ESM에서 보안이벤트 분석기술에 관한 연구

최대수○ 이용균
이글루시큐리티 인터넷보안연구소
{dschoi○, spider}@igloosec.com

A Study on Security Event Analysis Technique in ESM

Daesoo Choi○ Yongkyun Lee
Internet Security Lab, IGLOO Security

요 약

ESM 에서 보안이벤트 분석기술에는 실시간 보안이벤트 필터링 기술, 보안이벤트 상호연관분석기술, 보안이벤트 시각화 분석기술이 활용되고 있다. 기존 보안이벤트 분석기술에서 탐지하지 못하는 미탐을 감소시키고 침입 탐지율을 향상시키기 위하여 보안이벤트 프로파일링 기술을 접목한 침입추론 기술을 제안한다. 보안이벤트를 네트워크 분류, 호스트 분류, 웹 이벤트 분류로 유형을 구분하고 각각을 프로파일링 하여 네트워크 공격의 Anomaly 와 웹 어플리케이션 공격을 탐지할 수 있다.

1. 서 론

각종 웜과 바이러스 등 보안 위협이 날로 증가하고 있으며 학교, 기업 등 조직에서는 이에 대해 효과적으로 대처하기 위하여 방화벽, VPN, 침입탐지시스템, 바이러스월 등 다양한 단위보안제품들을 설치하여 대응하고 있다. 전사적인 보안관리 솔루션인 통합보안관리시스템(ESM; Enterprise Security Management)은 2001년도부터 등장하여 다양한 이기종의 정보보호시스템 보안이벤트를 수집하여 분석하고 일관된 정책으로 보안관리를 할 수 있도록 지원하고 있다[1].

본 논문에서는 ESM에서 이용되는 보안이벤트 분석기술에 대해 알아보고 기존 ESM의 분석기술에서 탐지하지 못하는 미탐을 감소시키고 침입을 탐지하기 위하여 보안이벤트 프로파일링 기술을 접목한 침입추론 기술을 제안한다. 본 기술을 활용하여 네트워크 공격의 Anomaly를 탐지할 수 있으며 웹 어플리케이션 공격에 대해서도 보안이벤트만 가지고 탐지할 수 있다. 결과적으로 미탐을 감소시켜 보안침해사고를 탐지하고 적절히 대응해 나갈 수 있다. 2장에서는 현재 ESM에서 사용되는 보안이벤트 분석기술에 관하여 조사하고 3장에서는 본 논문에서 보안이벤트 프로파일링 분석기술을 ESM에 도입한 방법에 대해서 설명하고 4장에서는 제안 기술의 성능을 평가한다. 5장에서는 결론 및 향후 연구방향에 대해 논한다.

2. 관련연구

2.1 실시간 보안이벤트 필터링 기술

ESM은 이기종 단위보안시스템에서 생성하는 보안이벤트를 실시간으로 수집 통합하고 분석할 수 있는 프레임웍을 제공한다. 실시간으로 수집된 이벤트를 이벤트 종류별로 또는 이벤트간의 공통요소를 기반으로 분석할 수 있다. 즉, 동일한 시간에 침입탐지 시스템과 침입차단시스템에서 동일한 공격대상장비로 관련 보안이벤트가 발생했을 경우에 대해서 실시간 분석할 수 있다.

그 외에도 이벤트 수집시간, 이벤트 발생시간, 근원지 IP, 근원지 Port, 공격대상 IP, 공격대상 Port, 프로토콜 등을 기반으로 상호간에 공통요소를 뽑아내어 실시간으로 분석할 수 있다. 또한 관제대상장비의 특성에 맞게 이벤트별 필터링을 수행한다. 실시간 보안이벤트 필터링 기술은 초기의 ESM 핵심 기술로서 이벤트 수집 및 실시간 분석 기술이다[1][2].

2.2 보안이벤트 상호연관분석 기술

현재 ESM 의 가장 핵심적인 기술로 다양한 보안이벤트간의 상호연관 요소를 기반으로 침입을 추론하는 기술이다. 이 기술에 대해서는 학문적, 상업적으로 많은 연구가 진행되고 있다[1][2]. 실시간 상호연관분석으로 탐지할 수 있는 시나리오는 다음과 같은 것들이 있다.

- 두가지 디바이스간의 관계적인 요소를 기반으로 분석
  네트웍 트래픽이 임계치를 초과하고, 그 시간대에 트래픽을 유발하는 바이러스가 발견된 경우
- 두가지 디바이스간의 인과적 요소를 기반으로 분석
  침입탐지시스템에서 불법접근시도에 관련된 이벤트가 탐지되고 그때 동일한 근원지 IP, 목적지 IP와 관련된 방화벽의 이벤트가 거부 또는 허용된 경우
- 세가지 디바이스간의 인과적 요소 분석
  침입탐지시스템에서 불법접근시도에 관련된 이벤트가 탐지되고 그때 동일한 근원지 IP, 목적지 IP와 관련된 방화벽의 이벤트가 허용되고 해당 목적지 시스템의 주요 파일에 변경이 발생한 경우

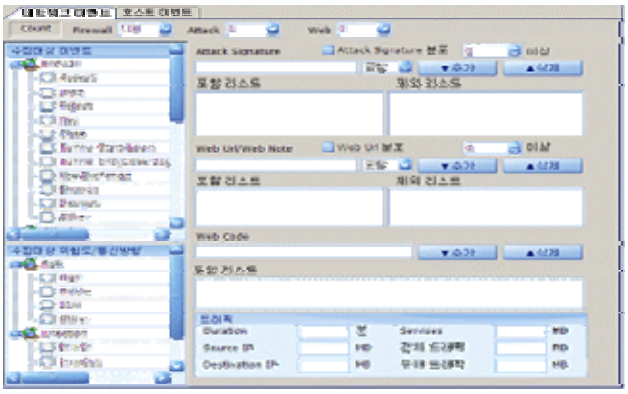

그림 2 보안이벤트 상호연관 분석 설정

2.3 보안이벤트 시각화 분석 기술

보안이벤트 시각화 기술을 도입하여 ESM에서 보안상황을 인지할 수 있는 기술은 최근 개발된 신기술이다[3][4]. 상황인지 기술은 인문과학에 있어서 과거부터 연구되어온 학문분야로 보안분야의 새로운 기술은 아니지만 이 기술을 ESM에 접목해 보다 진보된 형태의 보안상황을 인지하도록 할 수 있다. 네트워크상의 보안이벤트, 트래픽 정보들을 Information Visualization 기술을 이용하여 시각화하여 기존의 텍스트 기반의 네트워크 정보처리시스템에서 발견할 수 없었던 네트워크의 장애정보를 신속히 발견하여 관리자로 하여금 신속하게 적절한 대처를 할 수 있게 해준다. 그림 3 은 보안이벤트의 근원지 IP 와 출발지 IP 를 각 그룹별로 표현하였으며 각 좌표에 나타나는 막대는 이벤트 종류와 양을 시각적으로 표현하여 DDos 또는 웜과 같은 공격의 이벤트 특성을 이용하여 침입을 즉각적으로 인지할 수 있도록 한다.

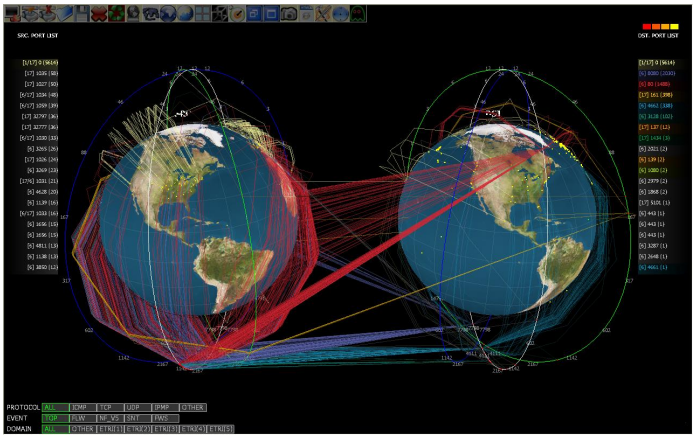

그림 3 보안이벤트 시각화분석 기술

3. 보안 이벤트 프로파일링 기술

2장에서 기술한 다양한 보안이벤트 분석 기술에도 불구하고 정보보안 침해사고는 지속적으로 증가하고 있다. 일반적으로 위협관리시스템(TMS: Threat Management System)에서 트래픽의 비정상 행위를 탐지하기 위하여 트래픽 프로파일링 기술을 활용한다[5][6]. ESM의 보안이벤트 분석기술을 보완하고 미탐을 감소시키기 위하여 보안이벤트 프로파일링 기술을 접목한 침입추론 기술을 제안한다. 제안한 방법에서는 보안이벤트를 크게 3가지로 분류하여 정규화하고 프로파일을 생성한다.

3.1 보안 이벤트 정규화

ESM에서 수집하는 각 단위보안시스템의 보안이벤트의주요 내용과 정규화 가능한 항목을 정리하면 표 1과 같다. 제안 시스템에서는 보안 이벤트를 정규화하고 프로파일링에 활용한다.

표 1 보안 이벤트 분류

유형	보안장비	내용
네트워크 유형	침입차단시스템	발생시간, 발생장비, 근원지 IP, 근원지 Port, 목적지 IP, 목적지 Port, Protocol, 이벤트종류(accept, drop, reject, error, close, 등), 중요도, 제품명, 발생횟수
	침임탐지시스템	발생시간, 발생장비, 근원지 IP, 근원지 Port, 목적지 IP, 목적지 Port, Protocol, 위험도, 공격종류, 공격명(Signature), 패킷의 크기, 제품명, 조치내역, CVE코드값, 발생횟수
	안티바이러스제품	발생시간, 발생장비, 근원지 IP(email 주소), 받는사람 IP(email 주소), 검사한 파일, 검사한 파일 위치, 바이러스명, 조치결과, 제품명
호스트 유형	메일보안	발생시간, 발생장비, 근원지 IP, 목적지 IP, 수신자 메일주소, 메일제목, 이벤트 처리내용 (Accept, Drop, Info 등), 첨부파일명, 제품명, 발생횟수
	서버보안	발생시간, 발생장비, 발생이벤트 처리내용, 근원지 IP, 근원지 port, 목적지 IP, 목적지 Port, 프로토콜, 패킷크기, 제품명, 이벤트발생규칙, 발생횟수
	문서보안	발생시간, 발생장비, 사용자(IP주소), 접근대상, 이벤트종류(폴더설정, 폴더삭제 등), 접근한 결과, 제품명, 발생횟수
웹 유형	웹로그	발생시간, 발생장비, 근원지 IP, 결과코드, 메소드, 쿼리값, 쿠기값, 발생횟수

3.2 보안 이벤트 프로파일링

프로파일 기반의 침입탐지는 정상행위를 기준으로 이와 위배되는 행위를 침입으로 간주하는 방법이다. 즉,

프로파일링 탐지기법은 공격행위가 정상행위와 다르다는 점을 가정한다. 프로파일은 네트웍 트래픽에 대한 데이터 마이닝, 감사 데이타 분석을 통한 통계적 분석, 그리고 운영체제 시스템 콜을 이용한 시퀀스분석등이 있다[5][6]. 제안 시스템에서는 감사 데이타 분석을 이용한 통계적인 분석으로서 네트웍 유형의 보안이벤트를 프로파일화 하고, 호스트 유형의 보안이벤트를 프로파일화 한다. 그리고 웹 어플리케이션 이벤트를 프로파일화 한다. 즉 3가지의 각기 다른 유형으로 정규화하여 프로파일화한 다음 네트워크 유형과 호스트 유형은 프로파일 값에서 벗어나는 경우를 비정상 행위로 간주한다. 그 외 웹 어플리케이션 프로파일의 경우는 웹 어플리케이션 요청 값의 파라미터 정보를 분석하고 데이터 타입, 허용 가능한 문자열, 입력 값의 길이 등을 사전에 학습 후 정상행위 프로파일을 생성하고 이와 비교하여 웹 어플리케이션 공격을 탐지한다.

표 2 보안 이벤트 프로파일

유형	프로파일 내용
네트워크 유형	- 근원지 IP, 목적지 IP, 목적지 Port, 프로토콜 - 근원지 IP, 목적지 IP, 공격명(바이러스명)
호스트 유형	- 목적지 IP, 발생이벤트(첨부파일명, 메일제목 등)
웹 이벤트 유형	- 프로파일 IP, 파라미터, 변수 (파라미터별 허용 가능한 문자열을 정의)

표 2 에서와 같이 이기종 정보보호시스템의 보안이벤트를 3가지로 크게 분류하였고 네트워크 유형의 프로파일은 2가지로 분류하여 프로파일화 한다. 그리고 호스트 분류의 프로파일은 목적지 IP, 발생 이벤트로 프로파일화 한다. 그래서 시간대별, 일별 프로파일화한 통계값을 활용하여 최상위 Top 100 과 최하위 100 가지의 이벤트를 위주로 정의한 임계치에서 벗어난 이벤트가 발생될 경우 비정상 행위로 간주하여 침입으로 탐지한다.

웹 어플리케이션 프로파일은 웹 어플리케이션의 구조를 파악하여 이를 데이터베이스화하는 것이다. 사용자 요청 데이터를 분석하여 그림 6 과 같은 프로파일을 구성한다. 사용자 요청은 '?' 문자로 구분되며 뒤쪽에 파라미터 변수와 값이 '=' 문자를 통해 대응된다. 웹 어플리케이션 프로파일링 모듈은 레코드 구성에 각 파라미터 변수를 연결하여 프로파일 레코드의 구분자인 ID 값을 구성한다. http://www.test.com/cgi-bin/ test.cgi?p1=v1& &...pn=vn 과 같은 사용자 요청이 있을 경우 요청에 대한 ID 값은 PROFILEID=/cgi-bin/test.cgi-p1..pn 으로 구성한다. 그리고 해당 ID 에 대응되는 파라미터 테이블들을 구성함으로서 비정상적인 요청을 탐지한다. 웹 이벤트 유형의 프로파일은 '프로파일기반 웹 어플리케이션 공격탐지 및 필터링 기법' 연구의 프로파일 방법론을 활용하였다[5].

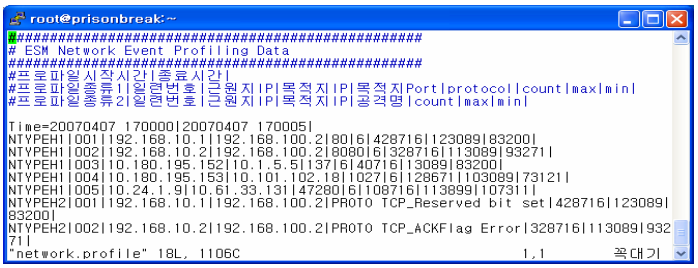

그림 4 네트워크 유형 프로파일

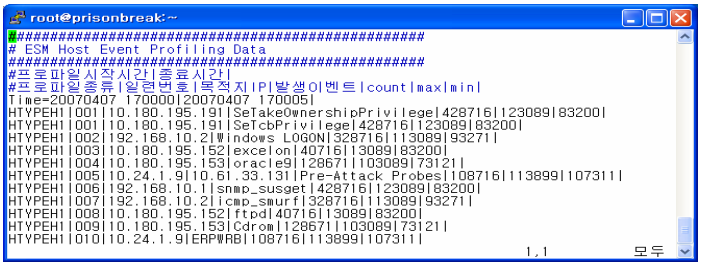

그림 5 호스트 유형 프로파일

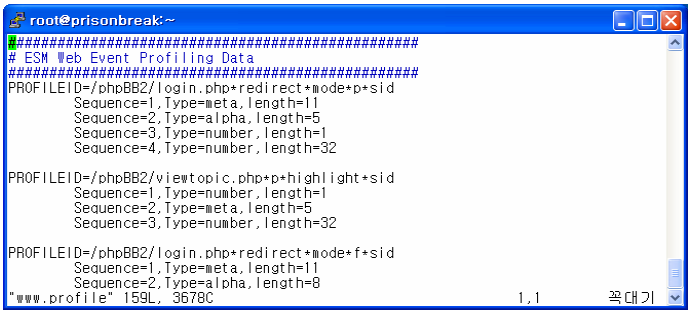

그림 6 웹 이벤트 유형 프로파일

3.3 제안 시스템 구조

그림 7 과 같이 제안 시스템은 보안이벤트 수집 모듈과 보안이벤트 분석 모듈로 구성된다. 보안이벤트 분석 모듈은 기존의 보안이벤트 상호연관분석 엔진과 보안이벤트 시각화 엔진이 있고 본 논문에서 제안한 보안이벤트 프로파일러와 보안이벤트 프로파일링 엔진으로 구성된다. 보안이벤트 프로파일러는 실시간으로 수집되는 보안 이벤트를 최소 5분단위로 이벤트 구성요소별 수집량과 최소 1분단위별 최대횟수, 최소횟수를 프로파일화 한다. 그림 4 와 그림 5 가 프로파일된 결과 예제이다.

그리고 웹 이벤트 프로파일 결과는 네트워크와 호스트 유형과 다른 프로파일 값을 갖는다. 즉, 정상적인 웹 입력값 검증을 위하여 프로파일 식별자별로 파라미터 변수의 타입과 파라미터 입력값 길이를 사전에 정의하여 프로파일화한다. 그림 6 이 웹 이벤트 프로파일 결과이다.

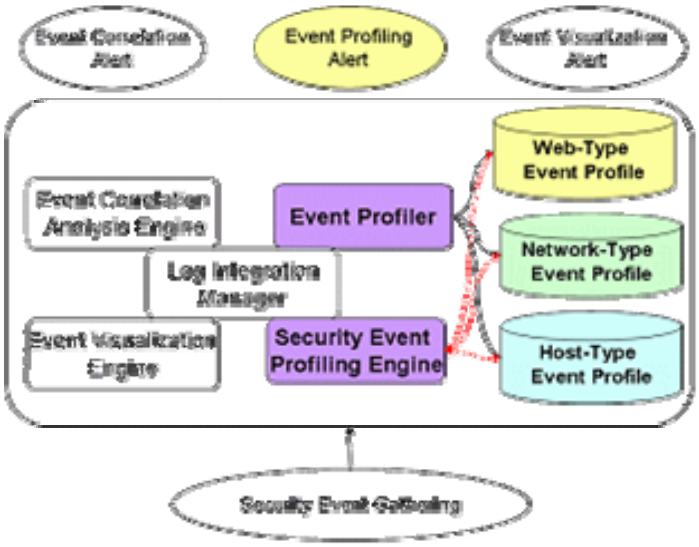

그림 7 제안시스템 구조

사용자 입력요청 값이 프로파일 레코드에 존재하지 않을 경우 비정상 요청으로 간주하고 공격으로 판단한다.

4. 제안 시스템 성능 평가

본 논문에서는 제안한 보안이벤트 프로파일링 기법 중에서 웹이벤트 유형 프로파일링에 대해서 성능평가를 하였다. 테스트에 활용된 웹서버는 Apache/2.0.40 이며 프로파일 데이타는 웹로그 파일일 읽어서 생성하였다. 시험에 사용된 웹 어플리케이션은 PHP 방식인 phpBB 2.09를 사용하였으며 프로파일 데이터 생성은 WebStripper 2.56 프로그램을 이용하였다[7][8][9].

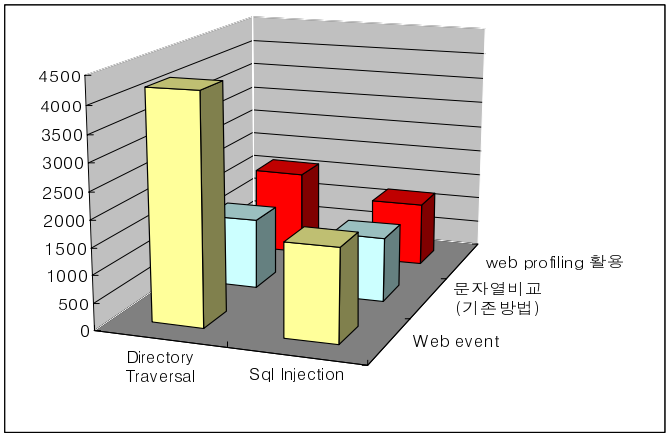

그림 8 웹 어플리케이션 스캐닝 후 침입탐지건수 비교

웹로그 파일에 나타난 정상적인 요청의 수는 276개였으며 프로파일링 된 개수는 7 개로 2.53% 의 프로파일 비율을 보였다. 프로파일 결과의 개수는 웹 어플리케이션마다 페이지 링크 구조에 따라 다를 수 있지만 결과적으로 요청수가 크게 늘어나도 레코드 수는 크게 증가하지 않는다. 즉, 비정상 요청 탐지에 효과적이다. 비정상 요청을 탐지하기 위하여 비정상 요청 생성프로그램으로 Acunetix 웹 취약점 스캐너 프로그램을 이용하였다[10]. 웹 어플리케이션 스캐너를 이용하여 웹 어플리케이션을 스캔 후 ESM 의 문자열 비교 기반의 침입탐지 기법과 탐지건수를 비교하였다. 디렉토리 이동공격과 SQL 인젝션 공격 2가지에 대해서 웹 프로파일링을 활용한 시스템이 약간의 우위를 나타냈지만 크게 차이는 없었다. 문자열 비교 방식은 SQL 문 또는 디렉토리 관련 문자열이 비교되면 무조건 침입으로 간주한다. 즉 오탐의 소지가 많다. 하지만 웹 프로파일링은 입력된 문자열의 종류와 길이를 기반으로 하기 때문에 오탐의 가능성이 줄어든다.

5. 결론 및 향후 연구 방향

ESM 에서 이용되는 보안이벤트 분석기술에는 실시간 보안이벤트 필터링 기술, 보안이벤트 상호연관분석 기술, 보안이벤트 시각화 분석기술이 활용되고 있다. 본 논문에서 제안한 보안이벤트 프로파일링 기술의 접목은 기존 이벤트 분석기술을 보완하고 미탐을 감소시키며 침입탐지율을 향상시킨다. 보안이벤트 프로파일링은 네트워크 공격의 Anomaly 와 웹 어플리케이션 공격을 탐지할 수 있다. 웹 어플리케이션 프로파일링을 활용하여 웹 어플리케이션 침입탐지의 성능평가를 하였고 오탐을 감소시킬 수 있다. 향후 연구방향으로는 보안이벤트 프로파일링 기술을 상호연관분석기술과 조합하여 활용할 수 있는 연구가 필요하다.

참고문헌

[1] 이글루시큐리티, "http://www.igloosec.co.kr"
[2] Christopher Kruegel, Giobanni Vigna, William Robertson, "A multi-model approach to the detection of web-based attacks", Computer Networks:Vol48, No.5, pp 717-738, August, 2005.
[3] 이수형, 방효찬, 장범환, 나중찬, “효과적 보안상황 분석을 위한 보안이벤트 처리”전자통신동향분석 제 22권 제 1호, 2007년 2월
[4] 이용균, “보안과 비즈니스 요구, 그리고 시각화”, 한국정보처리학회지 제16권 제2호, 2006년 4월
[5] 윤영태, 류재철, 박상서, 박종욱, "프로파일기반 웹 어플리케이션 공격탐지 및 필터링 기법", 한국정보처리학회논문지 C 제 13-C권 제1호, 2006년 2월
[6] 박채금, 노봉남, "웹어플리케이션 보안을 위한 프로파일 기반 탐지시스템 설계", 한국정보처리학회 추계학술발표대회 논문집 제12권 제2호, 2005년 11월
[7] Apache, “http://www.apache.org/”
[8] phpBB, “http://www.phpbb.com/”
[9] WebStripper , http://webstripper.net/
[10] Acunetix, "http://www.acunetix.com/"