

보안이벤트 연관관계분석 기반의 효율적인 보안관제체계 연구

이행곤*, 최상수*, 송중석*, 조기환**

요약

사이버 해킹 공격이 지속적으로 증가함에 따라 보안관제를 효율적으로 수행하기 위해서는 대량의 보안이벤트 중에서 가장 핵심적인 보안이벤트들에 대해서만 집중적으로 관제해야 할 필요가 있다. 본 논문에서는 백본 네트워크에 대한 보안관제를 기반으로 기 구축·운영 중인 각종 정보보호시스템들이 제공하는 보안이벤트를 수집하고 분류하여 상호 연관관계 분석을 수행하여 실제 보안관제요원들이 모니터링해야 하는 보안이벤트의 양을 최소화할 수 있는 보안관제 체계를 제안한다. 제안된 보안관제 체계는 각급 보안관제센터 구축 시 참고자료로 활용할 수 있을 것이다.

An Effective Security Monitoring Scheme Based on Correlation Analysis of Multiple Security Events

Haeng-Gon Lee*, Sang-Soo Choi*, Jungsuk Song*, Gi-Hwan Cho**

ABSTRACT

In order to cope with recent cyber attacks more effectively, it is needed to focus on only the significant security events from a large number of the original security events triggered by the security products such as IDS, TMS, etc. In this paper, we propose an effective security monitoring scheme which is able to collect and classify the security events provided by diverse types of the security products that are already deployed on the backbone network. In addition, the proposed scheme can contribute to the reduction of the security events that the security operators have to inspect. We expect that the proposed scheme can be used for reference model of the security centers to carry out incident response.

Keywords : Correlation Analysis, Security Events, Security Monitoring Scheme

* 한국과학기술정보연구원(✉hglee@kisti.re.kr)

** 전북대학교 컴퓨터공학과

· 제1저자(First Author) : 이행곤 · 교신저자(Correspondent Author) : 조기환

· 접수일(2012년 3월 15일), 수정일(1차 : 2012년 4월 13일), 게재확정일(2012년 4월 16일)

I. 서 론

인터넷의 발전과 함께 지식정보화사회에 진입하면서 정보와 지식은 가치 창출의 중요한 척도가 되었다. 따라서, 인터넷 상에 유통되는 방대한 양의 정보와 지식을 악의적으로 탈취하여 금전적 이득을 취하려는 해커들의 활동 또한 지속적으로 증가하고 있는 실정이다.

악의적 해커에 의한 사이버공격 시도가 급격하게 증가하면서 각급 기관에서는 각종 정보보호시스템을 도입·구축하여 침해사고 대응에 노력하고 있으나 정보보안 담당조직·인력 및 예산 확보 등의 어려움으로 24시간 실시간 모니터링·분석 및 대응과 같은 종합적인 침해사고 대응활동은 현실적으로 불가능한 실정이다.

따라서, 국가·공공기관을 중심으로 중앙집중형 보안관제센터를 설치하여 각급기관이 개별적으로 수행하기 어려운 보안관제 및 침해대응 활동을 지원하는 추세에 있다[1]. 일반적으로 중앙집중형 보안관제센터는 보안관제 대상기관의 백본 네트워크에 보안장비를 설치하여 실시간으로 보안이벤트를 수집하고 이를 토대로 보안관제 및 침해대응 지원 활동을 수행하고 있다.

그러나, 지속적으로 증가하는 사이버 위협 상황에 따라 발생하는 보안이벤트의 양도 기하급수적으로 증가하고 있기 때문에 신속·정확한 보안관제 활동을 수행하기 위해서는 발생하는 보안이벤트들 중에서 실제로 정보시스템에 피해를 줄 수 있는 중요한 보안이벤트를 선별해 내는 것이 중요한 문제점으로 대두되고 있는 상황이다.

이러한 문제점을 인식하고 다양한 연구자들이 보안이벤트 연관관계 분석에 대한 연구를 수행하고 있다 [2-8]. 그러나, 기존의 연구들은 단일 종류(예컨대, IDS)의 보안이벤트에 대한 연관관계 분석을 중심으로 하고 있기 때문에 다양한 정보보호시스템들이 제공하는 보안이벤트 정보를 효과적으로 활용하지 못하고 있다. 따라서, 다양한 정보보호시스템들이 제공하는 보안이벤트를 활용하여 백본 네트워크에서 탐지된 대량의 보안

이벤트들 중에서 중요한 보안이벤트만을 선별해 내기 위한 연구가 추가적으로 필요한 실정이다.

따라서, 본 논문에서는 기존 보안관제체계의 한계점을 분석하고 이를 효과적으로 개선하기 위하여 각급기관에서 기 구축·운영 중인 정보보호시스템의 보안이벤트를 추가 수집하여 백본 네트워크에서 수집된 정보와의 연관관계분석을 통해 중요 보안이벤트를 추출하는 방법을 제시하였다. 특히, 제안된 보안관제체계는 중앙집중형 보안관제센터의 신규 구축 및 고도화를 위한 참조모델로 활용될 수 있을 것으로 기대된다.

본 논문의 2장에서는 일반적인 중앙집중형 보안관제체계와 선행연구들의 한계점을 분석하고, 3장에서는 효율적인 보안관제체계 구성을 위한 접근방법, 추가 보안이벤트 수집 및 연관관계분석 방법을 제시하며, 4장에서는 제안된 보안관제체계를 기반으로 최근 3개월간의 데이터를 수집·분석함으로써 실효성 및 우수성을 입증하고 결론을 맺는다.

II. 관련 연구

2.1 일반적인 보안관제체계

대부분의 중앙집중형 보안관제센터에서는 그림 1과 같이 보안관제 대상기관의 백본 네트워크에 전용 보안장비를 설치하고 이를 통해 보안이벤트를 실시간으로 수집하여 침해대응 활동을 수행하고 있다.

기존의 보안관제체계는 다음과 같은 장점을 갖는다.

- ① 효용성 : 보안관제 대상기관 백본 네트워크에서 수집되는 전체 보안이벤트를 수집함으로써 보안관제 영역에 대한 전반적인 침해위협 동향 수집·분석이 용이하다.
- ② 일관성 : 전용 보안장비를 활용하여 보안이벤트를 수집하기 때문에 보안정책(탐지패턴) 개발·적용이 용이하고 이를 통해 일관성 있는 침해대응

활동을 수행할 수 있다.

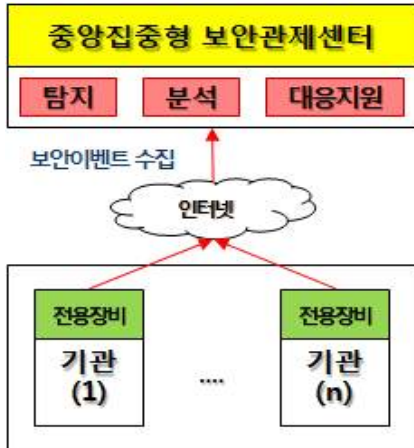


그림 1. 일반적인 보안관제체계
Fig. 1. Generic Security Monitoring Scheme

- ③ 신속성 : 해킹공격에 대한 사전징후 포착 시 전용 보안장비에 대한 보안정책 일괄적용이 용이하며, 동일한 구성이기 때문에 특정 기관에서 발생한 구조적 문제 또는 해킹사례를 분석하여 보안관제 영역 전반에 신속히 전파할 수 있다.

그러나, 해킹 기술의 진화와 함께 해킹 시도가 지속적으로 증가하면서 기존 보안관제체계는 다음과 같이 다양한 한계점을 보이기 시작하였다.

- ① 과부하 : 국내 중앙집중형 보안관제센터 중 하나인 과학기술사이버안전센터(S&T-SEC)는 과학기술 분야출연연구기관에 대한 보안관제를 수행하고 있다[9]. 과학기술사이버안전센터의 경우 그림 2와 같이 지난 1년간 월평균 약 1400만건의 보안이벤트가 수집되고 있으며, 이를 통계적으로 환산해 보면 1분당 최소 152건, 최대 595건, 평균 321건의 해킹 시도가 탐지된 것으로 분석되고 있다. 특히, 보안관제요원이 평균적으로 1분당 321건의 보안이벤트를 모니터링하고 특이 동향에 대

한 상세분석 후에 대응지원을 수행하는 것은 현실적으로 매우 힘든 일이다. 따라서, 실제 탐지·분석 및 대응지원 활동까지 연계되어 사고처리 건수는 1일 평균 5건 내외에 머물고 있다. 이러한 사고처리는 전적으로 보안관제요원들의 노하우와 전문성에 의존하고 있는 실정이다.

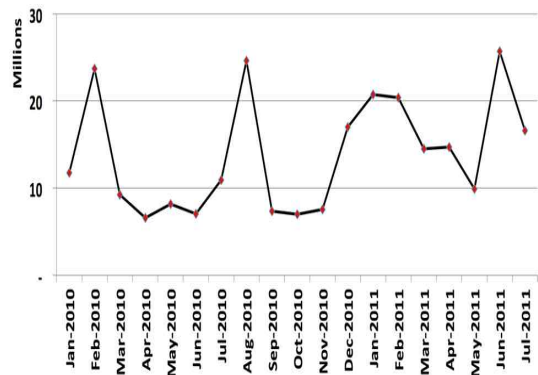


그림 2. 과학기술사이버안전센터의 보안이벤트 탐지 건수
Fig. 2. Detected Security Events by S&T-SEC

- ② 정확성 : 각급 기관에서는 자체적으로 침해사고 대응활동을 수행하기 위하여 다양한 정보보호시스템(방화벽, IDS/IPS, WAF 등)을 구축하여 운영하고 있다. 이러한 정보보호시스템들은 벤더사에서 제공하는 최신 보안정책을 적용하여 해킹 시도에 대하여 적절히 탐지·차단하는 기능을 제공한다. 따라서, 기존 보안관제체계와 같이 백본 네트워크 상에서 탐지된 보안이벤트 중 상당수는 차단되고 있을 가능성이 매우 크다. 특히, 과학기술사이버안전센터에서 최근 2년간 사고처리된 내역 중에서 전체의 55%(약 1,900건)이 자체 정보 보호시스템에 의해 차단된 것으로 분석되어 정확성 측면에서의 문제가 심각한 것으로 나타났다.
- ③ 미탐 : 보안관제 대상기관 내부에서 내부로의 해킹 시도는 탐지할 수 없는 문제(False Negative)

가 존재한다. 즉, 백본 네트워크에 진입하지 않는 내부 네트워크 내에서의 악성행위는 현재 보안관제체계에서는 탐지할 수 없기 때문에 악성코드 감염에 따른 좀비PC의 악성행위(내부 네트워크 스캔 및 감염시도 등)에 대해서는 무방비 상태라 할 수 있다.

2.2 보안이벤트 연관관계 분석 동향

위에서 언급한 문제점들을 해결하기 위하여 다수의 연구자들이 보안이벤트 연관관계 분석에 관한 연구를 수행하고 있으며, 기존 연구의 대부분은 TMS(Threat Management System)나 IDS(Intrusion Detection System)와 같은 정보보호시스템이 발생시킨 보안이벤트들 중에서 중요하지 않은(오탐) 보안이벤트를 필터링 하거나 보안이벤트들 간의 연관관계 분석을 통해 보다 위험하다고 판단되는 보안이벤트만을 추출하기 위한 연구가 주를 이루고 있다[2-8].

T.Bass 등은 차세대 IDS의 성능을 향상시키기 위해서 군(軍)용 어플리케이션에 대한 데이터 융합 기술을 소개하였다[2]. Yu 등은 IDS 보안이벤트 자체에 대한 분석 및 보안이벤트 간의 연관분석을 수행하기 위한 프레임워크를 제안하였으며, 신뢰도 스코어를 활용한 실험결과는 제안된 프레임워크가 보안이벤트에 대한 false positive를 줄이는데 기여할 수 있을 뿐만 아니라 공격자의 침입과정을 보다 알기 쉽게 분석하는데 유용하다는 것을 보여주었다[3]. Giacinto 등은 사이버 공격에 대한 일원화된 설명정보 및 사이버 침해위험에 대한 고차원적 통찰력을 제공하기 위하여 보안이벤트에 대한 클러스터링을 수행하였다[4]. Treinen 등은 보안이벤트 스트림으로부터 알려진 공격패턴을 추출하기 위하여 메타-보안이벤트 개념을 도입하였으며, 학습시간을 줄이기 위하여 『연관규칙』과 같은 데이터 마이닝 기술을 사용하였다[5]. Song 등은 보안이벤트로부터 현재 알려져 있지 않은 신·변종 사이버 공격을 탐지하

기 위한 클러스터링 및 일반화된 통계치 추출 기법을 제안하였다[6,7]. 또한 Song 등은 보안이벤트에 대한 오탐율을 줄이기 위하여 교토대학교 허니팟에서 수집한 침해위험 트래픽 데이터와 보안이벤트들 간의 연관 분석을 수행하였다[8].

상기와 같이 기존 연구들이 보안이벤트를 효율적으로 관리하고 활용하기 위한 방법들을 제시하였지만, 기존 연구의 대부분은 각급 기관의 네트워크 인입 지점(또는 네트워크 내 단일 지점)에 배치되어 있는 정보보호시스템이 탐지한 단일유형의 보안이벤트에 대해서만 적용이 가능하다는 문제점이 존재한다. 하지만 최근에는 다수의 사이버 공격이 각 조직의 외부뿐만 아니라 내부에서도 발생하고 있기 때문에, 내부에서 내부로의 사이버 공격에 대해서는 대응이 어렵다는 한계점이 있으며, 각급 기관은 자체적으로 여러 유형의 정보보호시스템(IDS/IPS, TMS, firewall, anti-DDoS, WAF)을 서로 다른 네트워크상에서 배치·운용하고 있기 때문에, 이러한 여러 유형의 보안이벤트를 활용하여 그들 간의 연관분석을 실시하고 그 결과를 실시간 보안관제에 도입·적용함으로써 정확성과 신속성을 더욱 향상시킬 수 있을 것이다.

III. 개선된 보안관제 체계 제안

본 장에서는 백본 네트워크에서 보안관제 범위 내의 전체 보안이벤트를 수집·분석하는 기존 보안관제체계의 한계점을 효과적으로 개선시킬 수 있는 연관관계 분석 기반의 보안관제체계를 제안한다.

3.1 접근 방법

일반적으로 사이버공격은 “알려진 공격”과 “알려지지 않은 공격”으로 구분할 수 있다. 또한, 이러한 공격들은 각종 정보보호시스템에 의해 탐지·차단되어 해당

시스템에 영향을 미치지 않을 가능성이 존재한다. 이러한 상황들을 보안관제의 관점에서 정리하면 그림 3과 같이 4개의 영역으로 구분할 수 있다.

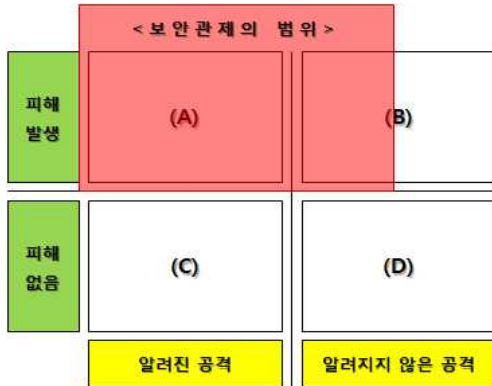


그림 3. 보안관제 범위
Fig. 3. Security Monitoring Scope

- ① A 유형 : 잘 알려진 공격으로 보안장비에 의해 탐지가 가능하지만 실제 정보시스템에 영향을 미칠 수 있는 유형이다.
- ② B 유형 : 알려지지 않은 공격으로 정형화된 보안장비에 의해 탐지가 매우 어려우며 실제 정보시스템에 영향을 미칠 수 있는 유형이다.
- ③ C 유형 : 잘 알려진 공격으로 보안장비에 의해 탐지 및 차단이 가능하여 정보시스템에 영향을 미치지 않는 유형이다.
- ④ D 유형 : 알려지지 않은 공격으로 정형화된 보안장비에 의해 탐지 및 차단이 매우 어려우나 실제 정보시스템에 영향을 미치지 않는 유형이다.

일반적으로, A와 C 유형은 패턴 기반의 침해대응 기술을 적용하고, B와 D 유형은 행위 기반의 침해대응 기술을 적용하여 보안관제를 수행하는 것이 효과적이다.

보안관제 영역을 선택하는 것은 효율적인 침해사고 대응을 위하여 매우 중요한 일이다. 특히, 국내외 대부분의 중앙집중형 보안관제센터들은 패턴 기반의 침해

대응 기술을 중심으로 보안관제 활동을 수행하기 때문에 본 논문에서는 패턴 기반의 침해대응 기술을 활용한 효율적인 보안관제체계 개선에 초점을 맞추고자 한다. 이러한 배경에서 패턴 기반의 보안관제에서 발생하는 대량의 보안이벤트를 효과적으로 축소시키고 중요 보안사고에 대한 침해대응에 초점을 맞추기 위하여 본 논문에서 고려한 상황들은 다음과 같다.

- ① 행위기반의 보안관제 기술은 본 논문의 연구범위를 벗어나기 때문에 B와 D 유형은 고려 대상에서 제외하였다. 단, 복수개의 패턴들에 대한 연관관계 분석을 통하여 일정부분은 탐지가 가능할 수 있다.
- ② 사이버공격 중에서 보안장비에 의해 성공적으로 차단된 이벤트(C 유형)는 실시간 보안관제에서 무의미하기 때문에 제외하였다.
- ③ 가장 중점적으로 보안관제를 수행해야 하는 부분은 보안장비에 의한 사전차단이 어려운 사이버공격(A 유형)이다. 따라서, C(일부 D 포함) 유형의 공격을 사전 필터링 함으로써 대부분의 무의미한 보안이벤트 숫자를 획기적으로 줄일 수 있다.

3.2 보안이벤트 수집 방법

보안관제 대상기관의 백본 네트워크에서 수집되는 보안이벤트를 중심으로 무의미한 이벤트를 필터링하여 중요도가 높은 핵심 보안이벤트에 대한 집중 보안관제를 수행하기 위해서는 다양한 유형의 보안이벤트를 추가적으로 수집하여야 한다.

일반적으로 패턴 기반의 정보보호시스템들이 생성하는 보안이벤트는 다음과 같이 2가지로 분류된다.

- ① 차단 이벤트 : 미리 정의된 보안정책을 기반으로 침해위협 시도를 실시간으로 차단한 정보로써, 침입차단시스템 계열(방화벽, 웹방화벽, IPS, Anti-DDoS 등)의 보안장비들이 제공하는 이벤트이다.

② 탐지 이벤트 : 미리 정의된 침해위협 탐지패턴을 기반으로 침해위협 시도를 실시간으로 탐지한 정보로써, 침입탐지시스템 계열(IDS, ESM 등)의 보안장비들이 제공하는 이벤트이다.

따라서, 본 논문에서는 위에서 분류한 2가지 유형의 보안이벤트를 효과적으로 수집하기 위하여 그림 4와 같은 체계를 제안하고자 한다.

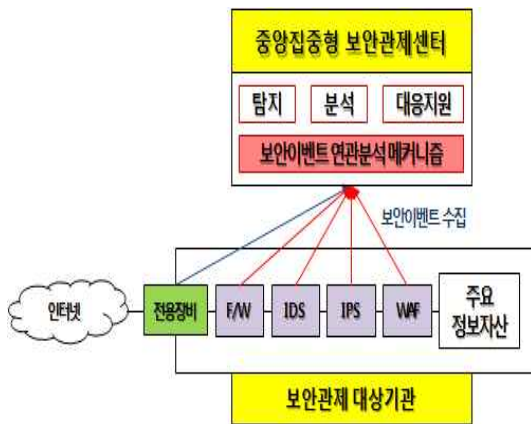


그림 4. 보안이벤트 수집 체계
Fig. 4. Collection Scheme of Security Events

특히, 연관관계분석에 필요한 다양한 보안이벤트 수집을 위하여 보안관제 대상기관에서 기 구축·운영 중인 정보보호시스템들이 생성하는 보안이벤트 정보를 수집하는 방식을 선택하였다. 이를 위하여 보안관제 대상기관이 보유한 정보보호시스템 현황을 분석한 결과 방화벽, 침입탐지시스템, 침입방지시스템 및 웹방화벽 장비가 가장 일반적으로 운영되고 있었다.

따라서, 본 논문에서는 기존의 백본 네트워크에서 수집된 보안이벤트 정보를 기준으로 각급 기관에서 운용 중인 4종의 정보보호시스템이 생성하는 보안이벤트 정보를 추가적으로 수집하여 이들 간의 연관관계 분석을 수행하는 체계를 제안하고자 한다.

3.3 보안이벤트 유형 분류

본 절에서는 보안관제 대상기관에서 수집되는 보안이벤트 정보들을 대상으로 연관관계 분석을 수행하기 위하여 그림 5와 같이 보안이벤트를 3가지 유형으로 분류하였다.

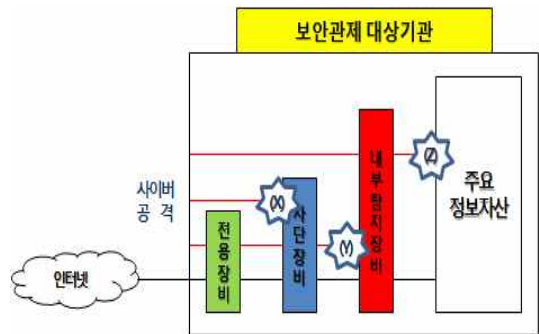


그림 5. 탐지된 보안이벤트 분류
Fig. 5. Classification of Detected Security Events

- ① 차단 이벤트(X) : 네트워크 인입 구간에서 위협상황이 탐지되지는 않았으나, 정보보호시스템(방화벽, IPS, WAF)에 의해 공격이 차단된 이벤트 유형이다.
- ② 탐지 이벤트(Y) : 네트워크 인입 구간에서 위협상황이 탐지되었으며, 정보보호시스템에 의해 공격이 차단되지 않은 이벤트 유형이다.
- ③ 내부탐지 이벤트(Z) : 네트워크 인입 구간 및 차단 기능을 제공하는 정보보호시스템에서 탐지·차단이 이루어지지 않았으나, 정보보호시스템(IDS)에 의해 공격이 탐지된 이벤트 유형이다.

차단 이벤트는 그림 3의 (C) 영역에 해당되므로 무의미한 이벤트 정보를 추출하는데 활용될 수 있으며, 내부탐지 이벤트는 (B) 영역의 일부를 탐지하는데 활용될 수 있다. 특히, 탐지 이벤트는 패턴 기반의 실시간 보안관제체계에서 가장 중요한 정보라 할 수 있다.

3.4 보안이벤트 연관관계분석 메커니즘

본 논문에서 제시하고자 하는 보안이벤트 연관관계 분석 메커니즘의 골격은 그림 6에서 보이며, 수집된 다양한 원천 데이터집합을 이용하여 2단계 분석을 수행한다. 특히, 보안관제 업무의 효율성을 극대화시키기 위하여 1단계는 “신속성” 중심의 보안이벤트 필터링에 2단계는 “정확성” 중심의 보안이벤트 정교화에 각각 초점을 맞추고 있다.

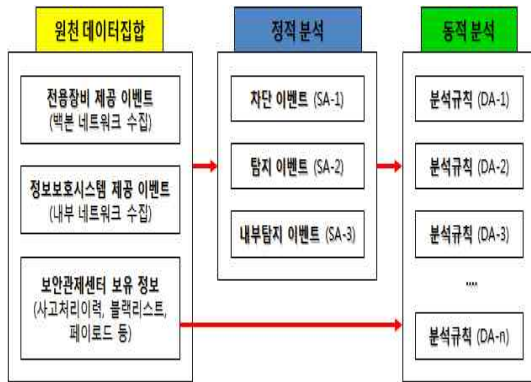


그림 6. 보안이벤트 연관관계분석 메커니즘

Fig. 6. Correlation Mechanism of Security Events

3.4.1 정적 분석(Static Analysis)

정적 분석의 핵심목표는 보안관제의 “신속성” 측면에서 무의미한 이벤트(SA-1)를 시스템적으로 필터링하여 핵심 보안이벤트(SA-2)를 중심으로 실시간 침해대응을 수행하는 것이다.

이를 위하여 보안관제 대상기관 백본 네트워크로부터 수집된 보안이벤트(대용량)를 중심으로 대상기관 내부의 정보보호시스템들이 제공하는 탐지 및 차단 이벤트, 중앙집중형 보안관제센터가 보유한 침해사고대응 관련 정보들을 종합하여 그림 5에서 설명한 3가지 핵심 보안이벤트 유형으로 재분류한다.

이와 같은 과정을 통해 대규모 보안이벤트 집합으로부터 무의미한 이벤트들을 필터링하여 보안관제요원

들의 침해대응 업무 경감 효과를 가져올 수 있다.

3.4.2 동적 분석(Dynamic Analysis)

동적 분석의 핵심목표는 보안관제의 “정확성” 측면에서 정적 분석 결과와 원천 데이터집합 사이의 연관성을 분석하여 사후처리 중심의 침해대응을 수행하는 것이다.

이를 위하여 정적 분석 결과와 원천데이터집합을 조합하여 새로운 분석규칙(탐지패턴)을 개발하고 이를 토대로 신종·변종 공격에 대한 탐지를 수행한다. 특히, 그림 6에서와 같이 다양한 형태의 분석규칙 생성이 가능하여 1:1 매핑(예컨대 SA-1과 보안관제센터 보유 정보)에서부터 동적 분석 결과 간의 매핑(예컨대, DA-1, DA-3)도 가능하여 다음 수식과 같이 분석규칙을 생성할 수 있다.

$$\text{동적 분석을 위한 분석규칙의 수} = \sum_{i=1}^n C_i$$

그러나, 동적분석을 위한 분석규칙의 수준이 증가할수록 복잡도 및 시스템 성능저하 문제가 유발할 가능성이 존재한다.

IV. 분석 및 결론

4.1 시뮬레이션 결과 분석

과학기술사이버안전센터는 과학기술 분야 출연연구기관에 대한 실시간 보안관제·분석 및 대응기술지원을 목적으로 2005년 한국과학기술정보연구원 내에 설립된 국내 주요 부문보안관제센터 중 한곳이다[1, 9]. 본 논문에서는 표 1과 같이 과학기술사이버안전센터를 통해 보안관제 대상기관으로부터 수집된 다양한 보안이벤트들을 활용하여 제안된 보안관제체계 내의 정적 및 동적 분석에 대한 시뮬레이션을 수행하여 제안된 보안관제체계의 실효성을 검증하였다.

4.1.1 정적 분석 결과

표 1의 원천 데이터 집합을 활용하여 정적 분석을 수행한 결과는 표 2와 같다. 보안관계 대상기관 백본 네트워크에서 탐지된 총 43,402,776건의 보안이벤트에 대한 필터링 결과 12,217,157건으로 약 72%가 감소하여 보안관계요원의 업무 부담을 획기적으로 개선하였다.

표 1. 원천 데이터 집합
Table 1. Security Event Set Collected by S&T-SEC

단위/건	보안이벤트 발생 건수 (분당)		
	전용장비 (TMS)	차단장비 (FW, IPS, WAF)	탐지장비 (IDS)
최소	1	16	2
최대	8,858	65,791	5,297
평균	229	5,315	124
총계	43,402,776	922,122,481	26,154,977

표 2. 정적 분석 결과
Table 2. Results of Static Analysis

단위/건	보안이벤트 발생 건수 (분당)		
	차단 이벤트 (SA-1)	탐지 이벤트 (SA-2)	내부탐지 이벤트 (SA-3)
최소	16	1	2
최대	65,971	2,974	5,297
평균	5,315	72	124
총계	922,117,369	12,217,157	26,154,634

4.1.2 동적 분석 결과

동적 분석을 위하여 표 3 및 표 4와 같은 분석규칙을 개발하여 적용하였다. 특히 분석규칙-1은 2개의 데이터를 분석규칙-2는 3개의 데이터를 활용하여 연관관계 분석을 수행하는 형태로 개발하였다.

표 3. 동적 분석 규칙-1

Table 3. Example of Dynamic Analysis Rule (1)

분석규칙명	Fosniw
연관 관계	탐지이벤트, 블랙리스트
규칙 쿼리	select * from 탐지이벤트 a, 블랙리스트 b where a.목적지 = b.도메인 and b.관련이벤트 like '%Fosniw%'
규칙 설명	탐지이벤트 중 블랙리스트 목록에 관련 탐지패턴으로 Fosniw를 갖는 도메인으로 접속하는 데이터

표 4. 동적 분석 규칙-2

Table 3. Example of Dynamic Analysis Rule (2)

분석규칙명	ssdt
연관 관계	탐지이벤트, 블랙리스트, 사고처리이력
규칙 쿼리	select * from 탐지이벤트 a, 블랙리스트 b, 사고처리이력 c where a.목적지 = b.도메인 and a.목적지IP = c.목적지IP and b.관련이벤트 like '%ssdt%'
규칙 설명	탐지이벤트 중 블랙리스트 목록에 관련 탐지패턴으로 ssdt를 갖는 도메인으로 접속하는 데이터, 이때 도메인 IP가 변경될 수 있기 때문에 기 사고처리 데이터 중 동일한 패턴명으로 사고처리된 목적지IP를 확인

표 3과 표 4의 분석규칙을 적용하여 동적 분석을 수행한 결과는 표 5와 같다.

표 5. 동적 분석 결과

Table 5. Results of Dynamic Analysis

분석규칙	이벤트 발생 건수	정답율
Fosniw	1,946	650 (33%)
ssdt	274	124 (45%)

기존의 보안관제체계에서는 탐지되지 않았거나 탐지되었다 하더라도 추가적인 분석이 요구되던 해킹 시도에 대해서도 효율적으로 탐지 및 대응이 가능한 것으로 나타났다.

4.2 결 론

본 논문에서는 백본 네트워크에서 수집된 보안이벤트 중심의 보안관제체계의 한계점을 개선하기 위하여 보안관제 대상기관 내에 기 구축·운영 중인 정보보호 시스템들이 생성한 보안이벤트들을 추가적으로 수집하여 3가지 유형으로 분류하고 이들에 대한 연관관계 분석 메커니즘을 기반으로 보안관제요원들이 신속·정확하게 침해대응 활동을 수행할 수 있는 효율적인 보안관제체계를 제안하였다. 또한, 제안된 보안이벤트 연관관계분석 메커니즘을 실제 보안관제센터를 통해 시뮬레이션을 수행하여 실효성을 검증하였다.

제안된 보안관제체계는 중앙집중형 보안관제센터 신규 구축 또는 고도화 시에 참조모델로 활용될 수 있을 것으로 기대된다.

참고문헌

- [1] 방송통신위원회, "2011년 국가정보보호백서," 2011.5.
- [2] Bass, T., "Intrusion detection systems and multisensor data fusion", Communications of the ACM, ACM Press, pp. 99-105, New York, NY, USA, 2000.
- [3] Dong Yu and Deborah Frincke, "A Novel Framework for Alert Correlation and Understanding", ACNS 2004, LNCS 3089, pp. 452-466, 2004.
- [4] Giorgio Giacinto, Roberto Perdisci, and Fabio Roli, "Alarm Clustering for Intrusion Detection Systems in Computer Networks", MLDM 2005, LNAI 3587, pp. 184-193, 2005.
- [5] James J. Treinen, Ramakrishna Thurimella, "A Framework for the Application of Association Rule

Mining in Large Intrusion Detection Infrastructures", RAID 2006, LNCS 4219, pp. 1-18, 2006.

- [6] J. Song, H. Ohba, H. Takakura, Y. Okabe, K. Ohira and Y. Kwon, "A Comprehensive Approach to Detect Unknown Attacks via Intrusion Detection Alerts", ASIAN2007 Focusing on Computer and Network Security, LNCS 4846, pp. 247-253, Doha Qatar, December 2007.
- [7] Jungsuk Song, Hiroki Takakura and Yongjin Kwon, "A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts", SAINT 2008, IEEE CS Press, pp.51-56, 2008.
- [8] Jungsuk Song, Hiroki Takakura, Yasuo Okabe and Yongjin Kwon, "Correlation Analysis Between Honeypot Data and IDS Alerts Using One-class SVM", Intrusion Detection Systems, InTech Open Access Publisher, pp. 173-192, 2011.
- [9] 과학기술사이버안전센터, <http://www.sntsec.or.kr/>

저자소개

이행곤 (Haeng-Gon Lee)



1997년 호원대학교 컴퓨터공학과
(공학사)

2000년 전북대학교 대학원 전자계산
학과 (공학석사)

2008년~현재 전북대학교 대학원 정보
보호공학과 박사과정

2000년~현재 한국과학기술정보연구원
과학기술사이버안전센터 선임연구원

※ 관심분야: 네트워크 보안기술, 보안관제, 침해사고
조사 및 대응



최상수 (Sang-Soo Choi)

2001년 한남대학교 컴퓨터공학과
(공학사)
2003년 한남대학교 대학원 컴퓨터
공학과 (공학석사)
2006년 한남대학교 대학원 컴퓨터
공학과 (공학박사)

2006년~현재 한국과학기술정보연구원
과학기술사이버안전센터 선임기술원

※ 관심분야: 보안관제, 침해사고대응, 보안공학



송중석 (Jungsuk Song)

2003년 한국항공대학교 항공통신
정보공학과 (공학사)
2005년 한국항공대학교 대학원
정보통신공학과 (공학석사)
2009년 교토대학교 대학원
지능정보학 (정보학박사)

2009년~2011년 일본정보통신연구원 (NICT) 선임연구원

2011년~현재 한국과학기술정보연구원 선임연구원

※ 관심분야: 네트워크 보안, 데이터 마이닝, 기계학습,
IPv6 보안, 스팸분석, 악성 웹사이트 분석



조기환 (Gi-Hwan Cho)

1985년 전남대학교 전산통계학과
(공학사)
1987년 서울대학교 대학원 전산통계
학과 (이학석사)
1996년 Newcastle대학교 대학원 전산
학과 (이학박사)

1987년~1997년 한국전자통신연구원 선임연구원

1997년~1999년 목포대학교 컴퓨터공학과 전임강사

1999년~현재 전북대학교 컴퓨터공학부 교수

※ 관심분야: 이동컴퓨팅, 무선 네트워크 보안, 센서
네트워크, 차량안전통신