연관성 분석 시스템 평가를 위한 요구사항 분석

송준학[1O], 서정택[2], 이은영[2], 박응기[2], 이건희[1], 김동규[1]
[1]아주대학교 정보통신 전문대학원, [2]국가 보안기술 연구소
{jhsong°, dkdim, icezzoco}@ajou.ac.kr, {seojt, eylee, ekpark}@etri.re.kr

A Requirement Analysis on Evaluation of Correlation System

Junhak Song[1O], Jung-Taek Seo[2], Eun-young Lee[2], Eung-ki Park[2], Gunhee Lee[1], Dong-kyoo Kim[1]
[1]Graduate School of Information and Communication Ajou Univ. [2]National Security Research Institute

요 약

현재의 침입탐지 시스템의 문제점들을 개선하기 위해 침입탐지 정보의 축약기술 및 연관성 분석 기법들에 대한 연구들이 진행 중이다. 또한 최근에는 침입탐지 정보의 연관성 분석 시스템에 대한 효과성 검증에 대한 연구도 진행 중이다. 본 논문에서는 침입탐지 정보의 축약기술 및 연관성 분석 시스템의 효과성을 검증하기 위한 평가방안을 제안하였다. 즉, 침입탐지 정보의 연관성 분석 시스템에 필요한 기능 요구사항을 제시하고, 그러한 기능을 객관적으로 평가할 수 있는 방법으로 가중치 및 행렬에 의한 방법을 제안하였다.

1. 서 론

최근 몇 년 동안 침입탐지 시스템은 정보자산을 보호할 수 있는 핵심기술 중 하나로 인식되면서 광범위하게 운용되고 있다. 그러나 네트워크 규모가 방대해지고 인터넷상의 공격들이 점점 더 정밀화, 분산화, 대규모화 되어 가고 있는 상황 하에서 침입탐지 시스템은 탐지 결과를 통한 원인 분석에 있어 여러 가지 문제점을 노출하게 되었다[1].

첫째, 네트웍 규모가 방대해지고 트래픽량이 증가해짐에 따라 침입탐지 시스템이 생성해 내는 침입탐지 정보도 기하급수적으로 증가하였다. 이러한 대량의 침입탐지 정보를 축약이나 분석 절차 없이 그대로 전달됨으로써 관리자의 부담감을 가중시킨다.

둘째, 네트워크의 현 상황이나 새로운 공격 패턴에 대한 판단은 전적으로 관리자의 수작업에 의존된다.

셋째, 현재의 공격 기법들은 연관성을 갖고 진행된다. 그러나 침입탐지 시스템은 이러한 공격 패턴에 대해 연관성을 가진 하나의 공격으로 판단하지 못하고 다수의 공격이 개별적으로 발생했다고 판단한다.

이러한 문제점들을 해결하기 위해 침입탐지 정보 축약 및 연관성 분석 등의 분석 기법에 대한 연구가 진행 중이다. 그러나 이러한 분석 기법들은 아직 개념을 정립하는 단계에 있다. 또한 이러한 기법을 적용할 시스템이 효과성을 가질 것인가에 대한 검증 작업도 초기 수준이다[2].

침입탐지 정보의 축약 기술 및 연관성 분석 기법은 현재의 침입탐지 시스템에 대한 보완 기술이 될 것으로 전망된다. 이에 따라 이러한 기술을 적용한 시스템의 효과성을 검증할 수 있는 기법에 대한 연구가 중요하다. 또한 이러한 평가에 대한 연구는 앞으로 구현될 여러 연관성 시스템에 대한 객관적 평가에 기여할 수 있다.

본 논문에서는 현재까지 연구된 축약 기술 및 연관성 분석 기법을 적용한 시스템에 대해 효과성 검증을 위한 요구사항들이 무엇인지 알아보고, 그러한 요구사항들을 평가할 수 있는 방안으로 가중치 및 행렬에 의한 방법을 제안하고자 한다.

2. 연관성 분석 시스템

2.1 시스템 구조

단위 네트워크 내에 설치된 침입탐지 센서들로부터 정보들을 모아 연관성 분석을 수행하는 시스템 구조는 그림 1과 같다.

연관성 분석 시스템의 내부구조는 필터(Filter), 집합기(Aggregator), 상호 연관기(Correlator)로 이루어져 있다. 필터는 단위 네트워크 내에 설치된 침입탐지 센서들로부터 생성된 정보들 중에서 사전 정의된 추출 패턴에 기준하여 필요한 이벤트만 추출한다. 집합기는 필터로부터 받은 정보들을 모아서 상위 수준의 이벤트로 변환하는 기능을 한다. 상호 연관기는 집합기가 변환시킨 이벤트들에 대해 다양한 연관성 기법들을 통하여 관리자에게 축약 또는 의미 있는 정보로 변환시켜 전달하는 기능을 한다.

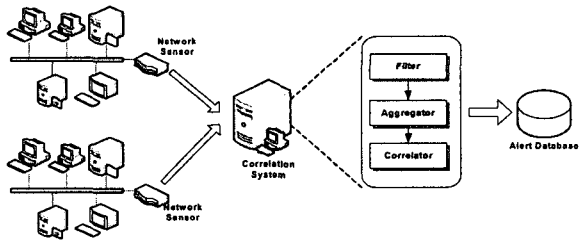

그림 1. 연관성 분석 시스템 구조

2. 2 연관성 분석 기법 및 시스템 적합성 연구동향

침입탐지 정보의 연관성 분석을 위한 기존 연구들은 데이터 마이닝 접근방법(Data Mining Approach), 확률적 접근방법(Probabilistic Approach), 시나리오 기반 접근방법(Scenario-based Approach), 우선순위 접근방법(Prioritization Approach)과 같이 총 4가지 범주로 나누어 살펴보고자 한다.

• 데이터 마이닝 접근방법 : 대용량의 데이터베이스에서 의미 있는 패턴과 규칙을 찾아내는 기법이다. 이 기법은 다양한 공격 유형 분석과 침입탐지 정보의 오류 긍정(False Positives)과 오류 부정(False Negatives) 데이터의 분석과 관리에 쓰일 수 있다. 데이터 마이닝 방법론으로는 분류(Classification)방법, 클러스터링(Clustering)방법, 연관규칙(Association Rules)방법, 빈도 에피소드(Frequent Episodes)방법 등이 있다. 이 기법의 한계점은 실시간으로 대량의 데이터 처리가 거의 불가능하다는 점이다[3].

• 확률론적 접근방법 : [4]에서 제안된 확률론적 접근방법은 특정 상황 하 완전히 일치하지 않더라도 최소한의 유사도가 보장되면 2개의 침입탐지 정보 간 연관성이 존재하는 것으로 판단하는 기법이다. 이러한 접근방법은 확률론적인 유사도를 분석하기 때문에 다른 분석방법보다는 유연성을 가질 수 있으나 실제 구현상에서는 성능상 한계를 드러내고 있다.

• 시나리오 기반 접근법 : [5]에서 제안된 시나리오 기반 접근법의 기본 개념은 침입탐지 센서들로부터 발생된 침입탐지 정보들 간의 인과관계를 분석하여 전체적인 공격 흐름을 관리자에게 전달하여 효과적으로 상황파악을 할 수 있도록 하는 기법이다. 즉, 발생된 침입탐지 정보에 대해 사전 침입탐지 정보들 간의 연계성을 정의한 지식 기반(Knowledge Base)를 통해 연계 경고(Hyper Alert) 인스턴스를 생성한다. 상호 연관 생성기(Correlation Engine)는 연계 경고 인스턴스를 이용하여 전체 공격 패턴 그래프를 생성한다.

• 우선순위 접근법 : [6]에서 제안한 우선순위 접근법은 침입탐지 정보에 대한 우선순위를 부여함으로써 관리자에게 침입공격에 대해 효과적으로 식별하고, 특정 침입정보에 관심을 가질 수 있도록 하는 기법이다. 즉, 어떤 종류의 공격에 관심을 가져야 할지 각 요소에 조건부 우선순위 테이블을 만들고, 현재 운용중인 시스템의 토폴로지 정보를 이용하여 탐지된 정보가 토폴로지 정보가 얼마나 관련성을 갖고 있는지 관련성 점수를 부여한다. 최종적인 우선순위 부여방법은 "Bayes Calculation"기법을 사용하여 조건부 우선순위 테이블, 관련성 점수 및 센서 출력 값을 종합하여 산출하게 된다. 이러한 기법은 침입탐지 정보에 우선순위를 부여함으로써 긴급성 부여 및 축약에 사용되어 질 수 있다.

[2]에서 제안된 연관성 분석 시스템의 적합성 평가에 대한 연구는 침입탐지 정보의 우선순위 부여, 침입탐지 정보들 간의 전후 관계 연계성, 다중 침입탐지 센서로부터 수집된 정보들의 분석 경우 세 가지 요소에 의한 행렬 방법으로 연관성 분석 시스템의 적합성을 보여 주었다. 또한 상위 계층에서의 결합된 침입탐지 정보들의 클러스터링, 잘못 결합된 침입탐지 정보의 처리, 평가요소의 제고 등의 추가적인 연구 과제를 제시하였다.

3. 연관성 분석 시스템 평가기준의 요구사항

연관성 분석 시스템 평가 기준을 위한 성능기능 요구사항은 우선순위 분석 능력, 침입탐지 정보들 간의 전후관계 분석 능력, 다중 센서 침입정보 분석 능력, 공격유형 클러스터링 분석 능력, 공격 받은 호스트 식별 능력, 오류 침입탐지 정보 축약 능력의 6가지 요구사항으로 이루어진다.

• 우선순위 분석 능력 : 연관성 분석 시스템의 우선순위 분석 능력은 침입탐지 정보를 분석하여 가중치에 의한 우선순위를 부여하는 능력이다. 침입탐지 정보의 우선순위에 따라 시스템은 클러스터링을 통한 축약도 가능하고 관리자는 중요도에 따라 공격에 대한 대응방법을 통제할 수 있다.

• 침입탐지 정보들 간 전후관계 분석 능력 : 침입탐지 시스템으로부터 발생된 각 침입탐지 정보들 간 전후관계를 통해 공격의 전체적인 형태를 분석해 내는 능력이다. 이러한 분석 결과는 관리자로 하여금 차후 공격 형태를 예측한다든가 대응방법을 구축하는데 도움을 줄 수 있다.

• 다중 센서 침입정보 분석 능력 : 최소한 서로 다른 두 개 이상의 침입탐지 시스템으로부터 침입탐지 정보를 종합하여 의미 있는 분석결과를 도출하는 능력이다. 이러한 분석 결과는 완전치 않은 침입탐지 정보들에 대해 여러 침입탐지 시스템으로 종합 분석함으로서 의미 있고 확실한 탐지 정보를 제공하는데 중요한 역할을 한다.

• 공격 유형 클러스터링 분석 능력 : 같은 공격 유형별로 분석하여 클러스터링 할 수 있는 능력이다. 이러한 클러스터링한 결과를 통해 관리자는 현재 공격 유형별로 대응방법을 통제할 수 있다.

• 공격 받은 호스트 식별 능력 : 관리자가 공격받고 있는 호스트의 정보를 알고자 할 때 의미 있는 정보를 제공해야 한다.

• 공격자 식별 능력 : 공격자에 대한 정보를 관리자가 알고자 할 때 적시성 있고 정확한 정보를 제공해야 한다.

• 오류 침입탐지 정보 축약 능력 : 침입탐지 시스템으로부터 발생된 오류 침입탐지 정보를 연관성 분석 시스템을 통해서 축약할 수 있는 능력이다. 연관성 분석 시스템이 축약한 오류 침입탐지 정보들은 침입탐지 시스템이 발생한 오류 침입탐지 정보들의 합보다 작아야 한다.

• 연관성 시스템 보고서(Report)의 표준화 : 연관성 시스템은 분석 결과를 보고서로 표현한다. 그러나 여러 연관성 분석 기법을 이용한 각 연관성 시스템들은 각기 다른 분석 보고서 형태로 표현함으로써 여러 연관성 시스템으로 나온 분석결과를 분석을 하거나 또 다른 연관성 분석 시스템에서 분석할 경우 문제가 발생하게 된다. 따라서 연관성 시스템 보고서에 대한 표준화 작업이 요구된다.

4. 연관성 분석 시스템 평가방법

연관성 분석 시스템 평가 방법으로 가중치 및 행렬에 의한 방법을 이용한 평가 방법을 제안한다.

평가방법으로 가중치와 행렬방법을 이용하는 목적은 세부 평가요소의 개발과 그 세부 항목의 중요도에 따라 가중치를 부여함으로써 여러 연관성 시스템을 평가 할 경우 항목별 점수화 부여로 객관화 평가를 하기 위해서 이다.

전체적인 평가방법은 공격 단위별로 연관성 분석 보고서를 통해 각 항목별 가중치 평가를 하게 되는데 각 항목 세부 요소별 가중치를 합산하여 전체 항목 행렬에서 전 항목을 합산하는 방식으로 이루어진다.

다음 아래는 공격 한 단계에 대한 여러 연관성 분석 시스템을 비교 분석한 예이다.

먼저 각 비교 항목에 대해 세부 항목을 개발하고 가중치를 부여한다. 아래 표 1은 "우선순위 분석능력"항목에 대한 가중치 부여 예이다.

항목 구분	세 부 항 목	가중치
우선순위 분석능력	① 공격 유형별 우선순위 표시	0.5
	② 보호해야 할 중요 자산별 우선순위 표시	0.3
	③ 우선순위에 따른 클러스터링 분석(IP, Port, 등)	0.1
	④ 우선순위와 클러스터링에 따른 대응방법 표시	0.1

표 1. 세부 항목별 가중치 부여(예)

그 다음 여러 연관성 분석 시스템에 대한 항목별 가중치 평가를 행렬로서 나타낼 수 있다. 여기에서는 우선순위 분석능력 항목에 대해서는 평가방법을 예로서 설명하겠다. 연관성 분석 시스템에 의해 제공되는 보고서 결과를 분석해 본 결과 우선순위 분석능력 항목에 있어 점수 결과는 아래와 같다.

- 분석 시스템 A(①②③항 분석) = 0.5+0.3+0.1 = 0.9
- 분석 시스템 B(①②항 분석) = 0.5+0.3 = 0.8
- 분석 시스템 C(분석사항 없음) = 0

이와 같은 방법으로 계산한 결과 항목별 가중치 합산 결과를 행렬 비교 방식으로 아래 표 2와 같이 나타낼 수 있다.

비교 항목	분석 시스템 A	분석 시스템 B	분석 시스템 C
우선순위 분석	0.9	0.8	0
이벤트 간 전후관계 분석	0	0.3	0.9
다중 센서 침입정보 분석	0.4	0	0
공격 유형 클러스터링	0.2	0.6	0.5
공격자 식별	0.8	0	0.6
공격 받은 호스트 식별	0.65	0.3	0.7
오류 이벤트 분석 축약	0	0.3	0.4
연관성 시스템 보고서 표준화	1	1	1
총 계	3.95	3.3	4.1

표 2. 항목별 가중치 합산결과 행렬방식 비교

이와 같은 평가 방법을 통하여 연관성 분석 시스템별로 탐지 및 분석 능력을 비교할 수 있는 수치화 제시가 가능하다. 또한 세부 항목에 대한 가중치 평가로 연관성 분석 시스템이 갖는 장단점을 분석해 낼 수 있는 장점이 있다. 반면 평가 세부 요소의 개발정도 및 가중치 부여 방법에 따라 평가 결과가 달라질 수 있으므로 이에 대한 객관적이고 타당성 있는 평가 요소 구성이 요망된다.

5. 결 론

본 논문에서는 연관성 분석 시스템 평가 기준의 요구사항과 평가방법을 제안하였다. 여기서 제안된 요구사항 및 평가방법은 현재까지 개발된 연관성 분석 기법을 토대로 제안되었으며, 완전한 분석 기법으로는 발전시키지 못하였다. 다만 장차 구현될 연관성 분석 시스템을 객관적이고 정확한 평가 할 수 있는 방법 구현을 위한 초기 연구로써 의미를 두고자 한다.

향후 연구과제로는 첫째, 연관성 분석 시스템에 대한 평가 기준의 각 항목별 세부 요소를 개발하고 정립 과정에 대한 연구가 필요하다. 둘째, 정립된 평가 기준에 따라 실험 평가를 통해 제안된 평가 방법이 타당한지 검증 작업이 필요하다.

6. 참고문헌

[1] 이수진 외 8명, "침입탐지 정보의 연관성 분석 시스템 설계 및 구현", 한국정보보호학회 동계 정보보호학술대회 논문집 Vol.13, No.2, p28, 12월 2003.

[2] Joshua Haines, Dorene Kewley Ryder, Laura Tinnel and Stephen Taylor, "Validation of Sensor Alert Correlators", IEEE Security & Privacy, Vol.1, No.1, pp. 46~56, January/February, 2003.

[3] Wenke Lee, Salvatore J. Stolfo, and Kui W. Mok, "A Data Mining Framework for Building Intrusion Detection Models", IEEE Symposium on Security and Privacy, 1999.

[4] A. Valdes and K. Skinne, "Probabilistic Alert Correlation", Fourth International Workshop on the Recent Advances in Intrusion Detection, Davis, USA, October 2001.

[5] Peng Ning, Yun Cui, and Douglas S. Reeves, "Constructing Attack Scenarios through Correlation of Intrusion Alerts", Proceedings of the 9th ACM conference on computer and communications security, pp. 1~35, November 2002.

[6] Philip A. Porras, et al, "A Mission impact-Based Approach to INFOSEC Workshop on the Recent Advances in Intrusion Detection", Zurich, Switzerland, October 2002.