해 사고가 국내·외적으로 빈번히 일어나고 있어, 이에 대한 대책이 절실히 요구되고 있다. 이와 같은 요구에 대비하고자 하는 대표적인 보안 대책으로는 암호화, 복호화 기술과 시스템 보안 기술등이 있다. 특히, 이러한 기술 중의 하나인 침입 탐지 기술은 침입 차단 기술과 함께 정보 시스템의 안전한 운영을 위해 필수적인 기술이라고 할 수 있다.

본 논문에서는 분산 시스템 환경에서 자연 면역시스템을 적용하여 실시간적으로 침입을 탐지하는 시스템을 제안한다.

1. 서론

네트웍 기반의 기술이 발전하고 그에 대한 의존도가 증가함에 따라 네트웍이나 컴퓨터에 대한 보안 문제는 사회적·경제적으로 큰 문제로 대두되고 있다. 이러한 컴퓨터 시스템에 대한 보안 문제에 대처하기 위해 정보시스템에 대한 불법 침입을 분석하고 탐지하는 기술인 침입 탐지 시스템(Intrusion Detection System : IDS)에 관한 연구가 활발히 진행되고 있다.

침입 탐지 시스템은 불법적인 침입으로부터 시스템을 보호하기 위해 침입을 탐지하고 이에 대한 적절한 조치를 취하는 역할을 수행한다. 침입 탐지 기술은 크게 오용 탐지(misuse detection)와 비정상 탐지(anomaly detection)으로 분류할 수 있다.

오용 탐지는 시스템에 대한 과거의 공격 패턴이나 취약점 등에 대한 정보를 저장한 다음 이러한 것들을 통해 시스템에 침투해 올 때 침입을 탐지하는 방법이다.

비정상 탐지는 시스템에 대한 정상적인 상태와 사용 프로파일(profile)을 만든 다음 여기에서 벗어나는 행위를 침입으로 간주하여 탐지하는 방법이다. 현재 이러한 탐지 방법들은 개별적으로 적용되지 않으며 두가지 방법을 통합한 하이브리드(hybrid) 형태의 침입 탐지 기술을 이용하고 있는 추세이다.

침입 탐지 시스템이 갖추어야 할 몇가지 필수 요건은 첫째, 탐지의 정확성이다. 정상적인 사용자일지

라도 침입 탐지 시스템에서는 조금이라도 정상 패턴에서 벗어나면 침입으로 간주하기 때문에 잘못된 판단을 내릴 수 있다. 반면에 새로운 기법의 공격 패턴이 나타났을 때 이를 정상이라고 간주하기 쉽다. 이러한 경우 전자에 비해 심각한 피해를 입을 가능성이 있으며, 지속적인 보안 대책의 수립이 필요하다.

둘째, 새로운 침입 유형의 변화에 대한 자체 학습 기능과 실시간적인 탐지 기능을 가져야 한다. 이와 같이 침입 탐지 시스템은 계속적으로 다양한 탐지 방법들과 모델들이 개발되고 있으나 네트워크의 복잡성, 시스템 자체의 버그, 보안에 대한 인식 부족 등으로 인해 아직까지 완전하지 못한 실정이다. 특히 정상 행위와 비정상 행위의 개념이 지속적으로 변화하기 때문에 비정상 침입 탐지 시스템이 오용 침입 탐지 시스템보다 구현하기에 어려운 점이 있다. 현재 구현된 대부분의 침입 탐지 시스템은 새로운 침입 패턴이 나타날 때 탐지해내지 못하는 오용 탐지 방법을 이용하고 있기 때문에 아직까지 알려지지 않은 새로운 공격 유형을 쉽게 탐지해 내지 못한다는 단점을 가지고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 침입 탐지 기술의 현황을 소개하고, 3장에서는 면역 시스템을 분산 침입 탐지 시스템에 적용하여 설계한다. 4장에서는 결론 및 향후 연구 방향에 대해 기술한다.

2. 침입 탐지 기술의 분류

침입 탐지 시스템은 특정 시스템에 불법적으로 접속하여 시스템을 사용, 오용, 남용하는 것을 감지하고 문제점을 해결하는 시스템이라고 정의할 수 있다. 침입을 탐지하는 방법은 침입 탐지 모델을 기반으로 하는 방법과 탐지 영역을 중심으로 분류하는 방법으로 나눌 수 있다.

2.1 모델 기반 침입 탐지 시스템 분류

2.1.1 비정상 탐지(Anomaly Detection) 모델

비정상적인(anomaly) 침입이란 컴퓨터 자원의 비정상적인(anomalous) 행위(behavior)나 사용(use)에 근거한 침입을 말한다. 예를 들면,한 사용자가 시스템내에서 항상 해오던 작업 외에 관리자 영역에 들어온다던지, 시스템 내의 중요 파일을 삭제하려고 시도하는 경우 올바른 로그인 이름과 패스워드를 사용한 정당한 사용일지라도 침입으로 경우를 들 수 있다. 대표적인 비정상적인 침입 탐지 방법을 들면 다음과 같다.

- 통계적인 방법(Statistical approaches)
- 특징 추출(Feature Selection)
- 비정상적인 행위 측정방법들(anomaly measures)의 결합
- 예측가능한 패턴생성(Predictive Pattern Generation)
- 신경망(Neural Network)

이들은 어떤 방법이나 매개체를 사용하느냐에 따라 분류하였을 뿐 본질적으로 비정상적인 침입을 탐지하는 목적은 같기 때문에 방법은 거의 유사하다. 이중에서 가장 많이 사용하는 방법은 통계적인 방법으로 과거의 경험적인 자료로부터 침입을 탐지하기 때문에 자료의 양이 많을수록 정확하게 침입을 탐지할 수 있다. 그 외의 방법들은 다른 방법이나 매개체를 사용하여 비정상적인 침입을 탐지할 수 있다는 가능성을 보이는 의의가 있을 뿐, 현실적으로 사용하기에는 많은 문제점을 가지고 있다. 이 방법들은 각기 독립적으로 사용하기보다는 각각의 방법의 단점을 보완하기 위해 서로 결합하여 사용하는 것이 현실적으로 더 유리하다.

2.1.2 오용 탐지(Misuse Detection) 모델

오용(misuse) 침입이란 시스템이나 응용 소프트웨어의 약점을 통하여 시스템에 침입할 수 있는 잘 정의된 공격 형태를 말한다. 예를 들면, finger나 sendmail의 버그를 통한 인터넷 웜(Worm)의 공격 형태가 오용 침입의 대표적인 경우라고 말할 수 있다. 대표적인 오용 침입 탐지 방법의 종류를 들면 다음과 같다.

- 조건부 확률(Conditional Probability)
- 전문가 시스템(Production/Expert System)
- 상태 전이 분석(State Transition Analysis)
- 키-스트로크 관찰(Keystroke Monitoring)
- 모델에 근거한 침입 탐지 (Model-based intrusion Detection)
- 패턴 매칭(Pattern Matching)

전문가 시스템은 IF - THEN - RULE에서 공격 패턴들에 대한 지식을 표현하여 Audit trail event와 일치하는 fact들을 탐지해 낸다.

모델에 근거한 침입 탐지 방법은 오용의 발생을

탐지하기 위해 공격 관련 특정 모델을 만들어 DB로 구축한 다음 특정 공격 패턴이 발생할 경우 이 DB를 참조하여 탐지한다.

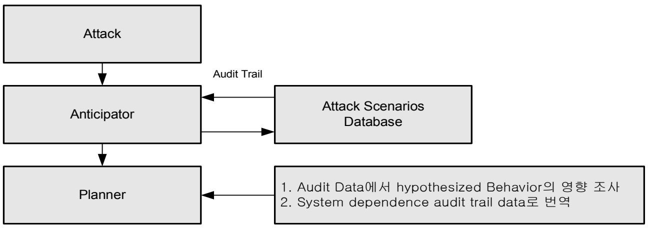

그림 2.1 모델에 근거한 침입 탐지

2.2 데이터 소스 기반 분류

단일 호스트로부터 생성되고 모아진 감사 데이터(audit data)를 침입 탐지에 사용하는 단일 호스트 기반(single host based)과 여러 호스트들로부터 생성되고 모아진 감사 데이터를 침입 탐지에 사용하는 다중호스트 기반(multi host based), 그리고 네트워크의 패킷 데이터를 모아 침입을 탐지하는 네트워크 기반(network based)으로 구분할 수 있다.

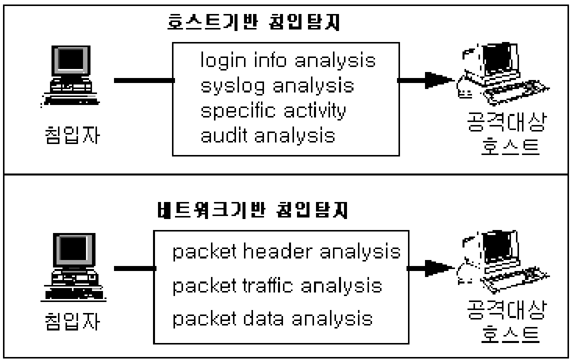

그림 2.2 데이터 소스 기반 분류

3. 분산 침입 탐지 시스템

3.1 면역 시스템

자연 면역 시스템은 여러 단계를 거처 방어 할 수 있는 다계층적인 방어와 한곳에서 탐지 하지 않고 여러 곳에서 탐지할 수 있는 분산 탐지 능력 그리고 새로운 공격 패턴이 나타났을 때 이를 민감하게 탐지하여 면역력을 갖추고 다른 호스트에도 면역력을 향상시킬 수 있는 특징을 가지고 있다.

특히, 새로운 유형의 공격 패턴이 출현했을 때 이 공격 정보를 여러 침입 탐지 호스트와 공유해 분산하여 대처할 수 있는 장점을 가지고 있다.

3.2 감사 데이터 분석

Anomaly detection과 Misuse detection에서 기본적으로 분석할 자료가 시스템 프로파일(profile)이다. 이러한 사용자의 로그 기록은 시스템 관리자에게 시스템 보안과 관련된 주요한 정보를 제공한다. 본 논문에서는 기본적인 로그 분석뿐만 아니라 종합적인 문제 분석까지 가능하게 하여 시스템의 부하를 최대한 줄이고 여러 개의 시나리오를 통해서 종합적인 분석 기능을 향상시켰다.

실시간으로 감사 데이터를 수집하기 위해서 4가지 시나리오를 작성하여, 수집된 감사 데이터를 분석한다. 시나리오의 구조는 다음과 같다.

- 시나리오 1 : 자신의 홈 디렉토리가 아닌 사용자의 홈 디렉토리에 불필요하게 드나드는 행위
- 시나리오 2 : 작업 내용을 은폐할 목적으로 일부 로그 파일을 삭제하는 행위
- 시나리오 3 : 처음으로 로그인 된 호스트로부터의 사용자가 중요한 파일을 파괴하는 행위
- 시나리오 4 : 잦은 로그인 실패한 사용자가 중요 파일을 파괴하는 행위

3.3 감사 데이터 표준화

지금까지 연구되어온 침입탐지 시스템의 감사 데이터 기법은 시스템 의존적인 특성을 지니고 있어서 분산된 이종의 환경을 지원하는데는 미흡한 점이 있다. 따라서, 본 연구에서는 감사 데이터 분석기에서 각각의 시나리오에서 수집되어 분석된 로그 데이터는 로그필터(log filter)를 이용해서 감사 데이터를 표준화하여 일관된 로그 감사 데이터 구조를 유지하게 하였으며, 생성 구조는 그림 3.1과 같다.

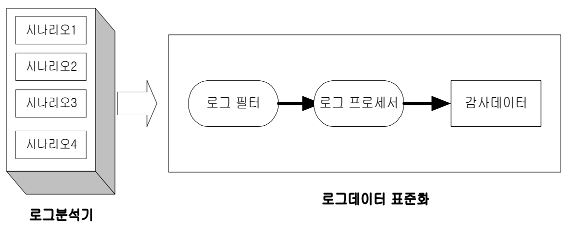

그림 3.1 로그필터를 이용한 감사 데이터의 표준형식 생성 구조

생성 단계는 각 운영체제의 로그 분석기에서 필요한 로그 정보를 수집한 다음, 로그 필터를 통해 로그 프로세서에서 필요로 하는 로그 필드만을 추출하고 로그프로세서에 의해 표준 형식으로 변환한다.

이때 로그프로세서는 침입 탐지 시스템에서 필요로 하는 감사 데이터를 표준화된 구조대로 생성하는 역할을 하게된다.

3.4 제안된 분산 침입 탐지 시스템 설계

분산 환경에서 실시간으로 침입을 탐지하기 위해서는 다중 호스트들을 대상으로 하는 침입 탐지에 대해 분석해야 한다. 하지만 각각의 호스트들이 독자적으로 침입을 분석하기 위해서는 침입 탐지 호스트의 부하가 심하게 되어 효율성이 떨어지게 된다. 따라서 본 논문에서는 인체 면역 시스템의 원리를 적용하여 하나의 호스트가 공격을 받거나 침입을 탐지하게 되면 분산되어 있는 모든 호스트에게 침입 경보와 침입 패턴에 대한 정보를 제공하여 자체적으로 그러한 정보들을 업데이트(update) 하도록 하였다.

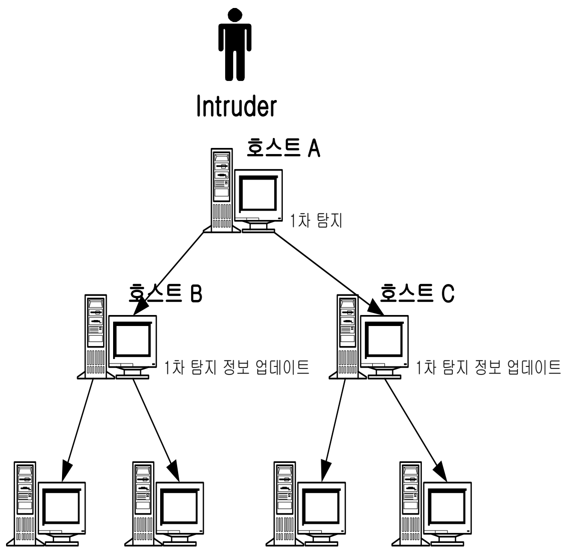

그림 3.2 분산된 계층 구조

이때 처음으로 침입 여부를 판단하는 침입 탐지 시스템 호스트는 계층 구조 상 맨 위에 위치하게 되어 다른 호스트들에게 정보를 제공해주는 서버의 역할을 하게 된다. 각각의 호스트들은 서로 독립적으로 탐지 활동을 하거나 동적으로 시스템에 추가되거나 삭제가 가능하며, 하나의 침입 탐지 호스트가 정보를 제공해주는 서버의 역할을 하게 되면 다른 호스트들은 잠시 클라이언트의 역할을 수행하게 된다.

4. 결론 및 향후 연구 방향

본 논문에서 제안한 분산 면역 시스템은 인체의 면역 시스템 원리를 응용하여 자체적으로 침입 정보에 대한 업데이트가 가능하게 하였고 분산되어 있는 침입 탐지 호스트와 정보를 공유하여 불필요한 업그레이드 과정을 줄일 수 있었다. 또한 감사 데이터 수집 단계에서 감사 데이터 양식을 표준화 함으로써 이종의 시스템간의 탐지나 정보의 공유가 원할하도록 하였다. 향후 연구 방향으로는 업그레이드 된 정보의 탐지 정확성 문제와 탐지율을 높이는 것과 사용자들의 행동 패턴을 자동으로 분석하여, 다음의 이벤트들을 예측하여 침입 탐지에 적용하는 방법에 대한 연구를 하는 것이다.

참고문헌

[1] 한국정보보호센터, 실시간 네트워크 침입탐지 시스템 개발에 대한 연구, Dec., 1998.
[2] 한국정보과학회 학회지, 침입 탐지 기술의 현황과 전망, Jan.,2000
[3] 한국정보처리학회 논문지, 컴퓨터 면역 시스템을 기반으로 한 지능형 침입탐지시스템, Dec., 1999
[4] Joseph Barrus "A Distributed Autonomous agent network Intrusion Detection and Reponse" Proc., 1988 Command and Control Research and Technology Symposium, Monterey CA, June-July 1998.
[5] Mark Crosbie and Eugene Spafford.. Defending a computer system using autonomous agent. In Proceeding of the 18th National Information System Security Conference, Oct 1995.
[6] S.Kumar and E.Spafford, A pattern matching model for misuse intrusion detection. Seventeenth National Computer Security Conference, Baltimore, MD, October 1994.
[7] Wenke Lee and Salvatore J.Stolfo, Data Mining Approaches for Intrusion detection, in Proceeding 7th USENIX security Symposium, January, 1998.
[8] S.Stolfo, A.Prodromidis, S. Tselepis, W. Lee, JavaAgents for Meta learning over Distributed Databases, in AAAI97 workshop on AI Methods in Fraud and Risk Management
[9] Neil C.rowe and Sandra Schiavo, An intelligent tutor for Intrusion Detection on Computer System, code Cs/rp, Department of Computer Science, Naval postgraduate school monterey, 1997