https://doi.org/10.33778/kcsa.2020.20.5.041

보안 시그니처 탐지를 위한 필터링 우선순위 알고리즘 구현★

전 은 아*, 김 점 구**

요 약

본 논문은 보안 이벤트 위험성에 따른 능동적 대응을 위해서 우선순위 알고리즘을 구현하는 것이며, 이를 기반으로 효율적인 이벤트 처리를 수행하는 이벤트 스케줄러를 구현하고자 한다. CVE나 CVSS 같이 세계적으로 표준을 가지고 있는 기준에 따라, 보안 이벤트를 실행시켰을 때 점수를 매길 수 있는 기준을 마련하고, 정형화 하여 보다 객관적으로 우선순위를 정할 수 있도록 한다. 그래서 이를 바탕으로 보안 이벤트 데이터베이스를 구축하고, 이를 이용하여 스케줄링을 할 수 있도록 한다. 또한 보안 이벤트 스케줄링 우선순위 알고리즘을 우리나라 보안 이벤트 실정에 맞게 개발하고 적용함으로써 국내 기관 및 기업의 정보보호에 대한 신뢰성 확보와 산업 발전에 기여하게 될 것이다.

Development on Filtering Priority Algorithm for Security Signature Search

Eun-A, Jun*, Jeom-goo, Kim**

ABSTRACT

This paper implements a priority algorithm for active response to security event risk, and implements an event scheduler that performs efficient event processing based on this. According to the standards that have global standards such as CVE and CVSS, standards for scoring when security events are executed are prepared and standardized so that priorities can be more objectively set. So, based on this, we build a security event database and use it to perform scheduling. In addition, by developing and applying the security event scheduling priority algorithm according to the situation of security events in Korea, it will contribute to securing the reliability of information protection and industrial development of domestic organizations and companies.

Key-words: CVE, CVSS, Algorithm, Security, Signature

접수일(2020년 11월 30일), 수정일(2020년 12월 16일), 게재확정일(2020년 12월 31일)

★ 이 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2020R1I1A3067375).

* 남서울대학교 컴퓨터소프트웨어학과 외래교수
** 남서울대학교 컴퓨터소프트웨어학과 교수

1. 서 론

최근 다양하고 새로운 형태의 네트워크 위협공격이 지속적으로 등장하고 있다. 많은 정보자원을 보유하고 있는 주요 공공기관 및 기업에서는 이러한 위협에 대처하기 위해서 다양한 보안시스템을 운영하고 있다. 그중 국·내외적으로 정교하고 복잡한 네트워크 공격들이 등장함에 따라 이를 탐지·예방하기 위해서 여러 보안 장비들로부터 보안이벤트를 종합적으로 수집하여 관리자에게 제공하는 통합보안관리시스템(ESM) 운용이 증가하는 추세이다[1][2]. 하지만 이 통합관리시스템은 단순히 여러 보안 장비로부터의 보안이벤트를 종합적으로 수집하여 보안관리자에게 제공하기 때문에 보안이벤트의 false positive와 false negative가 많이 존재한다. 또한 각기 네트워크의 구성 상황에 따라 위협의 위험성이 다르고 이에 따라 우선순위를 가지고 먼저 처리되어야 하는 보안이벤트들이 존재하지만 통합관리시스템은 이를 제공하지 못한다. 통합관리시스템은 단순히 다양한 보안이벤트를 수집, 제공하는 기능만을 수행할 뿐이며 네트워크 상황에 따른 보안이벤트 처리는 결국 보안관리자의 책임으로 남게 된다.

이런 상황에서 공공기관과 기업들을 목표로 한 네트워크 공격이 점차 정치적, 경제적 목적을 띄고 있는 추세이다. 공격의 성패가 국·내외적인 공공기관, 기업 그리고 더 나아가서는 국가의 이미지 형성에 큰 변수가 될 수 있음을 감안 한다면 이를 보안 책임자에게만 담당하게 하는 것은 너무 과중하며, 통합보안관리시스템의 기능 개선을 위한 보안이벤트 처리 우선순위 알고리즘 개발의 필요성이 절실하다 할 수 있다.

따라서 본 논문은 동시 다발적으로 발생되는 공격에 대한 보안이벤트가 발생되었을 경우 네트워크 위협 상황과 보안이벤트의 위험성을 고려한 보안이벤트 우선순위 알고리즘을 구현하고자 한다.

2. 관련연구

2.1. 보안 이벤트

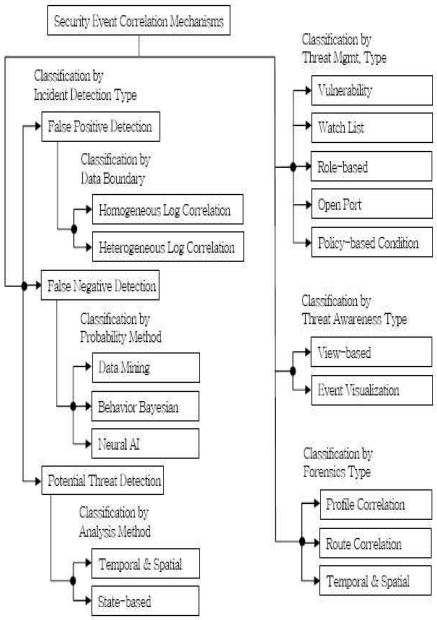
인터넷의 급격한 확산과 응용하는 수가 급격히 증가함에 따라 인터넷 상에서 이루어지는 사이버 공격의 발생 빈도는 점점 증가하고 있으며, 이로 인해 시간적, 경제적 피해 규모는 이전과는 비교할 수 없을 정도로 커지고 있다. 또한 공격 수준을 보면 기존의 가입자 단에 위치하는 시스템을 목표로 하는 공격에서 웜 확산에 따른 인터넷 마비 사고처럼 네트워크 자체의 운용이나 성능에 영향을 미치고, 결과적으로는 네트워크 서비스 제공 자체를 위협하는 단계에 이르렀다.

따라서 효과적인 네트워크 보안을 강구하기 위해서는 관리 대상이 되는 도메인에서 이루어지는 공격에 대한 탐지와 그에 따른 단순한 공격 정보뿐만 아니라 그 공격으로 인한 피해의 정도와 범위, 탐지 이벤트의 신뢰성 문제, 또는 간접적 이벤트 분석을 통한 공격의 사전 탐지와 같은 보안 상황에 대한 분석기술이 반드시 필요하다. 과거 보안 상황 분석기술에는 이벤트 특성에 따른 분류로써 침입탐지시스템이나 방화벽 등에서 수집한 이벤트를 분석하여 침입 또는 공격이 있었는가를 판단하는 것과 네트워크의 패킷(트래픽)을 분석하여 트래픽의 이상 상태 여부를 판단하는 것이 주를 이루었다. 그리고 분석방법에 따른 분류로써는 로그기록을 분석하여 공격자의 시그니처를 찾는 오용탐지와 정상적인 행동을 기반으로 비정상적인 행동을 찾는 비정상행위 탐지가 있다[4].

하지만, 이와 같은 방법들은 최근 폭발적인 이벤트 양과 오탐율(False Positives) 때문에 신속성을 요구하는 공격(Zero-day Attacks)의 분석과 알려지지 않은 공격 등을 판별하는데 많은 문제점을 드러내고 있다. 또한, 관리자들은 대량의 발생 이벤트로 인해 단순히 이벤트 정보만을 분석해서는 관리대상 도메인 네트워크 내에서 보안상황을 인식할 가능성은 전무한 상태이다. 따라서 대량의 보안 이벤트의 발생 시 그것을 일일이 사용자가 해결하기는 힘든 상황이다. 그렇다고 하나의 이벤트에만 집중하고 있을 수도 없으니, 공격에 대한 정보와 보안 상황에 대한 정보를 수집하여 보안 이벤트 스케줄러를 통한 각 이벤트에 대한 우선순위를 정한다.

2.2. 보안 이벤트 연관성 분석

이벤트 연관성 분석기술은 처음에는 네트워크 관리 분야에서 다양한 형태로 연구, 개발되어 왔으나 최근에는 네트워크 보안관리 분야에서도 커다란 이슈가 되고 있다. 보안 이벤트 연관성 분석기술이 급증하고 있는 네트워크 보안에 관련된 대량의 이벤트 정보를 운용자가 수작업으로 처리할 수 없는 문제를 해결하기 위한 정보관리 기술로써, 또한편으로는 독립적으로 발생한 다수의 이벤트 정보 간의 연관 관계를 분석함으로써 보안침해 사건의 근본적인 원인을 규명하기 위하여 지식 창조 프로세스로 적용되고 있는 상황이다. (그림 1)은 보안 분야에서 보안 이벤트 연관성 분석기술을 적용하기 위한 영역별로 그 분야를 나타낸 것이다[5].



(그림 1) 보안 이벤트 연관성 분석 기술 적용분야

2.3. 보안 이벤트 프로파일링 기술

일반적으로 위협관리시스템(TMS : Threat Management System)에서 트래픽의 비정상 행위를 탐지하기 위하여 트래픽 프로파일링 기술을 활용한다. 이런 방법에는 보안 이벤트를 크게 3가지로 분류하고 프로파일을 생성한다.

2.3.1. 보안 이벤트 정규화

<표 1> 보안 이벤트 정규화 가능한 항목

유형	보안 장비	내 용
네트워크 유형	침입 차단 시스템	발생시간, 발생장비, 근원지 IP, 근원지 포트, 목적지 IP, 목적지 포트, 프로토콜, 이벤트종류(Accept, Drop, Reject, Error, Close 등), 중요도, 제품명, 발생횟수
	침입 탐지 시스템	발생시간, 발생장비, 근원지 IP, 근원지 포트, 목적지 IP, 목적지 포트, 프로토콜, 위험도, 공격종류, 공격명, 패킷의 크기, 제품명, 조치내역, CVE 코드값, 발생횟수
	안티 바이러스 제품	발생시간, 발생장비, 근원지 IP, 목적지 IP, 검사한 파일, 검사한 파일 위치, 바이러스명, 조치결과, 제품명
호스트 유형	메일 보안	발생시간, 발생장비, 근원지 IP, 목적지 IP, 수신자 메일주소, 메일제목, 이벤트 처리내용 (Accept, Drop, Info 등), 첨부파일명, 제품명, 발생횟수
	서버 보안	발생시간, 발생장비, 발생 이벤트 처리내용, 근원지 IP, 근원지 포트, 목적지 IP, 목적지 포트, 프로토콜, 패킷크기, 제품명, 이벤트 발생규칙, 발생횟수
	문서 보안	발생시간, 발생장비, 사용자(IP주소), 접근대상, 이벤트 종류(폴더설정, 삭제 등), 접근한 결과, 제품명, 발생횟수
웹 유형	웹 로그	발생시간, 발생장비, 근원지 IP, 결과코드, 메소드, 쿼리값, 쿠키값, 발생횟수

각 단위 보안시스템의 보안이벤트의 주요 내용과 정규화 가능한 항목을 정리하면 다음의 <표 1>과 같다.

2.3.2. 보안이벤트 프로파일링

프로파일 기반의 침입탐지는 정상행위를 기준으로, 위배되는 행위를 침입으로 간주하는 방법이다. 즉, 프로파일링 탐지기법은 공격행위가 정상행위와 다르다는 점을 가정한다. 프로파일은 네트워크 트래픽에 대한 데이터 마이닝, 감사 데이터 분석을 통한 통계적 분석, 그리고 운영체제 시스템 호출을 이용한 시퀀스 분석 등이 있다[7].

본 논문에서는 감사 데이터 분석을 이용한 통계적인 분석으로 네트워크 유형의 보안이벤트를 프로파일화 하고, 호스트 유형의 보안이벤트를 프로파일화 하며, 웹 어플리케이션 이벤트를 프로파일화 한다. 즉, 3가지 각기 다른 유형으로 정규화 하여 프로파일화 한 후 네트워크 유형과 호스트 유형은 프로파일 값에서 벗어나는 경우를 비정상 행위로 간주한다. 그리고 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> 보안이벤트 프로파일 분류

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)

위 <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 시간대 및 일별 프로파일화한 통계 값을 활용하여 최상위와 최하위의 각각 Top 100가지 이벤트를 위주로, 정의한 임계치에서 벗어난 이벤트가 발생될 경우 비정상 행위로 간주하여 침입으로 탐지한다.

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. 그리고 해당 ID 에 대응되는 파라미터 테이블을 구성함으로써 비정상적인 요청을 탐지한다. 웹 이벤트 유형의 프로파일은 '프로파일 기반 웹 어플리케이션 공격탐지 및 필터링 기법' 연구의 프로파일 방법론을 활용하였다.

2.4. 각 평가 기준 및 평가 스케일 조사 연구

본 논문이 CVSS, CVE를 기반으로 우선순위를 위한 점수를 매기지만, 그 외에 다른 평가 기준들에 대한 평가 점수와 그 기준을 어디에 두는지 그리고 그러한 기준을 두는 개념이 어떻게 되는지 조사를 해보았다.

조직의 정보시스템에서 최소의 비용으로 최대의 보안성을 얻기 위한 체계적인 방법인 보안관리는 보안정책 수립, 보안 대책의 실행 및 위험분석 과정을 통해 이루어진다. 따라서 보안 관리를 위해서는 보안대책에 의해 보호되어야 하는 자산을 식별하고 그 가치를 평가하여 자산에 가해지는 위협과 취약성을 평가해야 한다. 또한 CC(Common Criteria)와 같은 정보보호시스템 평가체계상에서 보안제품의 공통기능 및 보증요구사항이라 할 수 있는 PP(Protection Profile)을 개발하기 위해서라도 이와 같은 업무를 수행해야 한다. 국내·외로 보안관리, 위험분석 및 PP개발을 위한 다양한 방법(또는 지침 및 표준)이 제시 및 사용되고 있지만, 각 방법마다 프로세스, 자산, 위협, 취약성의 분류체계(schema), 평가기준 및 스케일이 서로 다르다. 따라서 새로운 보안관리, 위험분석 및 PP 개발방법 및 도구개발을 위해 다음 사항을 고려하여 정의해야 한다.

(1) 관리 및 평가 프로세스
(2) 자산의 분류체계, 평가기준 및 스케일
(3) 위협 및 취약성의 분류체계, 평가기준 및 스케일

이를 위해, 본 논문에서는 기존의 소프트웨어 공학 및 품질관리, 보안관리, 위험분석 및 PP 개발 부문의 각종 방법, 지침 및 표준들에서 정의된 프로세스, 자산, 위협 및 취약성의 분류체계와 평가기준 및 평가 스케일들을 조사 및 분석하였다.

2.4.1. 보안관리, 위험관리 및 위험 분석의 개념

정보보호관리는 위험관리의 상위개념이며 위험관리는 위험분석의 상위 개념이다. 각 개념들의 정의와 관련 표준, 도구 및 기술들은 다음과 같다.

(1) 정보보호관리(ISM) : ISM(Information Security Management)은 조직의 정보시스템에 대한 전반적인 사항을 다루며 정보보호에 관련된 업무를 몇 개의 통제 분야로 나누고 각 분야별로 다수의 통제대책으로 구성된다[8][9]. ISO/IEC-13335 (GMIT), 영국의 BS-7799 (ISO/IEC-17799), 독일 BSI(Bundesamt Fur Sicherheit in der Informarionstechnik)의 BSI IT Baseline Protection Manual, 카네기멜론 대학의 SSE-CMM, 국내의 「정보보호관리기준」은 ISM을 위한 표준 및 지침들이다. 국내·외 보안관리 기준은 <표 3>과 같이 다양한 통제항목이 제시되어 있으며, 이러한 통제항목은 보안관리의 수준(또는 보안 위험성)을 상위 수준 또는 관리적, 비기술적 수준에서 평가하는데 활용될 수 있다.

(2) 위험관리(IRM) : IRM(Information Risk Management)은 ISM시에 최적의 비용으로 최고의 효과를 거두기 위해 통제분야의 우선순위를 결정하고 실제의 통제를 수행하는 방법 중 하나이다. 일반적으로 위험관리는 매우 광범위하며, 소프트웨어 개발 시의 위험관리 등은 정보시스템개발 시의 위험관리에 적용할 수 있다. 특히 IRM은 정보보호 차원에서의 위험관리를 의미한다[10].
그리고 일반적으로 IRM은 위험분석과 보안대책의 선택을 포함한다. 미국 NIST의 FIPS-65, FIPS-191, SP-800-30, NISTIR-4387, NISTIR-4325, GAO의 AIMD-00-33, 캐나다의 CSE(Communications Security Establishment) 및 우리나라 TTA의 TTAS.KO-12.007 등은 정부차원의 IRM 지침이다. 카네기멜론대학의 OCTAVE, C R AMM, INORSEC-92, BDSS, RiskWatch, Expert, 우리나라의 PRAM(국가보안연구소), 팬타(한국과학원) 및 HAWK(한국전산원), CISSP, Open Framework 등은 프로토타입 또는 상용화된 IRM 지원도구이다[11].

(3) 위험분석(IRA) : IRA(Information Risk Analysis)는 보안관련 항목들에 대한 위험파악과 위험평가로 구성된다. RI(Risk Identification)는 정보시스템 내에 각 항목의 세부사항을 발견 및 식별하는 것이며, RA(Risk Assessment)는 파악된 항목에 대해 그 발생 가능성과 피해 가능성 등을 수치 또는 등급으로 부여하는 것이다.

<표 3> 보안 관리 기준의 통제항목 비교

보안관리기준	통제항목 분류				최상위 클래스명
	클래스	패밀리	컴포넌트	엘리먼트	
BS7799	10	36	127	550	정책, 조직, 자산, 인사 물리/환경, 통신/운영, 접근통제, 개발/유지보수, 연속성, 준수
국내기준	12	-	131	-	정책, 조직, 아웃소싱/ 제3자 접근, 자산, 인사, 교육/훈련, 접근통제, 물리적, 운영 개발, 연속성, 사고대응/복구, 준수
GMIT	2	12	63	N/A	관리/정책, 준수, 사건처리, 인사, 운영, 연속성, 식별/인증, 접근통제/감사, 악의적 코드보호, 망관리, 암호
독일 IT baseline	6	-	544	N/A	기반구조, 조직, 인사, HW/SW,통신, 비상계획
SSE-CMM	3	22	128	744	기본, 프로젝트, 조직
Vallabhaneni	7	-	-	58	물리적, 인사, 자료, 응용SW, 시스템 SW, 통신, 운영

2.4.2. 평가 스케일의 비교

일반적으로 측정(Measurement)할 수 있는 것만 관리(통제)할 수 있으므로, 관리를 위해서는 관리대상 항목의 척도(Metric)를 정의하고 가급적 정량적(수치적)으로 척도 값을 부여해야 한다. 척도에 척도값을 매핑하는 과정을 측정 또는 평가라 한다. 예컨대, 정보시스템의 위험 관리를 위해서는 위험의 측정(분석, 평가)이 필요하다.

(1) 소프트웨어 공학부문
소프트웨어 제품 평가기준인 ISO/IEC 14598-5 (평가 프로세스), ISO/IEC 14598-6(평가 모듈), 소프트웨어 제품 평가기준(품질 특성 및 사용지침)인

ISO/IEC-9126, 카네기멜론대학의 소프트웨어 개발조직의 성숙성 평가기준인 CMM, 국내 정보통신부의 「소프트웨어사업대가의 기준(2003)」, B. Boehm이 개발한 소프트웨어 개발비 산정방법인 COCOMO-2에서 측정 스케일에 관한 지침들을 조사하였다. <표 4>는 소프트웨어공학 부문에서의 측정 스케일을 보인다.

각 기준에서 측정 스케일은 3단계부터 6단계까지 있으며, 모든 측정대상 속성의 평균 단계 수는 4.26단계이다. 대부분 평가지침들은 서술적으로 되어있다. 특히, 소프트웨어 품질에 관련된 국제표준은 ISO/IEC 14598에서와 같이 4단계로 분류하고 있다.

<표 4> 소프트웨어공학 부문에서의 측정 스케일

기준	측정대상 속성	측정스케일	구간 수	등급화 기준
ISO/IEC 14598-5,6	안정성, 경제성, 보안성 환경	A, B, C, D	4	서술적
	순응성, 적절성, 정확성, 상호운용성, 보안성	1(poor), 2(fair), 3(good), 4(excellant)	4	0~1 사이 구간 숫자
CMM	개발 환경의 성숙도	1(initial), 2(repeatable), 3(defined), 4(immanaged), 5(optimizing)	5	서술적
한국 SW 사업 대가 기준	영향도	0, 1, 2, 3, 4, 5	6	서술적
	품질	상, 중, 하, 불량	4	0~100 사이 구간 숫자
	기능점수, 미디어복잡도, 계획	단순, 보통, 복잡	3	서술적
COCOMO-2	스크린, 문서, 복잡도	단순, 보통, 복잡	3	서술적
	경험, 능력, 프로세스, 팀	VL, L, N, H, VH, Extremly High	6	서술적
	고장 심각성	None, L, M, H, Critical	5	서술적

(2) 정보보호시스템 보안성 평가부문

국제공통 평가기준인 CC(Common Criteria)의 평가지침인 CEM, 유럽의 정보보호시스템 평가기준인 ITSEC, ITSEC의 평가지침인 ITSEM, 미국의 평가기준인 TCSEC, 캐나다의 평가기준인 CTCPEC 및 국내의 평가기준에서 측정 스케일에 관한 지침들을 조사하였다. <표 5>는 정보보호시스템 보안성 평가부문에서의 측정 스케일을 보인다.

<표 5> 정보보호시스템 보안성 평가부문에서의 측정 스케일

기준	측정대상 속성	측정 스케일	구간 수	등급화 기준
CC	보안기능의 보증수준	EAL0~EAL7	8	서술적
한국 정보보호 평가기준	보안기능의 보증수준	K0~K7	8	서술적
ITSEM	보안강도	Not-basicm Basic, Medium, High	3	서술적, 수치
	전문성	laynam, proficient, expert	3	서술적, 수치
	공격시간	minute, day, month	3	수치
	공격장비	unaided, domestic equipment, special equipment	3	서술적, 수치
	공격기회	결탁, 기회, 반전	3	서술적, 수치
	공모	alone, with user, with adm	3	서술적, 수치
CEM	보안강도	High, Medium, Basic, Norate	4	서술적, 수치
	보호(저항) 강도	H, Moderate, Low, No rate	4	수치
	공격경과시간	.5H이하, 1일이하, 1월이하, 1월이상, 기타	5	수치
	전문성	layname, proficient, expert	3	수치
	TOE 지식	none, public, sensitive	3	수치
	TOE 접근시간	.5H이하, 1일이하, 1월이하, 1월이상, 기타	3	수치
	공격장비	none, standard, specialised, bespoke	4	수치

3. 보안 이벤트 스케줄링을 위한 우선순위 알고리즘 구현

3.1. 보안 이벤트 정량화 방법

보안 이벤트 우선순위를 측정하기 위해서는 먼저 보안 이벤트를 정량화해야 한다. 이를 위한 방법으로 유사한 보안 이벤트들을 분류하고 각기 위험성에 따른 위험점수를 부여해야 한다. 아래의

CVE와 CVSS는 이들에 대한 내용이 담겨있는 문서들이며 이를 분석하여 보안 이벤트를 정량화하도록 한다.

3.1.1. CVE 분석

CVE란 공개적으로 알려진 보안 취약점에 대한 공통적인 이름을 제공하는 리스트로써 하나의 취약점에 대응하는 하나의 표준 이름이다. 이것은 이기종 기기들의 같은 명칭으로 취약성을 말할 수 있는 방법이다. 아래는 특징을 나열한 것이다.

<표 6> CVE의 구성

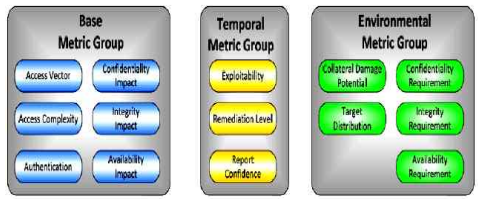
Name
Published Before
Summary
Severity
Attack Range
Vulnerability Type
Loss Type
Vulnerable Elements
Reference Web-site
Vulnerable Versions

- 하나의 취약점에 대응하는 하나의 이름
- 각 취약점에 대응하는 하나의 표준 Description
- 데이터베이스 보다는 사전에 가까운 형식
- 이기종 데이터베이스 혹은 툴이 같은 언어로 말할 수 있는 방법
- 상호 공동운영 및 보안 커버리지 확대의 의미
- 툴 및 데이터베이스간 평가의 기본
- 인터넷에서 조회하거나 바로 다운로드 할 수 있는 접근성

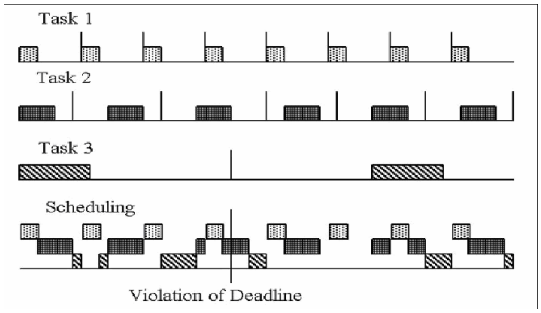
3.1.2. CVSS(Common Vulnerability Scoring System) 분석

여러 종류의 취약점들을 평가하고 확인할 때 사용하며 취약점의 근본적인 특징을 정의하고 전달하려는 목적으로 만들어 졌다. 취약점으로 위험에 처했을 때 올바른 의사결정을 위한 정보를 제공한다.

CVSS는 Base Metric Group, Temporal Metric Group, Environmental Metric Group의 3가지로 구성되어 있다.



(그림 2) CVSS Metric Group



(그림 3) RM으로 스케줄링한 예

(1) Base Metric Group : 사용자 환경을 넘나들며 끊임없이 취약점의 특징을 포착한다. 공격 수행 위치(Access Vector), 공격 복잡도(Access Complexity), 인증 필요여부(Authentication) Metric들은 취약점이 접근하는 방법과 특별한 조건들이 취약점을 공격하기 위해 요구되는지 여부를 포착한다. 3가지 공격영향 Metric은 공격 가능한 취약점이 IT 자산에 직접적으로 영향을 끼치는 방법과 기밀성, 무결성, 가용성의 손상 정도를 독립적인 정의가 가능한지 판단한다.

(2) Environmental Metric Group : 여러 환경에서 취약점은 조직이나 책임자들을 괴롭히는 거대한 잠재적인 위험을 가지고 있다. CVSS Environmental Metric Group은 사용자의 IT 환경과 그와 관련된 취약점의 특징을 잡아낸다. Environmental Metric이 옵션이기 때문에 점수에 영향을 주지 않는 개별적인 Metric 값을 갖는다. 이 값은 사용자가 특별한 Metric을 적용할 수 없을 때나, 건너뛰고 싶을 때 사용된다.

3.2. 이벤트 관리 우선순위 스케줄링 기법

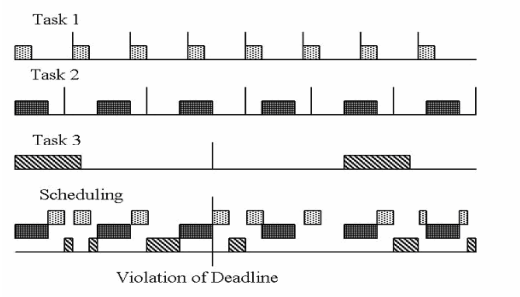
처리해야 할 대상에 우선순위를 부여하며, 우선순위에 따라 스케줄링 하는 순서대로 처리하는 기법으로 정적(Static) 우선순위 방법과 동적(Dynamic) 우선순위 방법이 존재한다. 이 방법들에 대한 연구를 통해 우선순위 알고리즘에 따른 보안 이벤트 관리 스케줄러를 개발한다.

3.2.1. 정적 우선순위 방법

컴파일 시 모든 대상에 우선순위를 부여하여, 실행 중 우선순위를 변경하지 않는 방법으로 동적 우선순위 방법에 비해 구현이 쉽고 시스템 오버헤드가 적다는 장점을 지니고 있지만 환경변화에 적응하지 못한다는 단점이 존재한다. Rate Monotonic(RM), DeadLine Monotonic(DM)이 있다.

(1) Rate Monotonic(RM)
- Task의 생성 주기가 가장 짧은 Task가 가장 높은 우선순위로 고정된다.
- Dispatcher는 항상 가장 높은 우선순위 Task를 Dispatch한다.

(2) Deadline Monotonic (DM)
- Deadline이 가장 짧은 Task가 가장 높은 우선순위로 고정된다.
- Dispatcher는 항상 가장 높은 우선순위 Task를 Dispatch한다.



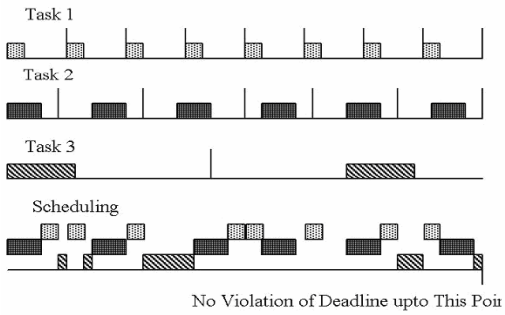
(그림 4) DM으로 스케줄링한 예

3.2.2. 동적(Dynamic) 우선순위 방법

응용프로그램 실행 중 작업의 우선순위를 바꿀 수 있는 방법으로 상황 변화에 대한 적응이 가능하며, 시스템의 응답속도를 증가시켜 보다 효율적이다. 하지만 구현이 복잡하고 오버헤드가 많다는 단점이 있다. Earliest DeadLine Firest(EDF), Time Driven Scheduler(TDS), Least Laxity First(LLF), Shortest Remaining Time(SRT)가 있다.

(1) Earlist Deadline First(EDF)
- Optimal, Dynamic preemptive 스케줄링으로 우선순위가 동적으로 변한다.
- 가장 짧은 Deadline을 가진 Task가 가장 높은 우선순위를 가진다.
- 새로운 Task가 도착할 때마다 우선순위가 조정된다. Dispatcher는 항상 가장 높은 우선순위의 Task를 Dispatch한다.
- 구현이 어렵다는 단점이 있지만 Processor 활용도가 100%에 이르고 가장 효율적인 알고리즘이란 것이 증명되었다.

(2) Time Dirven Scheduler(TDS)
- EDF를 확장한 알고리즘으로써 Task 스케줄링은 Deadline에 따라 스케줄링 하는 것이 EDF와 같으나, TDS는 과부하 상태를 다룰 수 있다.
- 만약 과부하 상태가 발생하면 스케줄러는 Deadline을 맞추지 못하더라도 그 Task를 중지한다.
- Overload 상태가 계속되면 스케줄러는 비중이 낮은 작업을 제거한다.
- Row value density는 Task의 중요도에 의해 결정된다.



(그림 5) EDF로 스케줄링한 예

(3) Least Laxity First(LLF)

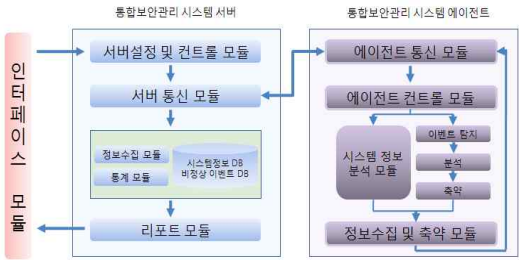
- 가장 여유시간이 짧은 작업에 우선순위를 주는 알고리즘이다.
- 여유시간은 마감시간까지 남아있는 Processing Time이 가장 여유가 없는 작업을 말한다.
- 여유시간을 계산할 방법이 모호하다.
- 여유시간이 계산 된다고 해도 EDF 보다 이론적 성능이 떨어진다.

(4) Shortest Remaing Time(SRT)

- 비 선점 방식인 SJF 방식을 선점 형태로 바꾸어 놓은 것이다.
- 어떤 프로세스를 실행하고 있다가, 새로운 프로세스가 들어오면 둘 중 남은 CPU 요구 시간을 비교하여 더 짧은 CPU 시간을 가지는 프로세스를 Running 시키는 방법이다.

3.3. 전체 시스템 구성

하드웨어 성능이 발전하지 못했던 과거에는 네트워크 기반의 위협관리 시스템이 각광을 받았지만, 하루가 다르게 발전하는 다양한 위협을 탐지 및 관리하기에는 많은 애로점이 있다.



(그림 6) 보안 이벤트 스케줄러 기반의 통합보안관리 시스템 내부 구성도

현재는 네트워크 기반의 위협관리 시스템과 호스트 기반의 위협관리 시스템을 혼용하여 사용하고 있으며, 이들 시스템도 보안의 관리를 위한 시스템이 아닌 보안 시스템 및 시스템 모니터링, 네트워크 모니터링 시스템을 혼용 운용(ESM : Enterprise Security Management)하고 있다. 이는 관리자에게 더 많은 지식과 업무의 부담을 주고 있으며, 관리하는 시스템은 더욱더 증가하는 초례를 가지고 있다. 따라서 이러한 ESM의 단점을 보완하고 하나의 시스템으로 종합적으로 위협을 탐지하고 분석/평가를 하는 통합보안관리 시스템 개발을 하였다. 세부 개발 항목은 다음과 같다.

- 네트워크 보안 시스템 관리 자동화 점검 기술 개발
- 네트워크 보안 시스템 능동적 위협관리 기술 개발
- 네트워크 보안 시스템 관리 자동화 기술 개발
- 네트워크 통합 보안 관리 기술 개발
- 국제 표준 평가기준(CVE/CVSS)를 데이터 무결성 분석평가 보호 프로파일 작성에 적용
- 보호 프로파일을 토대로 데이터 무결성 평가분석 항목과 시나리오를 작성

4. 검증

4.1. 시스템 기능

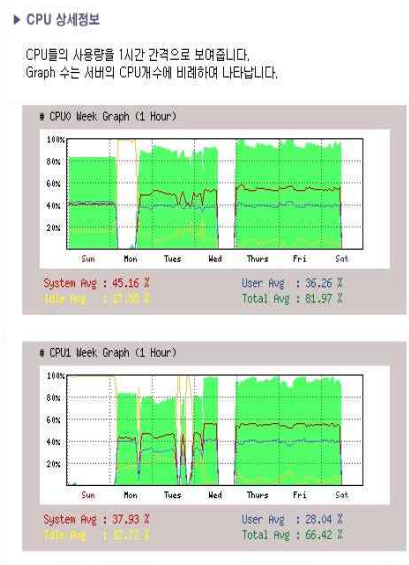
4.1.1. 시스템 실시간 통합 모니터링

보안관리자는 각 정보보호시스템의 성능 관리상태 및 비정상 이벤트 정보를 웹을 통해 실시간으로 통합 모니터링 할 수 있다.

(그림 7) 정보보호 시스템 실시간 모니터링

(그림 8) CPU 정보

(그림 9) 비정상 이벤트 탐지



(그림 10) 상세 CPU 정보

4.1.2. 주기별 보고서 자동화

보안관리자는 일일, 주간, 월간 및 연간 점검에 대한 보고서를 관리자가 원하는 날짜와 시간에 보고서로 출력 할 수 있다.

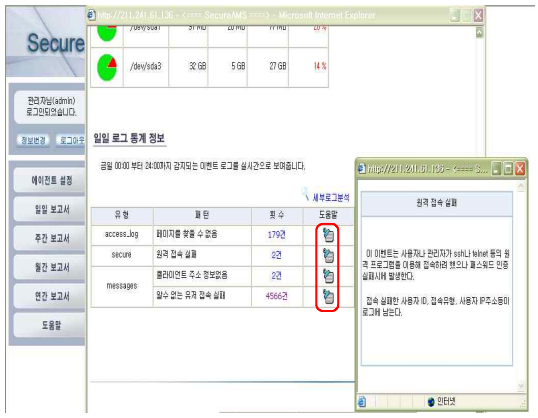
(그림 11) 주간 보고서

4.2 비정상 이벤트 탐지 및 분석

정보보안시스템 및 주요 데몬에서 발생되는 비정상 이벤트를 수집 및 축약해서 보안 관리자에게 제공한다.

4.3 비정상 이벤트에 대한 상세한 도움말 기능

정보보호 시스템의 비정상 이벤트에 대한 상세한 도움말을 제공되어, 비전문가도 쉽게 이해할 수 있다.



(그림 12) 비정상 이벤트 도움말

5. 결 론

인터넷의 급격한 확산과 그것을 이용하는 응용 프로그램의 수가 급격히 증가함에 따라 인터넷을 사용하는 사용자 수가 급격히 늘어나고 있다. 그로 인해 최근 이루어지는 사이버 공격들의 형태가 점점 더 다양해지고, 공격의 전파 속도가 빨라지고 있으며, 이로 인해 입게 되는 시간적, 경제적 피해 규모는 상당하다. 따라서 기존의 침입탐지 기법으로는 이러한 공격을 신속히 탐지, 차단이 힘들어졌다.

과거 보안 상황 분석기술에는 이벤트 특성에 따른 분류로써 침입탐지 시스템이나 방화벽 등에서 수집한 이벤트를 분석하여 침입 또는 공격이 있었는가를 판단하는 것과 네트워크의 패킷을 분석하여 트래픽의 이상 상태 여부를 판단하는 것이 주를 이루었다. 그리고 분석 방법에 따른 분류로써는 로그 기록을 분석하여 공격자의 시그니처를 찾는 오용탐지와 정상적인 행동을 기반으로 비정상적인 행동을 찾는 비정상행위 탐지가 있다. 하지만 이와 같은 방법들은 최근 폭발적인 이벤트 양과 오탐율 때문에 신속성을 요구하는 공격의 분석과 알려지지 않은 공격 등을 판별하는데 있어서 많은 문제점을 가지고 있다. 최근에 이와 같은 문제를 해결하기 위해 네트워크 보안 이벤트에 관한 연구들이 매우 활발히 진행되고 있다.

본 논문 역시 이러한 이벤트에 관한 연구 중 하나로 보안 이벤트의 발생 상황, 어떤 이벤트가 발생하였는지, 그 이벤트의 위험, 위협 정도를 판단하여 우선순위를 판단하고, 그 공격에 대한 능동적인 대응을 목적으로 국내·외 통합보안관리시스템 동향에 맞추어 개발한 것이다. 이러한 점에서 국내 정보보안시장의 활성화에 조금이나마 기여하고, 나아가 세계 보안 시장에서 국가 경쟁력 확보에도 기여하여 국가적 이득으로 생각해 볼 때 중요한 자료가 될 것이다. 또한 네트워크 환경에 맞는 더욱 더 빠른 보안 이벤트 처리가 가능하여, 그동안 발생 가능했던 손실을 줄여 국가적, 기업적 차원에서의 기술, 경제에 대한 손해를 막을 수 있을 것으로 기대되며, 이를 통해 IT 선진국으로서의 위치를 공고히 다질 것이다.

참고문헌

[1] Internet Security - Mission Critical, Techpress Inc, 2015.

[2] W.Richard Stevens, "UNIX Networking Programming", Vol.1, 2nd Ed., 1998.

[3] Robert L. Ziegler, "Linux Firewalls", New Riders, 2014.

[4] Sean Walton, "Linux Socket Programming", SMS, 2011.

[5] AnalyZ Demonstration Copy User Guide, Zergo Limited, June 2015.

[6] Welcome to the World of BDSS, and OPA Inc. The Integrated Risk Management Group, OPA Inc., Janury 2016.

[7] ZUM Strarten hier kicken, "IP VPN Solution for Service Provider“ , Cisco Systems, 2015.

[8] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 2015.

[9] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload(ESP)“, RFC 2406,November 2015.

[10] Zenkins, Buddy, Security Analysis and Management Manual, Countermeasures Inc, 2014.

[11] Tom Olzak, Improve data protection processes with content discovery, monitoring and filtering, 2017.

[12] Jay Heiser, Understanding data leakage, Gartner, 2017.

[14] R. Erbacher, K. Christensen, and A. Sundberg, “Designing Visualization Capabilities for IDS Challenges,” IEEE Symp. on Information Visualization’s Workshop on Visualization for Computer Security (VizSEC), Oct. 2015.

[15] 한국 전자통신 연구원, ESM 개발 동향, 2013.

[16] 한국정보보호진흥원, “국제공통평가기준(v.3.1)", 2015.

[17] 펜타 시큐리티 시스템(주), “자동화된 위험분

석 틀의 구현", 2015.
[18] 정보통신부,"정보보호 중장기(2006~2010) 기본계획안", 2016.
[19] 국정원, 첨단 산업기술 보호동향, 제12호, 2018.
[20] 이철수, 한명묵, 정보 보호 개론(개정판), 정익사, 2016.

〔저자소개〕

전 은 아 (Eun-A Jun)
1999년 2월 원광대학교
전자재료공학과 공학사
2001년 8월 원광대학교
전자계산교육 교육학석사
2011년 8월 고려대학교
정보보호공학전공 박사
2017년 3월~ 현재 남서울대학교
컴퓨터소프트웨어학과
외래교수
email : eunajun@gmail.com

김 점 구 (Jeom Goo Kim)
1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교
컴퓨터학과 교수
email : jgoo@nsu.ac.kr