Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.6, Dec. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.6.1489

TF-IDF를 이용한 침입탐지이벤트 유효성 검증 기법

김 효 석,[1†] 김 용 민[2‡]
[1]전남대학교 정보보안협동과정, [2]전남대학교 전자상거래전공

A Validation of Effectiveness for Intrusion Detection Events Using TF-IDF

Hyoseok Kim,[1†] Yong-Min Kim[2‡]
[1]Interdisciplinary Program of Information Security, Chonnam National University
[2]Dept. of Electronic Commerce, Chonnam National University

요 약

웹 애플리케이션 서비스의 종류가 다양해짐과 동시에 사이버 위협이 급증하여 침입탐지에 대한 연구가 계속되고 있다. 기존의 단일 방어체계에서 다단계 보안으로 진행됨에 따라 대량의 보안이벤트 연관성을 분석하여 명확한 침입에 대해 대응하고 있다. 그러나 대상시스템의 OS, 서비스, 웹 애플리케이션 종류 및 버전을 실시간으로 점검하기 어려운 측면이 있고, 네트워크 기반의 보안장비에서 발생하는 침입탐지 이벤트만으로는 대상지의 취약여부와 공격의 성공여부를 확인 할 수 없는 문제점과 연관성 분석이 되지 않은 위협의 사각지대가 발생할 수 있다. 본 논문에서는 침입탐지이벤트의 유효성을 검증하기 위한 기법을 제안한다. 제안된 기법은 공격에 상응하는 대상시스템의 반응을 사상(mapping)하여 응답트래픽을 추출하고, TF-IDF를 통해 라인(line)기반으로 가중치를 환산하고 높은 수치부터 순차적으로 확인하여 대상시스템의 취약여부와 유효성이 높은 침입탐지이벤트를 검출하였다.

ABSTRACT

Web application services have diversified. At the same time, research on intrusion detection is continuing due to the surge of cyber threats. Also, As a single-defense system evolves into multi-level security, we are responding to specific intrusions by correlating security events that have become vast. However, it is difficult to check the OS, service, web application type and version of the target system in real time, and intrusion detection events occurring in network-based security devices can not confirm vulnerability of the target system and success of the attack A blind spot can occur for threats that are not analyzed for problems and associativity. In this paper, we propose the validation of effectiveness for intrusion detection events using TF-IDF. The proposed scheme extracts the response traffics by mapping the response of the target system corresponding to the attack. Then, Response traffics are divided into lines and weights each line with an TF-IDF weight. we checked the valid intrusion detection events by sequentially examining the lines with high weights.

Keywords: Intrusion Detection, Web Traffic Analysis, Text Mining, TF-IDF

I. 서 론

오늘날 인터넷의 보급이 일반화되고 기업의 자산이 데이터화함에 따라 각각의 애플리케이션이 갖는 취약점을 이용한 많은 사이버 위협이 발생하고 있다. 특히, 웹 공격을 유발하는 공격도구와 온라인 사이트 등이 인터넷을 통해 전파되면서 공격이 증가하는 추세이며, 2018년 상반기 웹 관련 취약점은 전체 취약점의 46.3%를 보인다[1]. 이에 따라 기업들은 네트워크 기반의 보안장비(IPS, IDS, 방화벽 등)를 이

Received(09. 27. 2018), Modified(10. 30. 2018), Accepted(10. 30. 2018)
† 주저자, chil530@naver.com
‡ 교신저자, ymkim@chonnam.ac.kr(Corresponding author)

용하여 내부 네트워크를 보호하고 있다. 위협트래픽을 자동차단하는 비율이 20~30% 정도이며[2], 차단되지 않는 경우는 위협 트래픽이 내부 네트워크로 유입되었다는 것을 의미하여 추가적인 분석이 필요하다. 기존의 네트워크 보안장비는 침입탐지의 내용을 알림 형태로 경고를 생성하기 때문에 대응과 관련된 절차에는 관여하기 어렵다. 위협트래픽을 자동으로 방어할 수 있는 침입대응시스템(IRS)이 연구되고 있으나 오탐대응, 불확실성, 대응과 의사결정의 메커니즘 개발비용 요구, 부적절한 대응이 실행될 수 있다[3,4]. 이러한 문제들은 서비스에 직접적인 영향을 미칠 수 있기 때문에, 현재까지 사람이 모니터링 및 대응하고 있다. 그러나 보안이벤트를 발생량 대비 처리량을 비교했을 때, 한 개도 빠짐없이 분석하는 것은 불가능하고 신종 해킹공격에 대한 대응능력이 부족하여 휴먼에러(human error)가 발생할 수 있는 여지가 있다[5]. 기존의 보안인프라는 다단계 보안과 연관성 분석이 제시되었으나, 기존의 탐지 및 차단기법으로는 이러한 문제들을 모두 해결하기 어렵고, 웹 서버가 출력하는 웹문서의 응답트래픽을 통해 비정상적인 증상을 원천지의 컴퓨터에게 전달하는 것으로 분석된다[6].

본 논문에서는 웹 관련 침입탐지이벤트에 상응하는 대상시스템의 응답트래픽을 추출한다. 저장한 응답트래픽을 TF-IDF를 이용하여 공격에 대한 서버의 반응에 높은 가중치를 부여하고 침입탐지이벤트의 유효성을 검증하여 자산(assets)에 영향을 미칠 수 있는 이벤트를 구분하고 순차적으로 검증 할 수 있는 기법을 제안한다.

II. 관련 연구

2.1 계층적 방어체계와 보안이벤트

오늘날 보안 아키텍처의 근간을 이루는 계층적 방어체계(defense in depth)는 Fig.1.과 같이 전체 시스템의 보안 수준을 강화하기 위한 계층의 단계적 보안 메커니즘이다. 하나의 방어 메커니즘이 뚫린 경우라도 또 다른 방어 메커니즘이 전체 시스템을 방어할 수 있는 구조로 단일실패지점(single point of failure)과 약한 고리 이론(weakest link of the chain)을 예방할 수 있다[6,7]. 계층적 방어 체계에서 위협트래픽이 자산에 도달하였을 때, 단일보안장비들의 이벤트를 확인하여 침해여부를 판단한다.

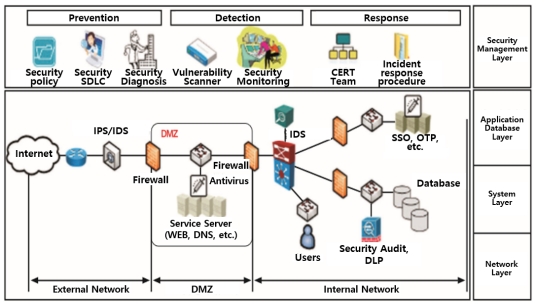

Fig. 1. Hierarchical security practices for Web-centric business[7].

그러나 발생된 모든 보안이벤트를 확인하는 것이 비효율적이고 많은 비용이 발생하게 한다.

이러한 문제로 인해 단일보안장비에서 발생하는 이벤트를 관리 할 수 있는 솔루션(ESM)과 최근에는 빅데이터 기반의 검색 및 분석 솔루션(SIEM)이 등장하여 다양한 측면에서 사이버 위협을 분석 할 수 있게 되었지만, 이기종 보안 솔루션에서 발생하는 이벤트의 항목들이 상호 비교 가능할 정도로 표준화되어 있지 않으며, 각각의 솔루션에서 위협정보의 갱신이 실시될 때, 탐지할 수 있는 위협의 세부적인 범위에 대한 연관성을 추가 구성해야 한다.

2.2 이벤트 상관관계 분석

상관분석(correlation analysis)의 대표적인 시스템인 SIEM(Security Information and Event Management)은 인프라 보안을 위해 다양한 종류의 장비에서 발생하는 이벤트를 수집 및 상관관계 분석하여 위협을 알린다[8].

기존의 연구에서는 대용량의 보안이벤트에서 중요하지 않은 보안이벤트를 필터링하거나 연관관계 분석을 통해 위험하다고 판단되는 보안이벤트만을 추출하기 위한 연구가 주를 이루고 있다. 최근의 상관관계와 관련된 연구는 이벤트별 분석방법을 다르게 하여 별도의 분석규칙과 상관관계를 분석하는 방법, 이기종의 보안장비의 개별 로그들의 데이터 필드를 연구하여 상관관계를 분석하고 다양한 사례의 시나리오로 침해사고를 탐지하는 방법, 취약점 진단의 결과를 DB에 저장하여 자산의 소프트웨어 취약점에 대한 정보를 인지하고, 취약 여부를 기준으로 위험도를 산정하여 분석하는 방법 등[9-11]이 연구되고 있다.

이벤트 상관관계 분석 연구가 계속되고 있는 이유 중 하나는 기존의 이기종 보안장비의 이벤트 및 로그

를 가지고는 다양한 위협에 대해 상관관계를 분석할 변수(data)가 부족하고, 단편적으로만 확인이 가능하다. 공격에 의한 자산의 영향 범위, 심각도를 판단하기 위해서는 공격의 유효성을 검증할 수 있는 실증적 증거(log)를 기록하고 분석해야 한다.

2.3 빅 데이터 분석 기법

빅 데이터 분석 기법의 발전과 함께 시스템의 성능이 좋아지면서 이상탐지 시에 기계학습을 적용한 연구가 진행되고 있다. 다양한 데이터마이닝 알고리즘을 이용하여 로그 기반의 이상거래를 탐지하는 연구사례들이 있으며[12], 텍스트마이닝을 사용하여 스팸과 정상문자에서 의미 있는 단어를 구분하고 데이터 셋을 구성하여 스팸문자 집합에서 동시 출현 단어를 분석하여 탐지하는 기법[13]도 연구되고 있다.

빅 데이터 분석 기법 중 텍스트마이닝의 벡터공간 모델(vector space model)은 텍스트 문서의 색인어(index term)와 같은 식별자들을 벡터로 나타내는 대수적인 모델이다. 문서(document)는 벡터로 표현되며, 각각의 차원(dimension)은 개별 단어(term)에 대응된다. 단어의 정의는 응용분야에 따라 다르며, 일반적으로 단어, 키워드(keyword), 긴 구문 등이 될 수 있다. 단어가중치(term weight)를 계산하는 데에는 여러 방법이 있으며, 가장 잘 알려진 방법 중 하나는 TF-IDF(Term Frequency Inverse Document Frequency) 가중치를 구하는 방법이다. TF-IDF에서 TF는 단어의 빈도이다. 특정한 단어가 문서 내에 얼마나 자주 등장하는지를 나타내며, 이 값이 높을수록 중요하다고 생각할 수 있다. 하지만 단어 자체가 문서군 내에서 자주 사용되는 경우엔 흔하게 등장한다는 것을 의미한다. 이것을 DF라고 하고, 이 값의 역수는 IDF라고 한다. TF-IDF는 TF와 IDF를 곱한 값이다[14].

기존의 연구들은 로그와 같은 문자의 집합 등에서 특정 텍스트의 빈도나 군집(clustering)을 통해 연관된 데이터를 추출하여 보다 정밀한 분석이 가능하게 되었지만, 공격이 다양해지면서 위협과 관련된 정책과 지침 그리고 데이터 셋에도 변화가 발생하게 된다. 그리고 비정상행위에 대해서는 실시간 분석이 가능하여야 한다. 본 논문에서는 웹에서 발생하는 침입탐지이벤트의 비정상행위에 대한 반응들을 실시간 추출한다. 추출한 데이터를 텍스트마이닝 기법을 사용하여 비정상행위의 대표반응에 높은 가중치를 산출하고 가중치가 높게 부여된 라인을 순차적 분석하여 이벤트 검증과 취약여부를 확인한다.

III. TF-IDF 침입탐지이벤트 유효성 검증

계층적 방어체계의 인프라에서 발생하는 보안이벤트를 상관관계분석 할 때, 유해트래픽의 탐지에 대한 명확한 근거를 갖게 하는 점은 우수하지만 실제 대응과 관련된 정보를 확인하는 것은 어려운 점이 있다. 대상시스템에 트래픽이 유입될 때, 발생하는 이벤트들은 제한적이고 상관관계분석으로 공격의 성공여부를 알 수 없는 측면이 있어 동일한 트래픽을 재생(reply)하거나, 네트워크 덤프솔루션에서 추가적인 분석을 요구하게 된다. 재생하여 분석하는 경우에는 공격자와 분석자가 획득하는 응답은 서로 상이할 수 있고, 이벤트마다 네트워크 덤프솔루션에서 트래픽을 추출하여 검증하는 것은 많은 시간과 비용을 투자하게 된다.

따라서 본 연구에서는 Fig.2.의 구성으로 공격에 상응하는 대상시스템의 반응을 사상하고 확보한 응답 트래픽에 TF-IDF 가중치를 환산하여 유효성이 높은 침입탐지이벤트를 검출하고자 한다.

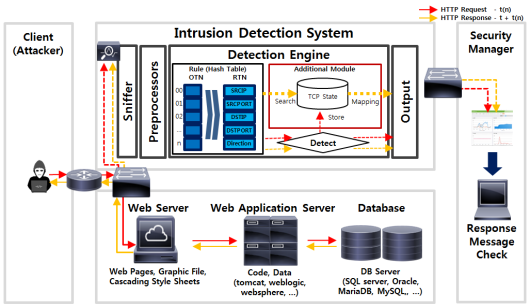

Fig. 2. HTTP Response Traffics Extraction Diagram

3.1 웹 응답 트래픽 추출 과정

웹 통신 중 HTTP가 가장 많이 사용되고 있다. HTTP는 무상태 프로토콜(stateless protocol)의 자체적인 기능으로 상호간에 인증데이터를 저장하는 메커니즘이 없음으로 서버는 사용자의 요청, 인증과 관련된 내용을 기억할 수 없다. HTTP는 TCP를 사용하는 대표적인 프로토콜이지만 지속적인 연결이 필요하지 않는 웹 서비스 특성상 TCP 상태를 종료

하기 때문에 HTTP 쿠키나 세션을 이용하여 추출하는 것에 어려움이 있다. 따라서 TCP/IP 응용계층에서 HTTP 요청에 상응하는 응답을 추출하는 것은 한계가 있어 전송계층에서 TCP 상태를 추적하여 응답트래픽을 추출한다. 즉, 클라이언트의 요청이 끝날 때, Table 1.의 No. 7-9번과 같이 응답(Ack)이 순서번호(Seq)와 뒤바뀌게 되고 데이터가 전송되는 점을 활용(Flag가 P, MSS의 값의 크기)하여 요청에 대한 응답을 구하고 이후에 발생되는 요청에 대해서는 추적하지 않는다.

Table 1. TCP status in HTTP (Compare Sequence Number with Acknowledgement)

No	SPort	DPort	Seq	Ack	Flag	MSS
1	9159	80	57fc1991	00000000	S	-
2	80	9159	d0ac8312	57fc1992	S,A	-
3	9159	80	57fc1992	d0ac8313	A	-
4	9159	80	57fc1992	d0ac8313	P,A	1354
5	9159	80	57fc1edc	d0ac8313	A	1460
6	80	9159	d0ac8313	57fc2490	A	0
7	9159	80	57fc2490	**d0ac8313**	P,A	1178
8	80	9159	**d0ac8313**	57fc292a	A	0
9	**80**	**9159**	**d0ac8313**	57fc292a	**P,A**	**1323**
10	9159	80	57fc292a	d0ac883e	A	0
11	80	9159	d0ac883e	57fc292a	F,A	-
12	9159	80	57fc292a	d0ac883f	A	-
13	9159	80	57fc292a	d0ac883f	F,A	-
14	80	9159	d0ac883f	57fc292b	A	-

3.2 웹 응답 트래픽 전처리 과정

침입탐지시스템에서 TCP 상태 값을 활용하여 확보한 응답트래픽을 Fig.3.와 같은 흐름으로 전처리한다. 응답트래픽에는 Interval Time, IP, TCP, Port, 메시지크기, 텍스트데이터로 구성되어 있다.

① 시간분석: 웹 기반 공격 중 서버의 자원을 지속적으로 할당 받거나 특정 파라미터의 취약점을 확인하기 위한 시간기반 공격을 진행하는 경우를 탐지하기 위해 시간차이를 구하여 비정상적인 트래픽을 별도 구분한다.

② 상태코드 분류: HTTP 상태코드는 대표적으로 '1xx'(조건부응답), '2xx'(성공), '3xx'(리다이렉션), '4xx'(요청오류), '5xx'(서버오류) 5가지로 분류된다.

상태코드별로 응답페이지의 양식이 다르기 때문에, 상태코드별 사용되는 응답 라인들의 가중치의 변화가 있을 수 있다. 또한 상태코드 별 의미하는 바가 상이하기 때문에 1차 분류한다.

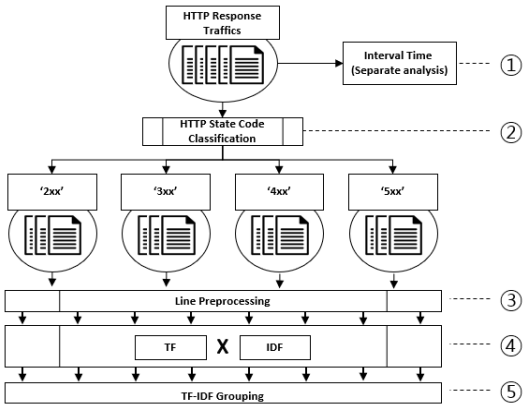

Fig. 3. Preprocessing HTTP Response Traffics

③ 라인(line) 전처리: 공격에 유효한 라인에 높은 가중치를 환산할 수 있도록 전처리 과정이 필요하다. 일반적인 단어 전처리(자음이나 모음만 있는 경우, 특수문자, 구두점 등 제거)과 다르다. 단어기반으로 전처리하는 경우 데이터의 양이 많아지게 되고 분류된 단어가 공격에 대한 서버의 취약반응인지, 일반적인 내용인지 구분하기 어렵고, 단어의 출처가 불분명해진다. 예를 들어 "Duplication entry 'qvzkq1qzzjq1' for key 'group_key' 라는 오류 메시지가 노출되었을 때, 단어기반으로 분류하게 되면 'Duplication', 'entry', 'for' 등은 일반적으로 사용되는 단어로 가중치가 낮게 나올 수 있고, 'qvzkq1qzzjq1'은 가중치가 높게 환산되지만 단어의 출처를 확인할 수 없으며, 취약반응으로 단정하기 어려워 추가적인 분석이 필요하다. 이러한 점 때문에 라인 기반으로 분리하고 전처리한다.

④ TF-IDF: TF-IDF 가중치를 환산한다.

$$TF_{td} = \frac{n_{td}}{N_d} \quad (1)$$

수식(1)에서 TF의 n_{td}는 응답데이터(d)에 포함되는 라인(t)의 출현 빈도이며 N_d는 응답데이터(d)에 출현한 모든 라인의 수이다.

$$IDF_t = \log\frac{D+1}{D_t} \quad (2)$$

수식(2)에서 D는 응답데이터군에서 응답데이터들의 총 개수이며, 라인(t)가 출현하는 문서의 수인

D_t를 이용하여 계산한다. 즉, IDF는 응답데이터의 총수(D)에 1을 더한 값을 특정 라인(t)가 출현하는 문서의 수(D_t)로 나눈 값의 log 값이다. 이후 TF와 IDF를 곱하여 가중치를 환산한다.

⑤ TF-IDF Grouping: TF-IDF를 이용하여 정제한 수치데이터를 기반으로 문자열 정렬을 실시한다. 취약반응으로 나타나는 라인들은 '특정페이지 전체내용', '특정파라미터에 대한 반응들'처럼 가중치 값이 유사하게 표현되기 때문에 그룹화 할 수 있다. 그룹핑한 데이터의 가중치 값이 높은 순서대로 분석을 실시한다.

3.3 침입탐지이벤트 유효성 검증

HTTP 응답은 브라우저에서 해석 가능한 웹문서의 구조를 가지고 있다. 이 구조의 특성을 이용하여 같은 페이지 또는 서로 다른 페이지에서 라인을 비교하고 TF-IDF 가중치를 부여하여 취약하지 않은 라인을 구별하고, 서로 다른 라인을 갖는 내용들에 대해서는 높은 가중치를 부여하여 취약반응이 일어날 수 있는 구간을 정의하도록 하였다.

Fig.4.는 공격에 의해 발생한 실제 응답트래픽이다. 응답라인에서 '〈html〉〈head〉', '〈!DOCTYPE HTML ~〉' 태그처럼 모든 응답트래픽에 포함되는 라인인 경우 가중치가 가장 낮게 추출된다. '〈title〉404 Bad Request〈/title〉', '〈h1〉 NOT FOUND〈/h1〉'는 상태코드가 404인 경우가 다수 발생한다면 그 다음으로 낮은 수치로 환산된다.

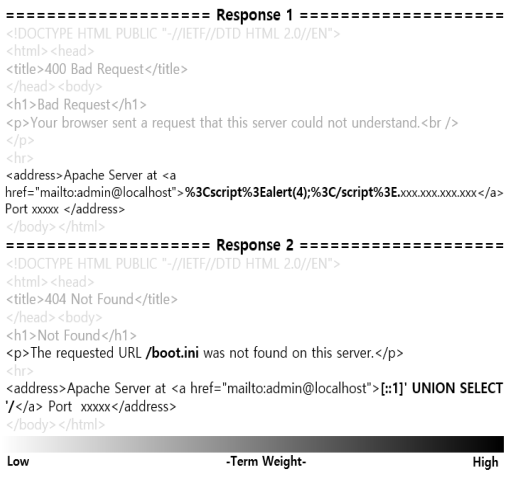

Fig. 4. Responses of server with status code '4xx' by attack

그러나 '〈address〉' 태그의 내용의 경우 공격구문이 포함되어 가중치 계산 시 높은 가중치를 갖게 되면서 공격에 대한 서버의 반응이 나타나는 부분으로 확인할 수 있다.

Fig.5.에서 전체 프레임을 구성하고 있는 정사각형은 신뢰구간과 비 신뢰구간을 구별하며, 구간 내 사각형(page X)은 크기나 형태로 서로 다른 응답트래픽이다. 각각의 응답트래픽들을 겹쳐 맞추었을 때, 겹치는 횟수가 많을수록 일반적으로 사용되는 HTML형식의 라인으로 구분되어 신뢰구간에 표현될 수 있고 신뢰구간에 포함되지 못하는 라인들은 공격요청에 대한 서버의 특별한 반응으로 확인할 수 있다. 즉, 공격요청에 대한 응답트래픽 데이터들을 라인기반으로 분리하여 상호 검증한다[15].

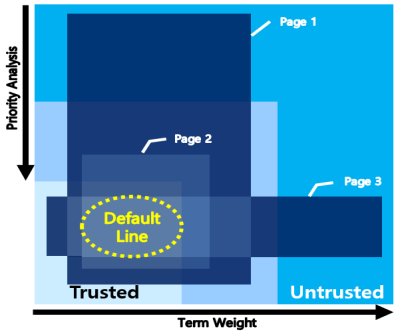

Fig. 5. Validation through line segmentation of response page

IV. 실험 및 분석

4.1 실험 방법

외부에서 내부로 웹 공격이 발생하는 경우에 공격자 IP, 공격벡터, 공격유형, 대상 서버IP의 수에 따라 여러 가지 유형이 나타난다. 또한, 웹을 통해 서비스를 제공하는 모든 기업의 인프라 구조가 동일하지 않고 서버환경설정, 보안장비, 시큐어코딩 등 보호조치가 상이하기 때문에 제안기법의 객관적인 결과를 도출하는 것에 제약이 있다. 그리하여 본 실험에서는 취약한 웹 서버인 DVWA[16]에 Appscan과 Sqlmap 2가지의 공격도구로 트래픽을 발생시키고 이를 침입탐지시스템으로 잘 알려진 Snort를 이용하여 탐지한다. 이후 제안한 기법을 이용하여 웹서버의 취약점 여부와 유효한 침입탐지이벤트를 검

출한다. Appscan 도구(release. 2017. 12)를 이용한 실험은 웹 서버에서 제공하는 모든 페이지(page)를 공격하였다. Sqlmap 도구(release. 2018. 01)를 이용한 실험은 하나의 특정 파라미터(parameter)로만 SQL Injection을 수행하며 실험에서 사용한 웹 관련 규칙(14,255개)은 Snort와 Suricata 엔진에 적용되는 Community, ET Rule[17,18]을 사용하였다.

4.2 실험 내용

공격도구를 이용하여 트래픽을 발생시켰을 때, Snort에서 탐지된 내용인 트래픽 발생 건수, 탐지된 규칙의 수, 탐지 수, 과잉탐지(over-detection)의 수를 Table 2.에 표기하였으며, 과잉탐지 항목은 Snort의 유사규칙에 의해 동일한 트래픽을 다수 탐지하게 되는 경우를 합산하였다. Appscan의 실험은 OWASP Top10[19]의 항목을 기준으로 Table 3.에 상세내용을 보였다.

Table 2. Intrusion detection events detected in the experiment

Tool	HTTP-Request	Snort Matching		
		Rule	Detection	Over detection
Appscan	6,668	291	9,916	3,268
Sqlmap	414	18	1,102	683

Table 3. Details of detected intrusion detection events in experiments using the Appscan tool

OWASP Top10	HTTP-Request	Snort Matching		
		Rule	Detection	Over detection
A1	1,125	29	2,971	1,846
A2	561	4	568	7
A3	10	1	10	0
A4	1	1	1	0
A5	1,702	25	2,409	727
A6	131	7	184	53
A7	1,924	63	2,190	266
A8	470	2	471	1
A9	6	3	8	2
A10	-	-	-	-
Etc.	738	156	1,104	366
Total	6,668	291	9,916	3,268

4.3 실험 분석

4.3.1 Appscan 도구를 이용한 검증

Appscan 도구로 웹 서버의 모든 페이지에 트래픽을 발생하면 침입탐지이벤트의 수는 총 9,916건으로 탐지되었으나 그 중 3,268건은 유사 규칙에 의해 과잉탐지이며 발생트래픽에 상응하는 응답트래픽은 6,668건('2xx': 2,603건, '3xx': 1,070건, '4xx': 2995건)이 확인되었다. 응답코드가 '2xx'인 경우, 가장 높은 가중치를 갖는 라인은 공격구문이 그대로 반환되는 라인들의 집합으로 확인되었다. 다음으로 높은 가중치를 갖는 라인들은 XSS, Directory Listing 공격 등으로 확인되었다.

Fig.6.에서 가중치가 높게 나타난 취약라인들은 HTML 태그를 포함하고 있기 때문에 〈html〉, 〈/html〉 태그만 존재하는 파일을 작성하여 Fig.7. 처럼 취약여부를 쉽게 확인할 수 있었다.

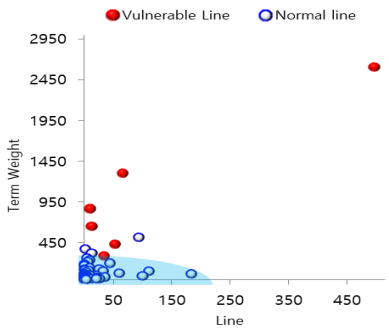

Fig. 6. Distribution of lines in the experiments with Appscan tool

Fig. 7. Analysis of vulnerable lines (ex. XSS, 496 : 2604(line : term weight) in Fig. 6.)

4.3.2 Sqlmap 도구를 이용한 검증

Sqlmap 도구는 웹페이지 내에 하나의 특정 파라미터로 트래픽을 발생시켰을 때, Snort에서 1,102건('2xx': 414건)이 탐지되었고 추출한 응답트래픽은 414건으로 확인되었다. '2xx'응답에서 실제 공격에 성공한 요청건수는 135건이다. 공격구문이 포함된 응답 중 DB 정보가 확인된 라인은 132건이고 Mysql 매뉴얼의 내용이 반환된 라인은 155건으로 확인되었다. DB 오류와 관련된 내용은 2건이 탐지되어 해당 라인들은 높은 가중치를 가지고 있었다.

Fig.8.에서 가중치가 가장 높은 457건의 라인들 중 132건의 라인은 Fig.9.처럼 SQL Injection 공격에 대한 서버의 반응으로 웹서버의 DB정보가 나타났으며 공격도구가 Hex 값을 이용하여 DB 필드를 분리시키고 중요 데이터를 확보하는 행위가 분석되었다.

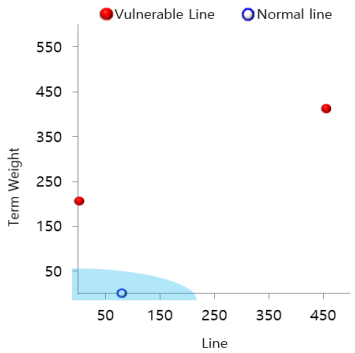

Fig. 8. Distribution of lines in the experiments with Sqlmap tool

Vulnerable Line

<pre>ID:asd' UNION ALL SELECT CONCAT(0x716a6b6b71,
IFNULL(CAST(column_name AS CHAR),0x20),0x7a6171776266,
IFNULL(CAST(column_type AS CHAR),0x20),0x716b6b6b71),NULL
FROM INFORMATION_SCHEMA.COLUMNS WHERE
table_name=0x434841524143544552 5f53455453 AND
table_schema= 0x696e666f726d6174696f6e5f736368656d61--agbS
firstname
qjkkqCHARACTER_SET_NAMEzaqwbfvarchar(32)qkkkq

separation

0x716a6b6b71	column_name	0x7a6171776266	column_type	0x716b6b6b71
qjkkq	CHARACTER_SET_NAME	zaqwbf	varchar(32)	qkkkq
qjkkq	COLLATION_NAME	zaqwbf	varchar(32)	qkkkq
qjkkq	COLLATION_NAME	zaqwbf	varchar(32)	qkkkq
qjkkq	TABLE_CATALOG	zaqwbf	varchar(512)	qkkkq
qjkkq	GRANTEE	zaqwbf	varchar(81)	qkkkq
qjkkq	ENGINE	zaqwbf	varchar(64)	qkkkq
qjkkq	EVENT_CATALOG	zaqwbf	varchar(64)	qkkkq

Fig. 9. Analysis of vulnerable lines (ex. SQLi, 455 : 413(line : term weight) in Fig. 8.)

Table 4. Number of Lines per status code for each experiment

Tool	Http state code	Sections		Total number of Lines (TF-IDF calculation)		
		T	UT	Before	After	To be checked
App scan	'2xx'	42	13	123,029	1,602	845
	'3xx'	6	-	2,141	10	-
	'4xx'	24	-	30,768	2,047	-
Sql map	'2xx'	1	2	27,057	537	457

T: Trusted, UT: UnTrusted

2가지의 실험에서 발생한 응답트래픽의 라인 수는 Table 4.와 같이 나타났다. TF-IDF를 사용하여 라인들을 분석한 결과, 같은 가중치를 갖는 라인들이 특정 구간들에 포함되는 것을 확인하였고 가중치가 높은 구간부터 순차적으로 분석하였다.

Appscan 도구를 이용한 실험에서 상태코드가 '2xx'인 경우에는 123,029개의 라인들 중 높은 가중치의 845개의 라인이 포함된 13개의 비신뢰 구간에서 취약한 반응을 확인 할 수 있었다. 그러나 '3xx'와 '4xx'인 경우의 라인들은 낮은 가중치를 가지고 있었고 모두 신뢰구간 내에 포함되어 취약한 반응이 나타나지 않았다. Sqlmap 도구를 이용한 실험에서는 가장 낮은 가중치의 80개 라인은 하나의 페이지를 구성하는 정상라인으로 1개의 신뢰구간에 포함되었고, 나머지 높은 가중치의 457개 라인에서 취약반응을 확인하였다. 서버의 반응인 응답트래픽을 정제하여 공격의 복잡성과 대상지 서버 변화(업데이트, 추가되는 서비스 등)에도 유연하게 서버의 취약유무와 침입탐지이벤트의 유효성을 검증할 수 있음을 확인하였다.

V. 결론 및 향후 연구

본 논문에서 웹 응답트래픽을 확보하고 TF-IDF를 이용해서 침입탐지이벤트의 유효성을 검증하여 신속하게 대응할 수 있는 기법을 제안하였다. 가중치가 높은 라인부터 대응순서를 자동적으로 지정할 수 있기 때문에 웹 서버의 취약여부를 빠르게 확인할 수 있었고, 응답트래픽과 위협트래픽을 사상시킴으로써 유효한 침입탐지이벤트를 즉각 확인 할 수 있었다. 또한, 웹 서버에 영향이 없는 침입탐지이벤트는 불필요한 트래픽으로 자동 분류하였다. 그러나

인증, 접근제어와 관련된 웹 취약점은 탐지규칙을 생성하기 어려운 측면이 있으며, 응답트래픽이 클라이언트로 전송되지 않는 경우(서버 내부 동작, 제 3자로의 접근 등)는 별도의 검증이 필요하여 공격유형의 분류를 세분화하여 검증할 수 있는 방안이 필요할 것으로 나타났다. 제안된 기법은 대량의 침입탐지이벤트의 분석 및 대응방향, 자동검증의 지표로써 활용할 수 있을 것으로 기대한다.

References

[1] "Mid-year 2018 Vulnerability Trends," Risk Based Security, Aug. 2018.

[2] Hayong Lee and Hyosik Yang, "Construction of Security Evaluation Criteria for Web Application Firewall," Journal of Digital Convergence, 15(5), pp. 197-205, May. 2017

[3] Zakira Inayat, Abdullah Gani, Nor Badrul Anuar, Muhammad Khurram Khan, and Shahid Anwar, "Intrusion response system: Foundations, design, and challenges." Journal of Network and Computer Applications, vol. 62, pp. 53-74, Feb. 2016.

[4] N.B. Anuar, S.M. Furnell, M.Papadaki, and N,L, Clarke, "Response Mechanisms for Intrusion Response System(IRSs)," University of Plymouth: Plymouth, UK. Nov. 2009.

[5] Kyuil Kim, Harksoo Park, Jiyeon Choi, Sangjun Ko and Jungsuk Song, "An Auto-Verification Method of Security Events Based on Empirical Analysis for Advanced Security Monitoring and Response," Journal of The Korea Institute of Information Security & Cryptology, 24(3), pp. 507-522, Jun. 2014.

[6] Byungha Choi, Sungkyo Choi, and Kyungsan Cho, "An Efficient Detecting Scheme of Web-based Attacks through Monitoring HTTP Outbound Traffics," Journal of the Korea Society of Computer and Information, 16(1), pp. 125-132, Jan. 2011.

[7] "Trends and Analysis of Internet Invasion Incident Monthly," KrCERT, Korea Internet & Security Agency, Feb. 2010.

[8] Andrey Fedorchenko, Igor Kotenko and Didier El Baz, "Correlation of security events based on the analysis of structures of event types," 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing System: Technology and Applications (IDAACS). vol. 1, pp. 270-276, Sep. 2017.

[9] HaengGon Lee, SangSoo Choi, Jungsuk Song and GiHwan Cho, "An Effective Security Monitoring Scheme Based on Correlation Analysis of Multiple Security Events," Journal of Knowledge Information Technology and Systems, 7(2), pp. 49-58, Apr. 2012.

[10] JinGuk Um and HunYeong Kwon, "Model Proposal for Detection Method of Cyber Attack using SIEM," The Journal of The Institute of Internet, Broadcasting and Communication, 16(6), pp. 43-54, Dec. 2016.

[11] Inseok Jeon, Keunhee Han, Dongwon Kim and Jinyung Choi, "Using the SIEM Software vulnerability detection model proposed," Journal of The Korea Institute of Information Security & Cryptology, 25(4), pp. 961-974, Aug. 2015.

[12] Seong Hoon Jeong, Hana Kim, Youngsang Shin, Taejin Lee and Huy Kang Kim. "A Survey of Fraud Detection Research based on Transaction Analysis and Data Mining Technique," Journal of The Korea Institute of Information

Security & Cryptology, 25(6), pp. 1525-1540, Dec. 2015.
〔13〕 Hayoung Oh, "Coward Analysis based Spam SMS Detection Scheme," Journal of The Korea Institute of Information Security & Cryptology, 26(3), pp. 693-700, Jun. 2016.
〔14〕 Min Song, Text Mining, Cheongram, Aug. 2017.
〔15〕 Hyoseok Kim, "A Validation of Intrusion Detection Events Using TF-IDF," M.S.Thesis, Chonnam National University, Aug 2018.
〔16〕 DVWA - Damn Vulnerable Web Apllcation, "DVWA", http://www.dvwa.co.uk/, Nov. 2017.
〔17〕 Snort - Network Intrusion Detection & Preventions System, "Snort", https://snort.org/downloads#rules, Dec. 2017.
〔18〕 Emerging Threats rule, "ET Rule", https://rules.emergingthreats.net/, Dec. 2017.
〔19〕 OWASP, "OWASP Top 10", https://www.owasp.org/images/b/bd/OWASP_Top_10-2017-ko.pdf, Nov. 2017.

〈저자소개〉

김 효 석 (Hyoseok Kim) 정회원
2014년 2월: 학점은행제 컴퓨터공학 학사
2018년 8월: 전남대학교 대학원 정보보안협동과정 석사
2018년 9월~현재: 전남대학교 대학원 정보보안협동과정 박사과정
〈관심분야〉 웹 해킹 및 보안, 네트워크 보안, 침해사고 대응

김 용 민 (Yong-Min Kim) 종신회원
2002년 2월: 전남대학교 전산통계학과 박사
2006년~현재: 전남대학교 문화콘텐츠학부 교수
〈관심분야〉 시스템 및 네트워크 보안, 전자상거래 보안 등