침입경보 축약을 통한 규칙기반 연관관계 분석기 설계

이성호*, 김민수**, 노봉남*, 서정택***, 최대식***, 박응기***
*전남대학교 전산학과,
**전남대학교 리눅스보안연구센터,
***국가보안기술연구소
e-mail:shlee2@lsrc.jnu.ac.kr

Design of a Rule-Based Correlation Analyzer through Reducing Intrusion Alerts

Seong-Ho Lee*, Min-Soo Kim**, Bong-Nam Noh*,
Jung-Taek Seo***, Dae-Sik*** Choi, Eung-Gi Park***
*Dept of Computer Science, Chonnam National University
**Linux Security Research Center, Chonnam National Univ.
***National Security Research Institute

요 약

전통적인 호스트 기반 침입탐지시스템과 네트워크 기반 침입탐지시스템은 각각 로그 데이터나 패킷 정보에서 단일 공격을 탐지하고 침입경보를 생성한다. 그러므로, 기존의 침입탐지시스템들은 침입경보간의 상호연관성에 대한 정보가 부족하게 되고, 다수의 거짓 침입경보를 발생시킨다. 이를 해결하기 위해, 본 논문에서는 추론 규칙을 이용하는 침입경보 연관관계 시스템을 제안한다. 제안한 시스템은 침입경보 수집기, 침입경보 전처리기, 침입경보 연관관계 분석기로 구성되어 있다. 침입경보 수집기는 각 침입탐지시스템으로부터 필터링 과정을 거쳐 전송된 침입경보를 받아 침입경보 데이터베이스에 저장한다. 침입경보 전처리기는 불필요한 침입경보를 줄임으로써 침입경보 연관관계 분석의 효율성을 높인다. 마지막으로, 침입경보 연관관계 분석기는 추론 규칙을 이용하여 침입경보간의 상호연관성을 파악한다.

1. 서론

침입탐지시스템은 1980년대 초에 등장한 이후로 과거 20년 동안 많은 발전을 거듭해 왔다[1]. 초기의 침입탐지시스템은 침입행위의 특정한 패턴을 탐지하기 위해 간단한 규칙기반의 논리(logic)를 사용하기도 했으며, 적법한 행위를 확인하기 위해 과거의 행위 프로파일에 의존하기도 했다. 오늘날의 침입탐지시스템은 무엇이 침입행위를 구성하는가를 파악하기 위해 데이터 마이닝이나 기계학습 기법을 이용하기도 하며, 일반화된 패턴을 식별하고자 공격명세 언어를 사용하기도 한다.

공격자는 보통 침입하고자 하는 시스템의 취약점을 수집하고 분석한 후에, 침입을 시도한다. 전통적인 호스트 기반 침입탐지시스템과 네트워크 기반 침입탐지시스템은 각각 로그 데이터나 패킷 정보에서 단일 공격을 탐지하고 침입경보를 생성한다. 그러므로, 기존의 침입탐지시스템들은 침입경보간의 상호연관성에 대한 정보가 부족하게 되고, 다수의 거짓 침입경보를 발생시킨다.

이를 해결하기 위해, 본 논문에서는 추론 규칙을 이용하는 침입경보 연관관계 시스템을 제안한다. 제안한 시스템은 침입경보 수집기, 침입경보 전처리기, 침입경보 연관관계 분석기로 구성되어 있다. 침입경보 수집기는 각 침입탐지시스템으로부터 필터링 과정을 거쳐 전송된 침입경보를 받아 침입경보 데이터베이스에 저장한다. 침입경보 전처리기는 불필요한 침입경보를 줄임으로써 침입경보 연관관계 분석의 효율성을 높인다. 마지막으로, 침입경보 연관관계 분석기는 추론 규칙을 이용하여 침입경보간의 상호연관성을 파악한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로서 기존의 침입경보 연관관계 시스템에 대하여 기술한다. 3장에서는 규칙 기반 침입경보 연관관계 시스템을 제시하고, 구성 모듈에 대해서 기술한다. 마지막으로, 결론과 향후 연구방향을 기술한다.

2. 관련 연구

2.1 CRIM

CRIM은 MIRADOR 프로젝트 내에서 개발된 침입탐지시스템간의 협동 모듈이다[2,3]. 프랑스 국방연구소는 협동적이고 적응적인 침입탐지시스템 플랫폼을 개발하기 위해서 MIRADOR 프로젝트를 시작했다. 그림 1에서 보는 것처럼, CRIM은 다섯 개의 함수로 구성되어 있다.

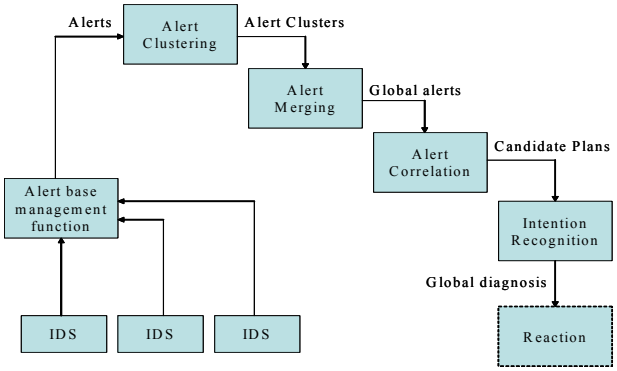

그림 1. CRIM 구조

침입경보 베이스 관리 함수는 여러 침입탐지시스템에서 생성된 침입경보를 IDMEF 형태로 받아 관계형 데이터베이스에 저장한다. 침입경보 군집화 함수는 데이터베이스에 접근하여 침입경보의 군집을 생성한다. 침입경보 군집화 함수는 동일한 공격에 해당하는 침입경보를 인지하고자 시도하고, 인지된 침입경보들을 유사도에 따라 군집에 포함시킨다. 각 군집은 침입경보 통합함수를 거친다. 각 군집에 대해서, 침입경보 통합함수는 각 군집을 대표하는 침입경보를 생성하거나 갱신한다.

침입경보 연관관계 함수는 보안 관리자에게 보다 더 통합적인 정보를 제공하기 위해 침입경보 통합함수에 의해 생성된 군집 침입경보(cluster alert)를 분석하고 연관시킨다. 결과적으로, 가능성이 있는 공격계획의 집합이 생성된다. 다음 단계의 공격의도 인지함수는 공격계획의 집합에서 공격계획을 하나씩 대입하여 실제 공격을 파악한다. 대응함수는 침입자에 의해 수행된 악의적인 행위들을 예방하기 위해서 시스템 관리자가 실시할 대응조치 중, 가장 최적의 것을 선택하도록 돕는다.

2.2 Hyper-alert Correlation Graph

노스캐롤라이나 주립대학의 Peng Ning은 침입경보 연관관계의 시각적 분석이 가능한 Hyper-alert Correlation Graph를 제안하였다[4,5]. 그림 2는 Peng Ning이 제안한 Intrusion Alert Correlator의 구조를 보여주고 있다.

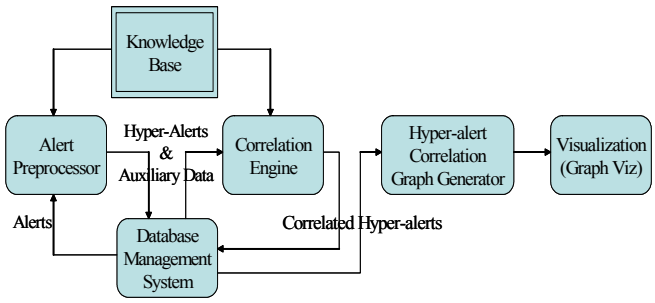

그림 2. Intrusion Alert Correlator 구조

침입경보 연관관계 분석기는 지식베이스, 침입경보 전처리기, 연관관계 분석 엔진, Hyper-alert Correlation Graph 생성기, 시각 컴포넌트로 구성되어 있다. 시각 컴포넌트를 제외한 다른 컴포넌트들은 모두 데이터베이스와 상호 작용한다. 프로그램은 자바로 개발되었으며, 데이터베이스를 접근하기 위해서 JDBC를 이용하였다. 시각 컴포넌트 개발에 들어가는 노력을 줄일 목적으로 GraphViz 패키지를 사용하였다.

3. 규칙 기반 침입경보 연관관계 시스템

그림 3은 본 논문에서 제안하고자 하는 규칙 기반 침입경보 연관관계 시스템의 구조이다. 제시된 침입경보 연관관계 시스템은 침입경보 수집기, 침입경보 전처리기, 침입경보 연관관계 분석기로 구성되어 있다. 침입경보 수집기는 각 침입탐지시스템으로부터 필터링 과정을 거쳐 전송된 침입경보를 받아 침입경보 데이터베이스에 저장한다. 침입경보 전처리기는 불필요한 침입경보를 줄임으로써 침입경보 연관관계 분석의 효율성을 높인다. 마지막으로, 침입경보 연관관계 분석기는 추론 규칙을 이용하여 침입경보간의 상호연관성을 파악한다.

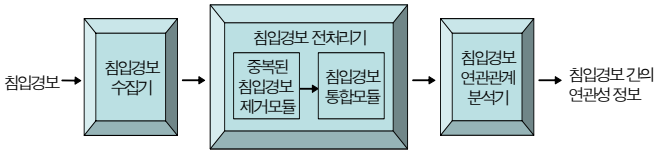

그림 3. 규칙 기반 침입경보 연관관계 시스템의 구성

3.1 침입경보 수집기

각 침입탐지시스템에서 받은 침입경보를 침입경보 데이터베이스에 저장한다. 침입경보 수집기는 확장이 용이하도록 에이전트와 매니저 구조를 하고 있다. 침입탐지시스템은 침입경보 메시지를 보내기 전에, 생성된 침입경보가 필터링 규칙을 만족하는가를 검사한다. 필터링 규칙은 보안 관리자가 관심을 갖고 보호해야 할 보호도메인에 대한 정보이다. 본 연구는 도메인 특성에 따라 보안 관리자가 필터링 규칙을 설정한다고 가정한다.

침입경보 수집기의 구조는 그림 4와 같다. 에이전트와 매니저 사이에 주고받는 메시지는 IDMEF(Intrusion Detection Message Exchange Format) 형태를 따른다. 따라서, 국제표준을 준수하는 침입경보 메시지는 모두 수집이 가능하다[6].

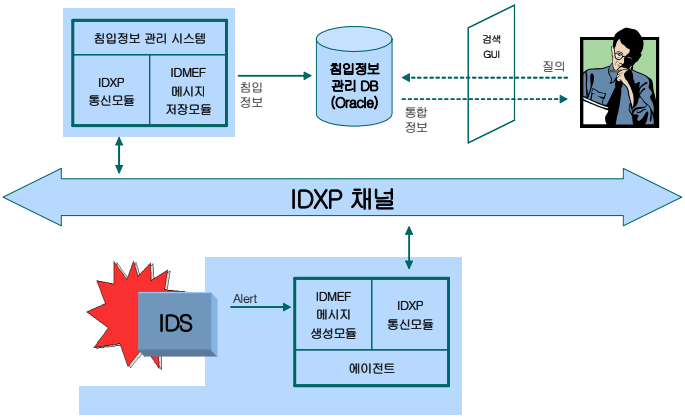

그림 4. 침입경보 수집기의 구조

추후 분석을 용이하게 하기 위해서, 본 연구에서는 IDMEF 메시지에 포함되어 있는 모든 정보를 저장하는 것이 아니라, 분석에 필요한 정보만 저장한다. 이는 침입경보 분석 과정에서 분석과 검색의 효율성을 향상시킨다. 저장되는 정보는 공격분류명, 공격분류 URL, 생성시간, 침입탐지시스템 식별자, 출발지 주소, 출발지 포트번호, 목적지 주소, 목적지 포트번호이다.

3.2 침입경보 전처리기

3.2.1 중복된 침입경보 제거

동일한 종류의 네트워크 기반 침입탐지시스템이 도메인 상에 여러 개 존재할 수 있기 때문에, 의심스러운 패킷마다 중복된 침입경보가 발생될 수 있다. 중복된 침입경보는 출발지 주소, 출발지 포트번호, 목적지 주소, 목적지 포트번호, 공격분류명이 같은 침입경보이다. 그림 5는 중복된 침입경보를 제거하는 알고리즘을 보여주고 있다.

```
deleteDuplicateAlerts( ) {
  Sort all the alerts by Creation time in ascending
order;
  for each alert
    Initialize Queue;
    for each alert among next ones within 1 minute
      if (Classification name, Source address, Source
port, Target address, Target port of these two alerts
are equal) then
        Put this alert into Queue;
      endIf
    endFor
    Delete all the alerts in Queue except the earliest
alert
  endFor
}
```

그림 5. 중복된 침입경보를 제거하는 알고리즘

3.2.2 침입경보 통합

한 공격에 대해 발생한 여러 개의 유사한 침입경보들을 하나로 통합하는 알고리즘은 그림 6과 같다.

```
mergeSimilarAlerts( ) {
  for each alert
    flag = 0;
    for each Queue in memory
      if (Creation time of this alert - time of Queue
> 30 seconds) then
        Create new tuple;
        Store this new tuple into DB;
        Free the Queue;
      endIf
    endFor
    for each Queue in memory
      if (the attributes of this alert and this Queue
are equal) then
        Put this alert into this Queue;
        Set Creation time of this alert to the time
of this Queue;
        flag = 1;
        break;
      endIf
    endFor
    if flag == 0 then
      Create new Queue;
      Set the attributes of this alert to this Queue;
    endIf
  endFor
}
```

그림 6. 침입경보 통합 알고리즘

3.3 침입경보 연관관계 분석기

본 컴포넌트는 취약점 정보를 수집하기 위한 공격과 침입공격 사이의 침입경보를 연관시킨다. 우리는 각기 취약점 정보를 수집하기 위한 공격과 침입에 해당하는 침입경보를 찾는다. 이를 위해, 우리는 침입경보 속성의 유사도를 이용하여 연관관계 데이터를 추출한다. 추출된 데이터에 대해 추론 규칙을 이용하여 추출된 연관관계 데이터의 유용성을 분석한다. 그림 7은 침입경보 연관관계 분석기의 구조를 보여주고 있다.

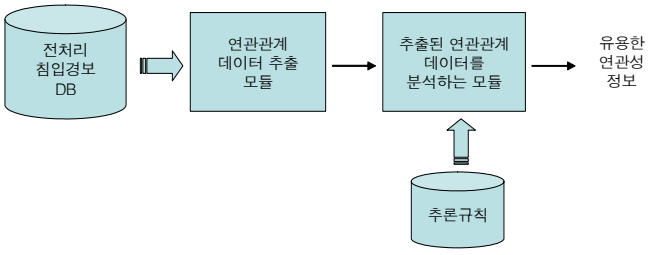

그림 7. 침입경보 연관관계 분석기의 구조

연관관계에는 두 가지 경우가 있다. 하나는 동일 목표에 대한 연속적인 공격을 연관시키는 것이고, 다른 하나는 동일한 침입자에 의한 공격들을 연관시키는 것이다. 연관관계 분석을 하기 위해서, 각각 목적지 주소와 출발지 주소를 이용하여 연관관계 데이터를 추출한다. 이렇게 추출된 데이터는 시간 순서대로 연결된다. 그림 8은 연관관계 데이터를 추출하기 위한 알고리즘을 보여주고 있다.

```
extractCorrelationData( ) {
  for each alert
    Initialize Queue1, Queue2;
    for each alert among next ones
      if (Target address of these two alerts are
equal) then
        Put this alert into Queue1;
      else if (Source address of these two alerts
are equal) then
        Put this alert into Queue2;
      endIf
    endFor
    Store correlation data in Queue1, Queue2 into
DB;
  endFor
}
```

그림 8. 연관관계 정보를 추출하는 알고리즘

4. 결론 및 향후 연구방향

본 논문은 규칙 기반의 침입경보 연관관계 시스템을 제안하였다. 제시한 침입경보 연관관계 시스템은 침입경보 수집기, 침입경보 전처리기, 침입경보 연관관계 분석기로 구성되어 있다. 침입경보 수집기는 필터링 과정을 거친 침입경보를 침입경보 데이터베이스에 저장한다. 침입경보 전처리기는 중복된 침입경보를 제거하고 유사한 침입경보를 통합한다. 침입경보 연관관계 분석기는 연관관계 정보를 추출하고, 추출된 연관관계 정보를 추론 규칙을 이용하여 분석한다. 향후에는 호스트 기반 침입탐지시스템과 보안 운영체제의 로그를 연관시켜 연관관계 기법을 발전시키고자 한다.

참고문헌

[1] N. Carey, A. Clark, G. Mohay, "IDS Interoperability and Correlation Using IDMEF and Commodity Systems", ICICS 2002, LNCS 2513, pp. 252-264, 2002

[2] F. Cuppens, "Managing Alerts in a Multi-Intrusion Detection Environment", In Proc. of Annual Computer Security Applications Conference (ACSAC 2001), Dec. 10-14, 2001, New Orleans, Louisiana

[3] 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

[4] P. Ning, Y. Cui, D. S. Reeves, "Analyzing Intensive Intrusion Alerts via Correlation", In Proc. of the 5th Int'l Symposium on Recent Advances in Intrusion Detection (RAID 2002), Oct 2002

[5] P. Ning, Y. Cui, D. S. Reeves, "Constructing Attack Scenarios through Correlation of Intrusion Alerts", 9th ACM conference on computer and communications security, pp. 245-254, Nov 18-22, 2002

[6] S. H. Lee, Y. C. Park, H. H. Lee, B. N. Noh, "The Construction of the Testbed for the Integrated Intrusion Detection Management System", In Proc. of 19th KIPS Spring Conference, Vol. 10, No. 1, pp. 1969-1972, May 16-17, 2003