韓國 OA學會 論文誌
第7卷 第4號, 2002. 12.

2002-7-4-3-3

보안정책 서버의 경보데이터 분석을 위한 데이터마이닝 엔진의 구현

정 경 자* 신 문 선**

Implementation of Data Mining Engine for Analyzing Alert Data of Security Policy Server

Kyeong-ja Jeong* Moon-sun Shin**

요 약

최근 네트워크 구성이 복잡해짐에 따라 정책기반의 네트워크 관리기술에 대한 필요성이 증가하고 있으며, 특히 네트워크 보안관리를 위한 새로운 패러다임으로 정책기반의 네트워크 관리 기술이 도입되고 있다. 보안정책 서버는 새로운 정책을 입력하거나 기존의 정책을 수정, 삭제하는 기능과 보안정책 결정 요구 발생시 정책결정을 수행하여야 하는데 이를 위해서는 보안정책 실행시스템에서 보내온 경보 메시지에 대한 분석 및 관리가 필요하다.

따라서 이 논문에서는 정책기반 네트워크 보안관리 프레임워크의 구조 중에서 보안정책 서버의 효율적인 보안정책 수립 및 수행을 지원하기 위한 경보데이터 관리기를 설계하고 구현한다. 경보 데이터 관리기는 데이터 마이닝 기법을 적용하여 경보 관리기나 고수준 분석기가 효율적으로 경보데이터를 분석하고 능동적인 보안정책관리를 지원할 수 있도록 한다.

Abstract

Recently, a number of network systems are developed rapidly and network architectures are more complex than before, and a policy-based network management should be used in network system. Especially, a new paradigm that policy-based network management can be applied for the network security is raised. A security policy server in the management layer can generate new policy, delete, update the existing policy and decide the policy when security policy is requested. The security server needs to analyze and manage the alert message received from server policy enforcement system in the

* 충청대학 컴퓨터학부 부교수
** 충북대학교 전자계산학과 박사과정

논문접수 : 2002. 9. 20
심사완료 : 2002. 11. 26

enforcement layer for the available information.

In this paper, we implement an alert analyzer that analyze the stored alert data for making of security policy efficiently in framework of the policy-based network security management. We also propose a data mining system for the analysis of alert data. The implemented mining system supports alert analyzer and the high level analyzer efficiently for the security.

Ⅰ. 서론

최근 인터넷은 모든 사람들에게 다양한 정보와 서비스를 제공받기 위한 창구로 사용되고 있다. 인터넷의 일반화 및 대중화로 기존에 오프라인으로 처리되는 기능들이 인터넷을 이용한 온라인 서비스로 변환되므로 많은 정보가 인터넷상에 노출되고 있다. 이러한 상황에서 네트워크 전반에서 보안의 필요성은 그 비중이 날로 증가하고 있다.

정책기반의 네트워크 관리는 네트워크 전반에 대해 일관된 정책을 수행하고 적절한 정책을 수립하며, 관리자의 요구에 대해 정책의 용이한 변경을 제공함으로써, 네트워크 전반의 중앙 집중적인 관리를 가능케 하는 메커니즘이다[4]. 네트워크 환경에서 동적으로 용이하게 네트워크의 운영 방침을 적용하여 효율적인 네트워크를 운용하는 것이 정책기반 네트워크 관리의 목적이다. 정책에 의해 운영자는 손쉽게 네트워크를 관리할 수 있으며 상세 구현과 상관없이 일관성 있고 통합적이면서도 이해하기 쉬운 네트워크의 관리를 가능하게 한다. 최근 네트워크 구성이 복잡해짐에 따라 정책기반의 네트워크 관리기술에 대한 필요성이 증가하고 있으며, 특히 네트워크 보안관리를 위한 새로운 패러다임으로 정책기반의 네트워크 관리 기술이 도입되고 있다.

또한 인터넷 위협에 대응하기 위한 네트워크 전반에 걸친 완벽한 관리 메커니즘이나 침입대응 시스템은 없으므로 인터넷 위협에 대한 네트워크 전반에 걸친 대응 메커니즘과 함께 실제 침입에 대응하기 위한 시스템의 개발도 침입 탐지 시스템을 중심으로 활발히 이루어지고 있다.

기존의 침입탐지 시스템 관련 연구들은 대규모의 하부구조를 지닌 네트워크에서의 정보 수집/분석이 각각 전담 시스템에서 수행되는 경우가 많았으며 또한 네트워크 기반 침입탐지 시스템이라 할지라도 갈수록 다양해지는 침입에 대해 능동적으로 대처하기에 어려움이 많았다. 따라서 최근 침입 탐지 시스템에 데이터 마이닝 기법을 적용하여 많은 양의 감사데이터를 효율적으로 분석하여 자동화된 침입탐지 모델을 구축하는 등의 연구가 활발히 진행되고 있다.

본 논문에서는 정책기반 네트워크 보안관리 프레임워크에서 보안정책실행시스템으로부터 보안정책서버에 보내어지는 경보데이터를 데이터 마이닝 기법에 의해 분석하는 경보 분석 데이터 마이닝 엔진을 설계하고 구현한다. 논문의 구성은 2장에서는 본 연구와 관련된 연구를 기술한다. 3장에서 데이터 마이닝을 이용한 경보 분석 데이터 마이닝 엔진의 설계 및 모듈 구조를 설명하며 4장에서는 경보 데이터 마이닝 처리과정과 구현된 시스템을 설명하고 적용한 결과를 분석한다. 마지막으로 결론 및 향후 연구로 구성된다.

Ⅱ. 관련연구

2.1 정책기반 네트워크 보안관리

정책기반 네트워크 보안구조(Policy-Based Network Management for Network Security: NS-PBNM)는 네트워크 보안을 위한 정책기반의 네트워크 관리 기법으로서 정책기반 네트워크 보안구조를 지칭한다.

정책기반 네트워크 보안관리의 프레임워크의 구성요소는 보안 정책을 생성하고 관리하는 PMT(Policy Management Tool), 보안 규칙에 따라 보안 행위를 결정하는 PDP(Policy Decision Point), 보안 규칙을 저장하는 PR(Policy Repository)과 보안 행위를 수행하는 PEP(Policy Enforcement Point)과 PDP와 PEP간의 보안 정책 전달을 위한 통신 프로토콜로 구성된다[5, 6].

네트워크 보안 정책을 위한 프레임은 정책기반 네트워크 보안 구조의 계층적인 구성을 가지며 적어도 두개의 계층으로 구성한다. 하나는 관리 계층에 해당하면 보안 정책 서버 시스템과 다른 하나는 실행 계층에 해당하는 접속점에서의 해킹 트래픽 감지 및 대응을 위한 침입탐지 기반의 보안정책 실행 시스템이다

정책기반 네트워크의 보안 정책 서버 시스템은 크게 PMT 블록과 PDP 블록, 보안정책 실행 시스템으로부터 전달된 경보를 처리하는 AM(Alert Manager)과 HA(High-level Analyzer)블록과 PR을 위한 디렉토리로 구성된다.

보안 정책 실행 시스템은 네트워크 접속점에서 입력

패킷에 대한 탐지와 분석을 제공하는 Sensor/Analyzer 블록과 보안정책 실행기능을 제공하는 PEP 블록으로 구성된다. 다음 [그림1]은 정책기반 네트워크 보안관리 의 구성 요소와 상호간의 관계를 나타낸 것이다.

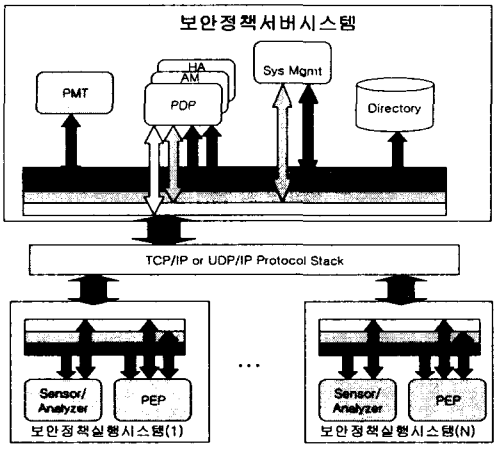

그림 2 정책기반 네트워크 보안관리의 프레임워크

2.2 침입탐지를 위한 기존의 데이터마이닝 기법

네트워크의 광역화와 새로운 공격유형의 발생으로 기존의 침입 탐지 시스템은 새로운 시퀀스의 추가나 수동적인 접근부분이 문제가 되고 있다. 침입 탐지 시스템은 정상 행위의 프로파일이나 공격 기법의 시나리오를 구축하기 위해서는 많은 양의 시스템과 네트워크 감사 데이터를 정확하고 효율적으로 분석해야 한다. 그러므로 최근에 침입 탐지 모델 구축에서 데이터 마이닝을 기법을 적용한 모델 연구가 많이 이루어지고 있다.

일반적인 침입 탐지 시스템을 위한 데이터 마이닝 프레임워크는 [그림2]과 같다[7,8,9].

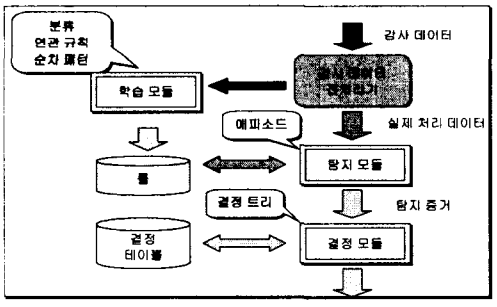

그림 3 침입탐지 시스템을 위한 데이터마이닝 프레임워크

[그림2]에서 학습 모듈은 침입 탐지 시스템의 룰을 생성하는 역할을 한다. 기존의 대량의 데이터로부터 정확한 모델을 계산하여 룰 집합을 생성한다. 생성된 룰의 방법론에 의해 탐지 모델이 결정되게 된다. 학습 엔진에 적용할 수 있는 데이터 마이닝 기법으로 분류, 연관 규칙, 순차 패턴 기법 등이 있다. 탐지 모듈은 학습 모듈에 의해 생성된 룰 집합을 바탕으로 하여 새로운 감사 데이터를 검사하는 역할을 수행한다.

이를 위하여 룰과 새로운 데이터에 대해 시퀀스 분석과 같은 기법을 적용한다. 결정 엔진은 탐지된 새로운 데이터를 결정 테이블에 의해 상응하는 결과나 대응 행동을 출력하는 역할을 수행한다. 이와 같이 기존의 침입 탐지 시스템의 수동적인 부분을 데이터 마이닝을 이용하여 자동화함으로써 정확하고 효율적인 시스템을 구축할 수 있다[10,11].

침입 탐지 시스템에서는 연관 규칙을 이용하여 감사 데이터의 속성 간의 상관관계를 분석함으로써, 침입 탐지에 적절한 시스템 특성의 선택하는 데 이용하거나, 사용자 프로파일이나 침입 행위의 패턴 생성을 위한 시퀀스 생성에 이용할 수 있다. 또한 순차패턴이나 빈발 사건 마이닝은 자주 반복되는 패턴을 탐지하고 이를 룰에 적용시키거나, 서비스 거부 공격의 지침으로 이용할 수 있다. 감사 데이터에서 정상 행위와 비정상 행위를 구분하기 위한 분류 기법을 적용할 수 있다.

Ⅲ. 경보데이터 분석을 위한 데이터마이닝 엔진

3.1 경보 데이터 분석기

보안정책 서버의 주요 기능 중 하나가 침입이 발생한 경우 보안정책 실행 시스템에서 보낸 경보 메시지에 대한 포괄적이고 광범위한 침입탐지 분석 및 대응 기능이다. 최근의 네트워크 공격은 사전 예측 및 정상 트래픽과의 구분이 어려우며, 그 피해 영역이 단순히 한 시스템이 대상이 아닌 네트워크 전체를 대상으로 하고 있다. 이와 같은 침입에 대응하기 위해서는 경보 데이터의 상관 관계를 분석하는 모듈이 필요하다[1, 2, 3].

[그림3]은 경보데이터 분석 모듈과 데이터 마이닝 엔진 등 시스템의 구성과 주변 모듈과의 상관 관계를 도식화 한 것이다[10,12].

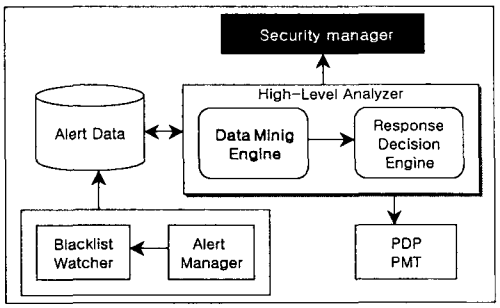

그림 4 경보시스템 구성 및 상관관계

경보 데이터는 Alert Manager에 의해 데이터베이스로 구축이 되고, 구축된 데이터베이스의 데이터는 경보데이터 분석기와 불량 사용자 및 호스트 관리기에 의해 분석되고 관리된다.

경보데이터 분석기는 경보 데이터의 상관 관계 분석을 위해 지능적인 분석과 탐지를 위해 데이터 마이닝 기법을 적용한 고수준의 분석 기능을 제공할 수 있도록 기존의 경보데이터 분석 모듈을 개선하였으며, 불량호스트와 불량사용자 관리는 데이터 마이닝 기법을 적용한 고수준 분석기에 포함되어 있다.

3.2 경보 데이터 분석 마이닝 엔진

경보데이터의 효율적인 분석을 위한 데이터 마이닝 기법의 적용한 경보 데이터 마이닝 엔진의 구조는 [그림4]와 같다.

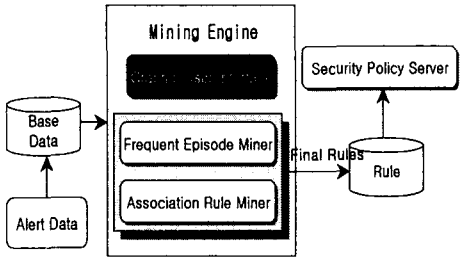

그림 5 경보데이터 마이닝 시스템 구조

[그림4]의 경보분석데이터 마이닝 엔진은 연관규칙마이너와 빈발 에피소드 마이너로 구성된다. 연관규칙 마이너는 레코드내의 속성간의 연관성을 탐사하고 빈발마이너는 레코드간 이벤트들의 패턴을 탐사하는데 사용되어진다. 또한 연관규칙마이너와 빈발마이너 모두 경보데이터의 특성을 고려하여 관심 있는 항목들만이 포함된 후보항목집합을 생성하도록 기존의 데이터 마이닝 알고리즘을 확장하였다. 즉 마이닝하고자 하는 항목들을 선택하여 관심 있는 항목들에 대해 융통성 있게 데이터 마이닝을 수행하도록 한다.

3.2.1 연관규칙 마이너

기존의 연관규칙 탐사 알고리즘은 트랜잭션 데이터 베이스를 사용하여 항목들을 그룹핑하여 연관성을 탐사하는 알고리즘이지만 이 논문에서 마이닝의 대상은 경보데이터로써 이는 트랜잭션 데이터베이스와는 개념이 다른 형태를 취하고 있기 때문에 Apriori 알고리즘에서 항목들간의 그룹핑은 하지 않고 연관성을 탐사한다[8,9].

또한 키항목(axis attribute)을 적용하여 관심 있는 항목들만을 가지고 규칙을 생성할 수 있다. [그림5]는 연관규칙 마이너의 수행단계를 보여준다. 확장된 알고리즘의 수행은 3단계로 이루어진다

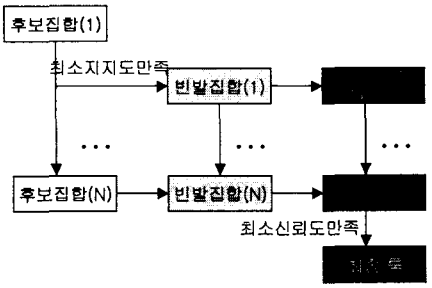

그림 6 연관규칙 마이너 생성 단계

1) 빈발항목 집합을 생성하는 단계

이 단계에서는 로딩된 테이블에서 관심 있는 속성들로 이루어진 항목들에 대해서 후보항목을 생성한 후 후보항목의 지지도(support)가 전체 레코드(D)에서 최소 지지도(minsupp)를 만족하는 후보항목에 대한 빈발 항목 집합을 생성한다. 이때 최소 지지도를 만족하지 못하는 항목들은 pruning 단계를 통해서 제거된다. 만일 항목집합 A, B에 대하여 A ? B이면, B를 지지하는 D 의 모든 항목들이 필연적으로 A 또한 지지하므로 support(A) = support(B)이다.

하지만, 항목집합 A 가 D에서 최소지지도에 미치지 못한다면, 즉 support(A) 〈 minsupp, support(B) =

support(A) 〈 minsupp 이기 때문에 A의 모든 상위집합 B는 빈발하지 않게 된다

2) 연관규칙을 생성하는 단계

이 단계에서는 pruning 단계를 거쳐 최소 지지도를 만족하는 항목들로 이루어진 빈발항목집합에 대해서 연관규칙을 생성하게 된다. 이때 빈발항목들간의 최소지지도를 가지고 최소 신뢰도(minconf)를 계산하여 연관규칙을 생성한다. 최소 신뢰도는 최소 지지도를 만족하는 항목에 대해서 얼마나 지지하는 지에 대해 예측하는 확률을 말하며, 빈발 항목에 대한 신뢰도 계산은 Conf(R) = p(X ⊆ D | Y ⊆ D) = p(X ⊆ D ∧ Y ⊆ D) / p(X ⊆ D) support (X U Y) / support(X) 으로 지지하는 항목에 대한 신뢰도를 구할 수 있다.

3) 최종 룰 생성 단계

이 단계에서는 이전 단계에서 만들어진 룰에 대해서 최소 신뢰도(minconf)를 만족하는 최종 룰, 즉 Conf(R) ≥ minimum confidence, 만을 생성하여 룰 테이블에 저장하게 된다.

위와 같이 3단계로 속성들간의 연관성을 마이닝 하여 많은 양의 감사데이터를 효율적으로 분석할 수 있으며 키 속성제약사항에 따라 관심 있는 속성들간의 연관성을 분석하며, 불필요한 룰의 생성을 줄일 수 있다.

3.2.2 빈발 에피소드 마이너

경보 데이터로부터 유용한 패턴을 찾기 위해 데이터 마이닝을 적용하는데 있어 기존의 알고리즘을 이용할 경우 속성들 간의 상관관계를 고려해야 하는 문제점이 발생한다. 경보데이터는 여러 가지 속성들로 이루어져 있으며 또한 각 속성들은 많은 값을 가지게 된다.

이 모든 데이터들을 binary 데이터베이스로 변환시킬 수 없기 때문에 이 논문에서는 row vector를 이용한 확장된 알고리즘을 제시한다. row vector라는 것은 빈발항목을 찾기 위해 사용되는 자료구조로써 아이템 집합이 포함된 트랜잭션을 기록한 비트를 포함시킨 것을 말한다. 이를 이용하여 속성들 간의 상관관계보다는 튜플들간의 상관관계만을 고려할 수 있다는 이점이 있으며 또한 기준속성을 적용함으로써 후보항목 생성 시 기준속성을 포함하고 있는 항목만을 고려할 수 있게 하였다.

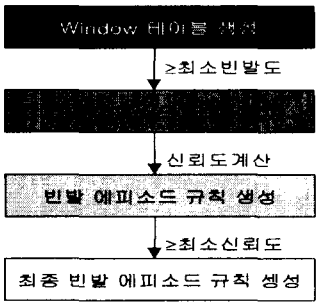

그림 7 빈발 에피소드 마이닝 수행과정

이는 규칙 생성 시 불필요한 에피소드 항목들이 많아지는 것을 줄일 수 있다. [그림6]은 빈발 에피소드 마이닝 수행과정을 나타내고 있다. 빈발 에피소드 마이닝은 다음과 같이3 단계로 나뉘어 마이닝을 수행한다.

1) 후보 에피소드 생성단계

이 단계에서는 로딩된 테이블에서 관심 있는 속성들로 이루어진 투플들에 대해서 주어진 time window 단위에 의해서 투플 들을 정렬한다. 윈도우 내의 time은 윈도우의 time 범위에 포함되어 있어야 한다. 즉, win = Te - Ts + width(w) , win_start time 〈= time 〈 win_end time 이다.

윈도우 단위로 정렬된 테이블을 가지고 후보 에피소드 집합을 생성하게 된다. 에피소드는 (V,≤,g) 노드들의 집합인 V와 V에 대한 부분 순서, 그리고 각 노드를 사건 형태와 연결하는 매핑인 g: V → E로 구성된다. 즉 g(V) 내의 사건들은 '≤' 에 의해 표현되는 순서대로 발생해야 한다.

에피소드 α가 이벤트 시퀀스 s 내에서 빈발하게 나타나면 모든 서브에피소드 β≤α 역시 빈발하게 나타난다. 후보항목 집합은 빈발한 작은 서브에피소드들로 구성 되어지며 이 것으로서 빈발하지 않을 수 있는 에피소드들에 대해 안전하게 제거할 수 있는 기준이 된다.

2) 빈발 에피소드 생성 단계

생성된 후보 에피소드 집합에서 최소빈발도(minimum frequent)를 만족하는 에피소드들을 추출하여 빈발한 에피소드집합을 한다. 에피소드들의 빈발도들에 대해서 신뢰도를 계산을 하게 된다. 에피소들에 대한 신뢰도 계산은 다음과 같이 구할 수 있다.

Conf(R) = p(X ⊆ D | Y ⊆ D)

$= p(X \subseteq D \wedge Y \subseteq D) / p(X \subseteq D)$

$\Rightarrow$ frequency (X U Y) / frequency(X)

3) 최종 에피소드 생성 단계

생성된 빈발 에피소드들로부터 최소 신뢰도(minconf)를 만족하는 빈발 에피소드를 생성해 낸다.

$\Rightarrow Conf(R) \geq minconf$

위의 단계로 마이닝을 수행함으로써 규칙 생성 시 불필요한 에피소드 항목들이 많아지는 것을 감소시킬 수 있다.

Ⅳ. 구현 및 적용

4.1 구현

구현 환경은 OS는 윈도우XP, 개발언어는 자바, 데이터베이스는 오라클8i를 사용하였다. 구현된 시스템은 사용자 인터페이스, 연관규칙 마이너, 빈발에피소드 마이너 등으로 구성된다. 먼저, 사용자 인터페이스 부분에서는 마이닝할 데이터를 선택하도록 되어 있다. 데이터베이스에 저장된 테이블중 마이닝을 수행할 테이블을 선택한 후 어떠한 속성값에 대해서 마이닝을 수행할 것인지를 선택한다.

이는 모든 항목을 대상으로 마이닝을 수행하지 않고 중요한 항목들에 대해서만 마이닝을 수행할 수 있도록 하기 위해서이다. 이렇게 특정 속성값을 선택함으로써 불필요한 많은 양의 후보항목집합을 줄일 수 있으며 또한 연관성 없는 항목들에 대한 연관규칙이나 빈발 에피소들 규칙을 줄일 수 있다.

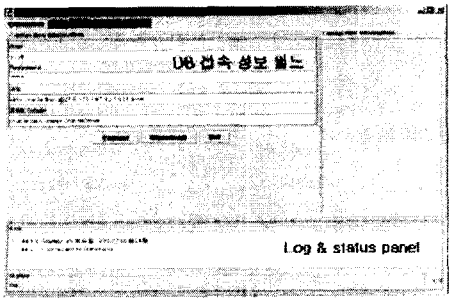

그림 8 사용자 인터페이스

[그림7]은 사용자 인터페이스 부분으로 연관규칙 마이너 탭을 선택하면 지지도와 신뢰도를 사용자가 입력할 수 있으며 관심 있는 항목 속성값을 선택한 후 마이닝을 수행할 수 있다. 또한 빈발에피소드마이너는 빈발도와 신뢰도 외에 타임윈도우의 값을 입력하여야 한다. 입력된 타임윈도우에 따라 최종 룰은 달라지게 된다.

4.2 적 용

이 절에서는 실제 경보데이터를 대상으로 마이닝을 수행한다. 경보데이터는 시뮬레이션 결과로 임의로 얻어진 데이터이며 [표1]은 저장된 경보데이터의 일부이다.

표 1 예제 경보 데이터

ALID	ATID	AT TYPE	DDATE	SCR_IP	DST_IP	SCR_PORT	DST_PORT	PROTO
1	50	7	2002-07-20 22:10:10	203.255.71.10	210.155.167.10	9158	21	TCP
2	50	6	2002-07-20 22:10:11	210.115.167.79	210.155.167.10	9159	21	TCP
3	50	5	2002-07-20 22:10:12	211.115.167.19	210.155.167.10	9160	21	TCP
...	..	...	..	..	..	..	..	..
3	50	5	2002-07-20 22:10:12	211.115.161.19	210.155.167	9160	21	TCP

이 경보데이터를 대상으로 연관규칙 마이너를 수행시킨 결과는 [그림8]과 같다. 또한 생성된 연관규칙 룰들의 의미를 정리하면 표2(a)와 같은 결과를 얻을 수 있다.

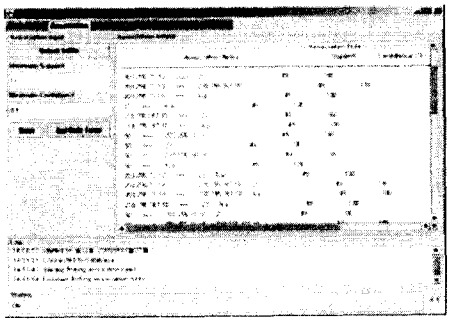

그림 8 연관규칙 마이너 실행 결과

또한 빈발 에피소드 마이너의 결과는 [그림 9]와 같으며 빈발에피소드 최종 룰의 의미를 정리하면 표2(b)와 같다.

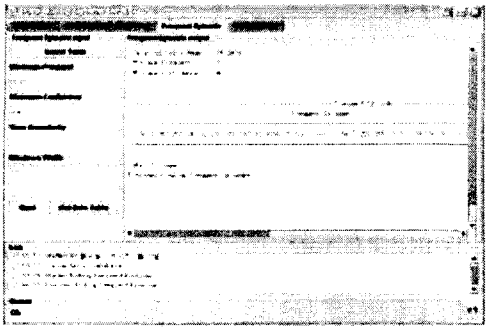

그림 9 빈발 에피소드 마이너 실행 결과

이러한 룰들은 지지도와 신뢰도에 근거한 신뢰성 정보라고 할 수 있다. 예를 들면 attack id가 50은 목적지포트번호 21번과 연관되어 있다는 것을 알 수 있다. 즉 연관규칙 마이너를 통해서 attack id속성과 destination port속성은 서로 밀접한 관계가 있다는 사실을 추출할 수 있다.

표 2 최종 규칙의 의미

Association Rule	Meaning
50<=>21 (supp : 49, conf : 100%,)	Attribute 50(Atid) correlated with attribute 21(dsc_port)
21<=>tcp (supp : 49, conf : 100%,)	Attribute 21(dsc_port) correlated with attribute tcp(protocol)
...	...

(a) 연관규칙

Frequent Episode Rule	Meaning
5001:210.155.167.10:21:tcp ⇒ 5007:210.155.167.10.21 :tcp (fre : 10, conf : 100%, time : 10sec)	If 5001(Ftp Buffer Ovrflow) occur, then 5007(Anonymous FTP) occur together.
...	...

(b) 빈발에피소드 규칙

또한 빈발 에피소드 마이너를 실행시킨 경우도 최종 규칙을 살펴보면 5001공격 다음에 5007 공격이 일어난다는 것을 알 수 있다. 이 실험에서 사용된 경보데이터는 단순한 시뮬레이션 데이터이다. 따라서 추가적으로 구현된 시스템의 성능을 평가하는 작업이 필요하다.

V. 결 론

본 논문에서는 보안정책 서버 시스템의 경보 데이터의 상관 관계를 분석하는 모듈을 구현하였으며 효율적인 분석을 위하여 데이터 마이닝 기법을 적용하였다. 침입탐지를 위해 적용되는 데이터마이닝 기법중 연관 규칙 마이너와 빈발 에피소드 마이너를 구현하여 경보데이터의 빈발 경보시퀀스분석과 빈발 공격시퀀스 분석에 활용하였다. 특히 경보데이터의 특성을 고려하여 관심 있는 항목에 대한 빈발 마이닝이나 연관규칙 탐사를 위하여 보안관리자가 마이닝을 수행할 항목을 경보데이터 테이블에서 선택할 수 있도록 하였다. 또한 침입에 대한 조기 대응이나 사전 방어를 위하여 유사 공격패턴을 분석하여 빈발공격 시퀀스중 유사한 패턴들을 클러스터링하여 동일 공격패턴으로 분류 할 수 있는지에 대한 연구가 진행 중이다. 또한 축적된 경보 데이터를 분석하여 네트워크 전체에 대한 포괄적인 침입탐지 기능을 제공하고 네트워크 전체에 대한 위험수준과 지역적인 네트워크에 대한 안전도 등을 판단하고 보안정책을 수립하기 위해 데이터 마이닝 기법을 적용하여 분석한 결과를 활용할 것이다. 이는 정량적인 임계치에 의한 경보데이터의 분석보다 효율적이고 능동적인 보안 정책 서버의 보안정책 구축을 지원하게 될 것이다.

참고문헌

[1] D. Schnackenberg, K. Djahandari, and D. Sterne,Infrastructure for Intrusion Detection and Response , Proceedings of the DARPA Information Survivability Conference and Exposition, SC, Jan. 2000.

[2] D.Schnackenberg, H. Holliday, R. Smith,

K. Djahandari, and D. Sterne, Cooperative Intrusion Traceback and Response Architecture (CITRA), DISCEX01, Anaheim, California, June. 2001.

[3] S. M. Lewandowski, D. J. Van Hook, G. C. OLeary, J. W. Haines, and L. M. Rossey, SARA: Survivable Autonomic Response Architecture, DISCEX01, Anaheim, California, June. 2001.

[4] IPHIGHWAY, Inc., Introduction to Policy-based networking and Quality of Service,

[5] E. Lupu and M. Sloman, Conflicts in Policy-based Distributed Systems Management, IEEE Transactions on Software Engineering, Vol. 25, No. 6, Nov. 1999.

[6] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, and S. Waldbusser, Terminology for Policy-Based Management, IETF ,July 2001.

[7] H. Mannila, H. Toivonen and A. I. Verkamo, "Discovery of frequent episodes in event sequences", Data Mining and Knowledge Discovery, 1(3), Nov. 1997.

[8] W. Lee, W. Fan "Mining System Audit Data: Opportunities and Challenges", College of Computing Georgia Institute of Technology Atlanta, GA 30332-0280, IBM T.J. Watson Research Center Hawthorne, NY 10532.

[9] W. Lee, S. J. Stolfo, K. W. Mok "A Data Mining Framework for Building Intrusion Detection Models"

[10] R. Heady, G. Luger, A. Maccabe, and M. Servilla. "The Architecture of a Network Level Intrusion Detection System", Technical report, University of New Mexico, Department of computer Science, Aug. 1990.

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

[12] H. S. Moon, M. S. Shin, K. H. Ryu and J. O. Kim "Implementation of security policy servers alert analyzer", ICIS, Aug. 2002.

저 자 소 개

정 경 자

1988 : 충북대학교 전산통계학과(학사)

1993 :충북대학교 전자계산학과 (석사)

1998.2 충북대학교 대학원 전자계산학과 졸업(박사)

1995~현재 충청대학 컴퓨터학부 교수

신 문 선

1988 : 충북대학교 전산통계학과(학사)

1997 : 충북대학교 전자계산교육(석사)

1999~현재:충북대학교 대학원 전자계산학과 박사과정재학