한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

침해위협 상관분석 기반의 보안관제시스템 설계

정기문°, 박학수*
°*한국과학기술정보연구원
e-mail: {kmjeong, hspark}@kisti.re.kr

Design of a Security Monitoring System based on correlation analysis

KiMoon Jeong°, HarkSoo Park*
°*Korea Institute of Science and Technology Information

● 요 약 ●

최근 정보화가 고도화됨에 따라 해킹, 웜바이러스 등 사이버 침해사고 또한 증가하고 있다. 이에 따라 사이버 침해사고를 예방하고 대응하기 위하여 보안관제의 필요성이 대두되고 있으며 이를 지원하기 위한 시스템이 등장하고 있다. 단순한 사이버 공격을 탐지하는 수준에서 벗어나 분석 및 대응 등 넓은 의미의 보안관제 활동을 수행하기 위한 시스템은 이기종 환경에서 대용량의 데이터를 처리하여 신속하고 정확한 탐지 결과를 보여줄 수 있어야 한다. 또한 다양한 보안관제 활동을 원활히 수행할 수 있는 기능을 제공하여야 한다. 본 논문에서는 이러한 요구사항을 반영하여 대용량 보안이벤트 데이터를 동적으로 상관 분석하여 탐지 효율성과 신속성을 향상시킬 수 있는 보안관제시스템을 설계 제안한다.

키워드: 보안이벤트(security event), 상관분석(correlation analysis), 보안관제(security monitoring)

I. 서론

고도화된 정보화 사회에서 산업, 금융, 방송, 의료, 교통 등 사회적 기반이 되는 서비스를 제공하기 위해서 인터넷 이용이 증가하고 있다. 이러한 정보화는 편리함을 제공하기도 하지만 이에 따라 발생하는 해킹, 웜바이러스와 같은 사이버 공격 등의 역기능 또한 가파르게 증가하고 있다.

최근에 발생한 3.4 DDoS 해킹공격은 지난 2009년의 7.7 DDoS 해킹공격보다 진화된 형태로서 국가차원의 많은 피해를 유발했었다[1]. 이 뿐만 아니라 금융업종 및 정보서비스 업종 등에서 끊임없이 해킹 및 정보유출사고가 발생하고 있다. 이러한 사이버 침해사고를 예방하고 대응하기 위하여 다양한 대응 방안이 마련되고 있으며 그 중에는 네트워크분석 도구 등을 이용하여 24시간 서버와 네트워크에 대한 침입시도를 감시함으로서 해킹사고를 예방하고 즉각적으로 대응하는 방안 등도 생겨나게 되었다[2].

이러한 정보보안 활동을 보안관제라 하는데 협의적으로는 사이버공격을 단순히 탐지하는 활동을 일컫기도 하고 광의적으로는 탐지, 분석, 대응까지 포함하는 전반적인 정보보안 활동을 의미하기도 한다[3]. 이러한 보안관제를 위해서는 침입탐지시스템(IDS) 기반의 시스템을 통하여 네트워크 또는 호스트기반의 침해위협을 탐지하는 것이 기본이 된다. 하지만 단순히 침입탐지시스템 단일 장비만 가지고는 다양하고 고도화된 침입시도 등을 탐지하기 어렵게 됨에 따라 다수의 침입탐지시스템 뿐만 아니라 방화벽, 침입방지시스템(IPS) 등 다양한 정보보안시스템으로부터 데이터를 수집하여 이들 간의 관계를 분석하는 상관분석 기법이 등장하게 되었다[4].

다수의 장비 및 이기종 장비간의 상관분석을 위해서는 다양한 형태의 보안이벤트를 수집해서 침해시도 정보를 정확히 분석할 수 있는 기술이 요구되는데 이러한 연구는 활발하게 진행되고 있는 반면 대용량의 보안이벤트 데이터를 처리하면서 발생하는 성능문제에 대한 논의는 부족한 실정이다. 더군다나 단순한 침입탐지에 머무르지 않고 전반적인 보안관제 활동을 수행하기 위한 시스템에 대한 연구도 많이 진행되지 않고 있다. 본 논문에서는 보안관제 활동을 효과적으로 수행하기 위하여 이기종 다수의 보안시스템으로부터 수집된 보안이벤트를 동적으로 상관분석하여 보안관제에 활용할 수 있는 시스템을 제안한다.

II. 관련 연구

1. 상관분석 동향

보안이벤트 및 로그 등에 관한 상관분석 기술은 활발하게 연구되고 있다. 이에 대한 연구 동향을 살펴보면 [5]에서는 상관분석 기술을 보안침해사건탐지 영역, 위협관리영역, 위협인지영역, 포렌식 영역 등으로 분류하였다. 보안침해사건탐지 영역은 상관분석을 통해 오탐지율(false positive)를 제거하고, 미탐지율(false negative)을 보완하며 잠재적 위협(potential threat)을 탐지하기 위한 기술이 대상이 된다. 위협관리영역은 공격징후에 대한 가중

치 계산을 통해 우선순위를 결정할 수 있는 기능을 제공하는 기술을 의미한다. 위협인지영역은 대용량의 보안이벤트를 분석하여 현재의 현황을 즉각적으로 인지할 수 있도록 하는 시각화(visualization) 기능 등을 의미한다. 포렌식 영역은 네트워크 상의 모든 원시데이터 및 타 보안시스템의 로그 데이터를 수집, 분석하여 네트워크 남용, 내부자료 도난, 정책 위반 등을 파악하는 기술을 의미한다.

[6]에서는 사이버 공격시나리오를 미리 정하고 이와 연관된 보안이벤트가 발생하면 탐지하는 시나리오 기반(Scenario-based) 상관분석, 특정 규칙을 기반으로 사건의 선후 관계를 분석할 수 있는 규칙기반(Rule-based) 상관분석, 다수 보안이벤트의 통계적 특징을 분석하는 통계(Statistical) 상관분석, 보안이벤트에 대하여 시간 관계에 대하여 분석하는 시간(Temporal) 상관분석으로 분류하였다.

2. 보안관제 활동

보안관제는 단순 탐지뿐만 아니라 탐지된 결과에 대한 분석과 이에 대한 대응업무 등을 포함한다 각 영역별 활동은 다음과 같다[2].

- 사이버 공격 탐지 : 네트워크 상의 전체적인 트래픽 급증, 급감 및 내부정보를 절취하기 위한 해킹시도 및 악성 해킹프로그램 유포와 같은 사이버 공격시도를 실시간으로 탐지하는 활동을 말한다.
- 탐지결과 분석 : 경유지악용, 해킹메일유포, 홈페이지 위변조, 자료절취 및 훼손과 같은 해킹시도를 탐지한 뒤, 관련 로그정보 및 최신 해킹기술 등을 수집하여 공격자정보, 공격방법 등을 알아나고 피해규모를 파악하는 활동을 말한다.
- 대응 : 해킹 사실을 통보하고 분석단계에서 파악된 공격자정보와 취약점 정보를 활용하여 피해시스템이 정상적으로 운영될 수 있도록 신속하게 전문기술을 제공하며 재발방지를 위한 일련의 활동을 말한다.

III. 본론

1. 보안관제시스템 설계를 위한 요구사항

네트워크 상에서 침해공격 시도를 탐지하고 대응하기 위한 보안관제시스템을 설계하기 위해서는 기본적인 보안관제 활동을 수행할 수 있도록 하여야 하고 사이버공격을 탐지할 수 있는 기능이 강화되어야 한다. 이를 위해 다음과 같은 요구사항을 만족하여야 한다.

- 사이버공격을 탐지하기 위하여 방화벽, IDS, IPS 등 이기종의 다양한 보안시스템으로부터 보안이벤트를 수집할 수 있어야 한다. 또한 다양한 종류의 보안이벤트를 정규화하여 통합할 수 있어야 한다.
- 실시간 보안관제가 가능해야한다. 사이버 공격이 발생하기 이전에 보안이벤트를 탐지하는 것은 어려운 일이지만 공격의 전조나 공격이 발생한 이후라도 최단 시간 내에 보안이벤트를 탐지할 수 있어야 한다.
- 대용량데이터를 처리할 수 있어야 한다. 이기종 시스템의 보안이벤트를 수집하기 때문에 규모에 따라 다수의 기관에서 데이터를 수집하는 경우 대용량의 데이터가 수집되므로 이에 대한 처리가 가능하여야 한다. 이를 통해 보안이벤트에 대한 분석 시간의 지연이 발생하지 않도록 하여야 한다.
- 보안이벤트에 대한 상관분석이 가능하여야 한다. 일반적인 침입탐지시스템의 오탐지, 미탐지 등의 문제점을 해결하기 위해서는 수집된 이기종 보안이벤트 간의 상관분석이 가능하여야 한다.
- 보안관제 활동을 지원할 수 있어야 한다. 탐지기능 뿐만 아니라 분석 및 대응 활동 등을 포함하는 전반적인 보안관제 활동을 지원할 수 있는 기능이 있어야 한다.
- 보안관제 현황을 한눈에 파악할 수 있는 기능이 필요하다. 이러한 시각화된 화면은 상세한 현황 파악은 어렵지만 즉각적인 인지에 유리하다.

2. 보안관제시스템 설계

위에서 분석한 요구사항을 기반으로 보안관제시스템을 설계하였다. 제안하는 보안관제시스템의 개념도는 그림 1과 같다. 보안관제시스템은 수집모듈, 관제분석 모듈, 현황뷰어 모듈, 지원모듈로 구성된다. 수집모듈은 침해위협탐지시스템(TMS), 방화벽(F/W), 침입탐지시스템(IDS), 침입방지시스템(IPS) 등으로부터 보안이벤트를 수집하는 기능을 담당한다. 관제분석 모듈은 수집된 이기종의 데이터를 가공하고 실시간으로 상관 분석하는 기능을 수행한다. 현황뷰어 모듈은 분석된 보안이벤트 및 침해 이력 등의 현황 통계자료를 한눈에 인지할 수 있는 기능을 수행한다. 지원 모듈은 탐지, 분석된 정보 등을 처리하고 대응하는 업무 등 전반적인 관제활동을 지원하기 위한 다양한 업무를 처리하는 기능을 수행한다.

그림 1. 제안시스템 개념도
Fig. 1. Concept of Security Monitoring System

시스템을 구성한 모듈 중 관제분석 모듈은 대용량의 데이터를 대상으로 상관분석을 통해 침해위협을 탐지하는 보안관제시스템의 핵심 모듈로서 대용량 데이터를 실시간으로 처리할 수 있도록 메모리 기반으로 데이터를 처리하며 여러 프로세스를 동시에 처리하는 병렬처리 방식으로 설계하였다. 제안하는 보안관제시스템의 구조는 그림 2와 같다.

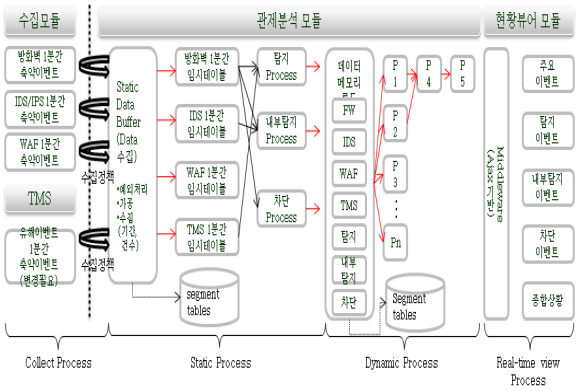

그림 2. 보안관제시스템 구조
Fig. 2. Architecture of Security Monitoring System

관제분석 모듈의 시스템 구조는 수집한 정보를 기본적으로 가공하는 Collect Process, 사전 정의된 상관분석 탐지 룰을 처리하는 static Process, 능동적인 상관분석을 지원하기 위한 dynamic Process. 처리된 데이터를 실시간으로 인지할 수 있도록 보여주는 Real-time view Process로 구성된다. 각 단계별 생성되는 데이터는 물리적 공간뿐만 아니라 메모리 버퍼에도 저장하여 상관분석 처리시간을 단축할 수 있도록 설계하였다. 또한 Static Prcoess와 Dynamic Process는 동시에 처리되도록 설계하여 성능향상을 도모하였다. 특히 제안시스템은 데이터의 관리 효율을 향상시키기 위하여 이벤트별 프로세스별 데이터 테이블을 세그먼트화 하였다.

3. 관제분석 프로세스

관제분석 모듈을 구성하고 있는 주요 단계별 프로세스를 상세히 살펴보면 다음과 같다.

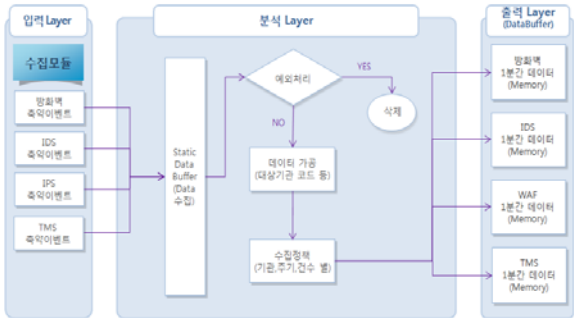

그림 3. Collect Process 구조
Fig. 1. Architecture of Collect Process

Collect 프로세스는 수집 모듈에서 수집되는 TMS, F방화벽, IDS, IPS 등 이기종 보안시스템의 보안이벤트를 ODBC를 통하여 관제분석 모듈의 Data Buffer 에 수집하는 역할을 수행한다. 이렇게 수집된 데이터는 메모리상에서 예외처리, 데이터 가공, 수집정책이 반영되도록 하는 과정을 거쳐 다시 새로운 메모리에 그 결과값을 저장할 수 있도록 하여 DB에 Insert 및 Select 하는 시간을 단축할 수 있도록 하였다.

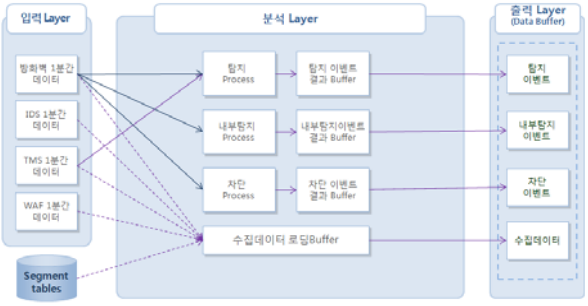

그림 4. Static Process 구조
Fig. 4. Architecture of Static Process

Static Process는 Collect Process에서 예외 처리되어 Data Buffer에 저장된 데이터를 사전 정의된 상관분석 탐지 룰인 탐지, 내부탐지, 차단 프로세스를 적용하여 그 결과를 메모리에서 처리하여 웹 서비스에 결과를 전송하고 Dynamic Process 기반 분석 데이터로 활용 가능한 상태로 유지하는 기능을 수행한다. 데이터 버퍼를 사용함으로써 데이터 입·출력 시간이 단축하여 성능을 향상시킬 수 있도록 하였다.

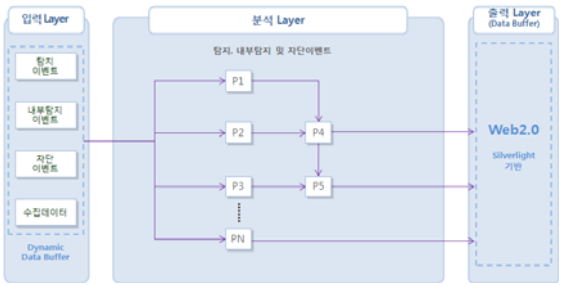

그림 5. Dynamic Process 구조
Fig. 5. Architecture of Dynamic Process

Dynamic Process는 상관분석을 위한 탐지 룰을 동적으로 생성하여 적용할 수 있는 기능을 제공 한다. 이는 사전 정의된 상관분석 룰로는 급변하는 사이버 공격을 탐지하기 어렵기 때문이다. Static Process를 통한 결과를 비롯하여 보안관제시스템에서 생성되는 모든 데이터를 활용하여 상관분석을 할 수 있도록 하였고 동적 탐지 룰 간의 상관분석 또한 가능하도록 설계하였다. 이를 통해 보안관제 탐지의 정확성을 향상시킬 수 있도록 하였다.

Ⅳ. 결론

우리는 본 논문에서 보안관제 활동을 수행하기 위한 상관분석 기반의 보안관제시스템을 제안하였다. 제안한 시스템은 이기종 환경에서 탐지의 정확도를 향상시키기 위하여 수집된 데이터를 규칙 기반 및 동적 분석을 수행할 수 있도록 설계하였다. 또한 대용량의 보안이벤트를 처리하기 위하여 메모리에서 데이터를 처리할 수 있도록 설계하였다. 제안한 보안관제시스템은 보안관제 업무를 수행하기위한 다양한 요구사항을 충분히 만족하는 것으로 기대되며 보안관제 업무의 효율성 증진에 기여할 것으로 보인다. 향후 본 논문에서 설계한 보안관제시스템을 구현하여 성능 및 효율성 등을 비교, 분석하는 연구를 추가적으로 진행할 예정이다.

참고문헌

[1] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20110307151006&type=det

[2] R. Bejtlich, “Tao of Network Security Monitoring, the beyond Intrusion Detection: What is Network Security Monitoring,” Addison Wesley Professional, pp. 40-41, July 2004.

[3] Young-Jin Kim, Su-yeon Lee, Hun-Yeong Kwon, and Jong-in Lim, “A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 19, No. 1, pp. 103-111, Feb. 2009.

[4] Robiah Yusof, Siti Rahayu Selamat, and Shahrim Sahib, “Intrusion Alert Correlation Technique Analysis for Heterogeneous Log,” International Journal of Computer Science and Network Security, Vol. 8, No. 9, pp. 132-138, Sep. 2008.

[5] S.H. Lee, H.C. Bang, B.H. Chang, and J.C. Na, “Security Event Processing for Effective Security Situation Analysis,” Telectronics and Telecommunications Trends, Vol. 22, No. 1, pp. 59-72, Feb. 2007.

[6] Reza Sadoddin, and Ali Ghorbani, “Alert Correlation Survey : Framework and Techniques,” Proceedings of the 2006 International Conference on Privacy, Security and Trust, Article No. 37, Oct. 2006.