IDS를 위한 규칙 기반의 경보데이터 상관성 모델 설계

홍지연*, 엄남경*, 이상호*
*충북대학교 전자계산학과
lphjy@orgio.net, family8@netsec.cbnu.ac.kr, shlee@cbnu.ac.kr

Design of Rule-based Alert Correlation Model for IDS

Ji-yeon Hong*, Nam-kyoung Um*, Sang-ho Lee*,
*Dept of Computer Science, Chung-buk National University

요 약

기존의 IDS는 침입 가능성이 있는 데이터에 대해 많은 양의 경보데이터를 발생시키고 이를 모두 로그의 형태로 저장한다. 이 때 대량의 로그 기록이 생성되는데, 이 대량의 로그가 기록된 데이터는 관리자가 실제로 위협적인 침입을 식별하고, 침입 행위에 신속하게 대응하는 것을 어렵게 한다. 따라서 이 논문에서는 IDS가 발생시킨 대량의 경보데이터를 규칙 기반 방법론을 적용하여 침입탐지에 필요한 데이터만 추출하여 로그에 기록함으로써 관리자가 IDS 관리를 효율적으로 할 수 있는 모델을 제시한다. 이 모델은 실시간으로 갱신되는 규칙에 의해 경보데이터 중 불필요한 것은 제거하고, 유사한 것은 통합함으로써 신속한 침입 탐지를 가능케 한다.

1. 서론

침입탐지시스템(Intrusion Detection System: 이하 IDS라 함)은 일반적으로 컴퓨터 시스템을 악용하려는 모든 침입을 즉각적으로 탐지하여 분석하고 차단함으로써 허락되지 않은 사용자의 불법적인 사용을 막는 시스템이다[1]. 또는 IDS를 사용자 및 외부침입자가 컴퓨터시스템과 네트워크의 자원을 권한 없이 불법적으로 사용하기 위한 시도 또는 내부 사용자가 자신의 권한을 오용하여 권한 이외의 자원을 사용하기 위한 시도를 탐지하여 그 피해를 최소화하는 시스템이라 정의하기도 한다. 인터넷 등의 네트워크 환경에서의 불법 침입은 어떤 형태의 침입을 막론하고 정보자산에 상당한 피해를 입히며, 정보 저장을 컴퓨터에 의존하고 있고 인터넷 인프라가 구축된 오늘날 악의적인 침입이나 공격에 대비하는 것은 매우 중요하다.

IDS에서 발생시키는 경보데이터(alert)는 권한이 없거나 시스템에 적대적인 행위를 탐지하여 시스템, 응용 프로그램 및 데이터를 안전하게 유지하므로 이것들이 오용, 남용되는 것을 차단한다. 특히, 경보데이터를 통한 시스템의 실시간 감시 기능은 시스템이 위협을 받았을 때 관리자에게 이 사실을 알려주므로 정보가 도난 또는 분실되기 전에 관리자들이 조치를 취할 수 있다. 또한 관리자는 새로운 보안 정책을 설정 및 적용할 수 있는데 이 때 시스템과 데이터의 가용성 및 통합성은 계속 유지된다. IDS의 경보데이터는 사건 사후 분석을 위해 감사용 로그를 중앙에서 수집하고 안전하게 보관하는 기능도 제공한다. 그러나 IDS에서 경보데이터가 다량으로 발생함에 따라서 탐지된 경보데이터 가운데 침입의 실제 탐지에 사용되는 경보데이터를 구분해내는 데 다수의 시간이 소요된다. 따라서 관리자가 효율적으로 IDS를 운용하기 위해서는 우선 IDS로부터 탐지된 경보데이터 가운데 실제 분석에 필요한 경보데이터만을 추출해야 하며, 이 논문에서는 규칙 기반의 방법론을 적용하여 침입 탐지에 필요한 경보데이터만을 기록하는 모델을 제안하고자 한다.

이 논문의 2장에서는 IDS에 대한 정의 및 관련 연구 동향에 대해 기술하며, 3장에서는 본 논문에서 제시하는 규칙기반 처리 모델에 관하여 설명하고 있으며, 4장에서는 제안 모델의 세부 모듈에 관하여 설명하고 있으며, 5장에서는 기존방법과 이 논문에서 제안하고 있는 방법간의 비교 검토를 통하여 정당성을 입증하는 단계이며, 6장에서는 결론과 향후 연구 방향을 제시한다.

2. 관련연구

2.1 IDS

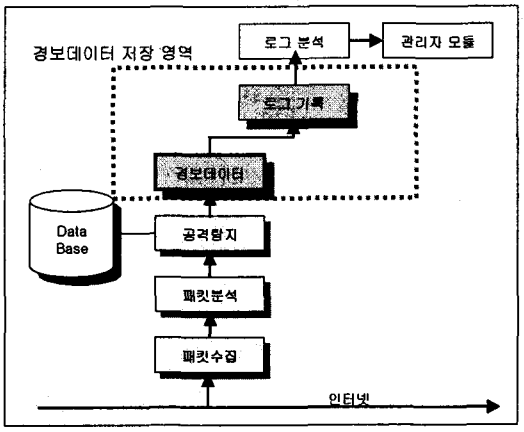
침입은 허가되지 않은 접근은 물론 컴퓨터 시스템의 보안 요소를 침해하는 모든 행위로 간주할 수 있다. 비밀번호 해킹을 통한 접근을 포함하여 실제적인 침입을 위한 포트 스캐닝(port scanning) 등 침입의 행위는 무한하다. 즉 침입과 침입을 위한 시도 등에 대해 보호하고자 하는 호스트나 네트워크에 대해 감시하고 실제 발견 시 경고 및 대응하는 행위를 침입 탐지라 할 수 있다. 또한 IDS는 보호하고자 하는 시스템으로부터 침입을 판단하기 위해서 데이터를 수집하고 중복되는 데이터나 쓸모없는 데이터는 필터링하고 침입 탐지 기법을 사용해 침입을 탐지하고 그에 상응하는 응답을 하는 시스템을 의미한다.

2.2 기존 IDS의 경보데이터 처리 구조

기존 IDS에서의 경보데이터 처리 구조는 [그림 1]과 같으며, 기본적인 모듈은 다음과 같다.

- 패킷 수집 모듈
- 패킷 분석 모듈
- 공격 탐지 모듈
- 경보데이터 발생 및 로그 기록 모듈
- 로그 분석 및 관리자 모듈

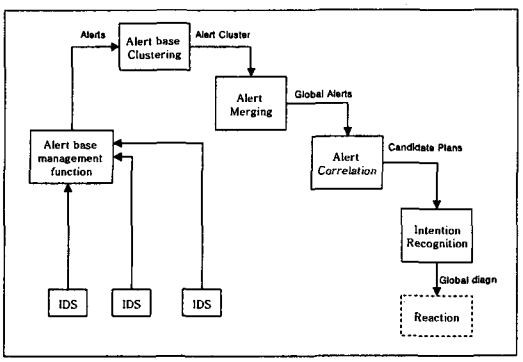
패킷 수집 모듈은 네트워크 상의 데이터를 수집하며, 수집된 패킷에 대해 전처리(preprocessing) 기능을 수행하는 패킷 분석 모듈이 있다. 이렇게 패킷 수집 및 분석 과정을 거친 데이터는 공격탐지 모듈로 이동하게 되는데, 이 과정에서 데이터베이스에 있는 침입탐지를 식별할 수 있는 데이터들과 비교 과정을 거쳐 침입 가능성이 있는 데이터에 대한 경보를 발생시키며, 경보에 대한 정보를 담고 있는 데이터를 경보데이터(Alert)라 할 수 있다. 이렇게 발생된 경보데이터는 로그 기록 모듈로 이동한다. 경보데이터들을 기록하는 로그에는 방대한 양의 경보데이터가 기록되며, 이 로그들은 로그 분석 과정을 거쳐서 관리자 모듈에서 실제적인 분석을 거치게 된다. 그러나 기존의 IDS에서는 이 과정에서 실제 침입과 관련 없는 경보데이터까지 다량으로 관리자에게 제공되므로, IDS 관리자가 침입을 정확하게 분석하고 발생한 침입에 대응하는 것을 어렵게 한다[2]. 따라서 [그림 1]에서 점선 부분으로 표시한 경보데이터 저장 영역의 과정을 개선하여 경보데이터가 대용량으로 저장되는 문제점을 해결할 수 있는 IDS 모델을 제안하고자 한다. 즉, 경보데이터 모듈에서 대량의 경보데이터를 규칙기반의 데이터마이닝 기법을 이용하여 감소시키고, 이렇게 정제된 경보데이터 만을 로그로 기록한다.



[그림 1] IDS의 경보데이터 처리 구조

2.3 관련 동향

[6]은 침입탐지 통합 모듈인 CRIM을 디자인하기 위해서 MIRADOR 프로젝트에서 행해진 연구이다. 이 통합 모듈은 경보데이터를 상관관계 짓고 병합하고 클러스터링 하는 함수를 구현했다. 실험을 통해서 이들 함수가 경보데이터의 양을 많이 감소시켰음을 보여주고 있다. 그러나 획득된 경보데이터는 보안 관리자가 관리하기에는 여전히 너무도 기본적인 것들이기 때문에 관리가 어렵다. 아래의 [그림 3]은 CRIM의 구조이다.



[그림 3] CRIM 구조

[7]은 침입탐지 콘솔을 구현하고 디자인 하는 부분에 집합 알고리즘과 상관관계 알고리즘을 적용한 논문이다. 이들 알고리즘은 경보데이터를 획득하는 것과 IDS의 보안 관점에서 상관관계를 통한 경보데이터 압축을 설명하고 있다.

3. 규칙 기반의 경보데이터 상관성

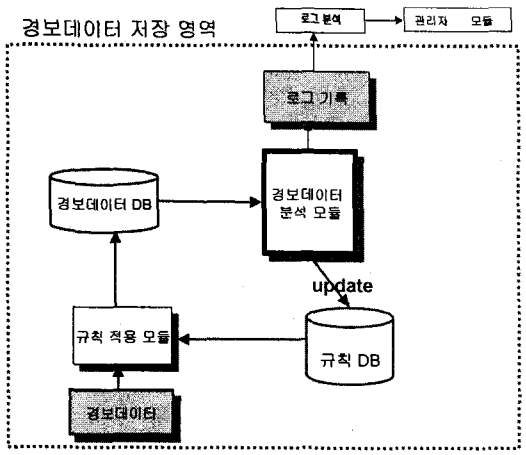
IDS에서는 침입 관련 행위가 탐지될 때, 대용량의 경보데이터가 발생하게 된다. 이 경보데이터가 모두 로그에 기록되면, 관리자는 실제 침입으로 예상되는 위협적인 경보데이터가 어떤 것인지 판단하기가 매우 어려워진다. 따라서 대용량의 로그 기록에서 관리자들이 경보데이터들에 관한 분석을 신속하게 해야만 위협적인 침입에 빠르게 대응할 수 있다. 제안하는 모델에서는 IDS에서 탐지된 다량의 경보데이터를 모두 로그에 기록하는 것이 아니라 일정한 규칙을 기반으로 감소시켜 저장하고, 침입탐지 경보데이터에 대한 상관관계 분석 알고리즘을 통하여 관리자에게 중요한 보안 관련 정보만을 정제하여 로그에 기록하는 모델을 제시한다. 정상적인 트래픽을 IDS가 공격이라 간주하여 경보데이터를 발생시키는 경우가 있다. *HTTP GET* 등과 같이 관리자에게 중요하지 않지만 계속해서 공격이라고 이벤트를 발생하는 경우에 대해서는 필터링(*filtering*) 기능을 수행한다. 또한 같은 시간대에 동일 호스트에서 발생된 경보데이터는 머징(merging) 기능을 수행한다.

즉, IDS에서 발생한 모든 경보데이터들을 로그에 기록하게 되면 관리자의 관리가 어려워지고, 신속한 대응이 이루어질 수 없기 때문에 필요한 경보데이터들만을 선별하는 과정을 거쳐서 통과한 경보데이터들만을 로그에 기록하는 규칙 기반의 필터링 및 머징 기능을 이용한다.

4. 제안 모델

4.1 전체 시스템 설계

제안하는 모델은 [그림 3]과 같다. 기존의 IDS에서의 처리구조를 나타내고 있는 [그림 1]의 경보데이터 저장 영역인 '경보데이터와 로그 기록' 간의 과정 사이에 대량의 경보데이터를 규칙기반으로 감소시킬 수 있는 과정을 추가한 시스템이다.



[그림 3] 전체 시스템 설계

[그림 3]에 제시하는 모델의 수행 순서는 같다.

- **1단계** : IDS에서 발생한 경보데이터들이 경보데이터 DB에 저장된다.
- **2단계** : 경보데이터 DB에 있는 경보데이터들을 이용하여 경보데이터 분석 모듈에서 규칙을 생성한다.
- **3단계** : 생성된 규칙들은 다음 단계에 이용되기 위해서 규칙 DB에 저장된다.
- **4단계** : 생성된 규칙들을 기준으로 규칙 적용 모듈은 IDS에서 발생하는 경보데이터들을 필터링한다.
- **5단계** : 규칙을 통과한 경보데이터들만이 로그 기록 모듈로 이동한다.
- **6단계** : 로그 기록 모듈에 기록된 경보데이터들을 가지고 로그 분석 한다.

4.2 주요 모듈 기능

[그림 3]에서 제시한 모듈 구조 중에서 경보데이터 분석 모듈과 규칙 적용 모듈을 적용하는 방법은 다음과 같다.

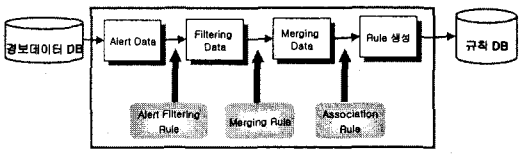
(1) 경보데이터 분석 모듈

중복하는 경보데이터들을 통합할 수 있으며, 불필요한 경보데이터를 제거하고, 근본 원인에 대한 정보를 획득할 수 있다. 또한 경보데이터들의 룰을 생성하는 역할을 한다.

- 적용 방법 : 학습(learning) 기능을 수행하는 모듈이다. 경보데이터 분석 모듈은 다음과 같은 기존의 데이터마이닝 기법을 적용하여 실행된다.
  - 분류
  - 연관 규칙
  - 순차 패턴
- 구성 : 구성 형태는 [그림 4]와 같다.

  경보데이터 DB의 경보데이터들을 이용해서 규칙을 생성하여 규칙 DB에 저장하는 과정이다.

  중복되는 경보데이터를 *Alert filtering Rule*을 기준으로 필터링하고, 필터링 된 경보데이터 중에서 유사한 데이터들을 *Merging Rule*을 기준으로 병합한 후 *Association Rule*을 적용하여 규칙을 생성하는 과정이다.



[그림 4] Alert Analyzer 구성

(2) 규칙 적용 모듈

경보데이터 분석 모듈에 의해 생성된 룰 집합을 바탕으로 새로운 경보데이터를 검사하는 역할 수행을 한다.

침입으로 예상되는 경보데이터들 간의 상관관계를 이미 생성된 연관 규칙을 적용하여 필터링한다.

5. 제안 모델의 평가

IDS는 많은 양의 경보데이터를 발생시키기 때문에 경보데이터가 플러딩(flooding)되는 경향이 있다. 그러나 제안하고 있는 방법에서는 중복되는 데이터를 필터링해서 로그에 기록하기 때문에 플러딩을 막을 수 있다.

[표 1]은 기존의 시스템에서의 경보데이터 처리 구조와 이 논문에서 제시한 모델에서의 방법을 비교 분석한 표이다. 즉, 기존의 IDS에서는 하나의 침입에 많은 양의 경보데이터를 발생시키는 경향이 있다. 이런 경우 유사한 종류의 경보데이터가 다량 발생하게 된다. 이에 반해 이 논문에서는 제안한 제안하는 방법에서는 경보데이터를 논리적으로 그룹화해서 유사한 종류의 경보데이터를 줄일 수 있다. 즉, 기존에는 침입에 대한 판단에 대해 false positive나 false negative와 같이 판단시의 오류를 범할 수 있는데, 제안 모델에서는 잘못 발생된 경보데이터들이 계속적으로 갱신 기능을 거치면서 규칙에 의해 필터링 되므로, 관리자에게 직접적으로 분석대상이 되는 로그가 감소됨을 알 수 있다. 또한 기존의 IDS에서는 대량의 경보데이터가 기록되는 로그에서 위협적인 경보데이터를 찾기가 어려웠지만, 제안하는 방법에서는 연관성을 적용해서 미리 세워진 규칙을 통해 경보데이터를 필터링 하기 때문에 시스템에 위협적인 경보데이터만이 로그에 기록된다.

[표 1] 기존 시스템과 제안 모델의 비교

평가기준	기존의 IDS	제안 모델
경보데이터 발생량	많은 양의 경보데이터를 발생시킴으로 인해 경보데이터의 플러딩 현상 발생	불필요한 경보데이터들을 제거
경보데이터 간의 통합	관련 있는 경보데이터들을 논리적으로 그룹화하기 어려움	유사한 경보데이터들을 통합
정확성	*false positive*나 *false negative* 등의 오류 생성	경보데이터가 들어올 때마다 규칙을 계속적으로 갱신하기 때문에 정확한 규칙 생성 가능
신속성	관리해야 하는 많은 경보데이터들을 해당 네트워크에서 위협적인 경보데이터인지를 확인할 필요 있음	상관관계 분석 알고리즘을 통하여 관리자에게 중요한 보안 관련 경보데이터만을 로그에 기록하기 때문에 신속한 침입 탐지 가능

6. 결론

이 논문에서는 IDS에서 발생한 다량의 경보데이터를 규칙을 기반으로 감소하는 모델을 제안했다. 즉, 중복되는 경보데이터들을 제거하고, 관련성 있는 경보데이터들은 통합하며, 규칙을 적용해서 이러한 경보데이터의 감소가 가능하다. 제안한 모델을 통해 IDS에서 발생시킨 침입 관련 경보 데이터에 대한 상관성 분석 방법을 통하여 관리자에게 중요한 보안 관련 정보만을 정제하여 통보해 주며 특정 경보데이터에 따른 자동 조치를 구현할 수 있는 환경을 제공하는 보안 관리를 할 수 있다. 경보데이터들의 상관성 분석을 통해 보안 문제 발생시 좀 더 쉽게 근본 원인에 대한 정보를 얻을 수 있으며, 신속한 대응이 이루어질 수 있다. 이러한 방법의 결과는 로그 기록에 모든 경보데이터가 기록되는 것이 아니라 위협적인 경보데이터들만을 로그에 기록하기 때문에 로그의 양이 많이 감소하며 관리자는 침입에 대해서 신속하게 대응할 수 있다. 따라서 IDS의 보안적인 측면에서도 효율성을 가진다.

향후에는 이 논문에서 제시한 시스템이 위협적인 경보데이터들을 더욱 신속하게 찾아낼 수 있는 방법론을 제시하고, 이를 입증하여 제안 시스템에 대한 효율성을 높이고자 한다.

참고문헌

[1] W. Lee, S. J. Stolfo. "Data Mining Approaches for Intrusion Detection", Columbia University, Computer Science Department, 20

[2] A. Valdes and K. Skinner "Probabilistic Alert Correlation" In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID) 2001

[3] Wenke Lee, Salvatore J. Stolfo, "Data Mining Approaches for Intrusion Detection*", Computer Science Department Columbia University 500 West 120th Street, New York, Ny 10027.

[4] A. Valdes and K. Skinner "Probabilistic Alert Correlation" In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID) 2001

[5] Tivoli Systems. TME 10 Enterprise Console, User's Guide, Version 3.7, November 2000.

[6] F. Cuppens, A. Miege, "Alert Correlation in a Cooperative Intrusion Detection Framework", In Proc. of the 2002 IEEE Symposium on Security and Privacy, May 2002

[7] H. Debar and A. Wespi, "Aggregation and correlation of intrusion-detection alerts", In Recent Advances in Intrusion Detection, number 2212 in Lecture Notes in Computer Science, 2001