JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 25, No. 3: 449~455, Mar. 2021

웹 모니터링 기반 암호화 웹트래픽 공격 탐지 시스템

이석우[1] · 박순모[1] · 정회경[2*]

Web Monitoring based Encryption Web Traffic Attack Detection System

Seokwoo Lee[1] · Soonmo Park[1] · Hoekyung Jung[2*]

[1]Graduate Student, Department of Computer Engineering, Paichai University, Daejeon, 35345 Korea
[2*]Professor, Department of Computer Engineering, Paichai University, Daejeon, 35345 Korea

요 약

본 논문에서는 기존의 웹애플리케이션 모니터링 시스템을 기반으로 한 암호화 웹트랜잭션 공격탐지 시스템을 제안한다. 기존의 웹트래픽 보안 시스템들은 클라이언트와 서버간의 암호화 구간인 네트워크 영역에서 암호화된 패킷을 기반으로 공격을 탐지하고 방어하기 때문에 암호화된 웹트래픽에 대한 공격 탐지가 어려웠지만, 웹애플리케이션 모니터링 시스템의 기술을 활용하게 되면 웹애플리케이션 서버의 메모리 내에서 이미 복호화 되어 있는 정보를 바탕으로 다양한 지능적 사이버 공격에 대한 탐지가 가능해 진다. 또한, 애플리케이션 세션 아이디를 통한 사용자 식별이 가능해지기 때문에 IP 변조 공격, 대량의 웹트랜잭션 호출 사용자, DDoS 공격 등 사용자별 통계기반의 탐지도 가능해 진다. 이와 같이 암호화 웹트래픽에 대한 비 암호화 구간에서의 정보 수집 및 탐지를 통하여 암호화 트래픽에 숨어 있는 다양한 지능적 사이버공격에 대한 대응이 가능할 것으로 사료된다.

ABSTRACT

This paper proposes an encryption web transaction attack detection system based on the existing web application monitoring system. Although there was difficulty in detecting attacks on the encrypted web traffic because the existing web traffic security systems detect and defend attacks based on encrypted packets in the network area of the encryption section between the client and server, by utilizing the technology of the web application monitoring system, it is possible to detect various intelligent cyber-attacks based on information that is already decrypted in the memory of the web application server. In addition, since user identification is possible through the application session ID, statistical detection of attacks such as IP tampering attacks, mass web transaction call users, and DDoS attacks are also possible. Thus, it can be considered that it is possible to respond to various intelligent cyber attacks hidden in the encrypted traffic by collecting and detecting information in the non-encrypted section of the encrypted web traffic.

키워드 : 웹애플리케이션 보안, 웹트래픽 보안, 지능적 사이버공격 탐지, SSL 암호화 트래픽 보안

Keywords : Securing web application, Securing web traffic, Detection of intelligent cyberattacks, Securing SSL encrypted traffic

Received 10 March 2020, **Revised** 10 March 2020, **Accepted** 15 March 2021

*** Corresponding Author** Hoekyung Jung(E-mail:hkjung@pcu.ac.kr, Tel:+82-42-520-5640)
Professor, Department of Computer Engineering, Paichai University, Daejeon, 35345 Korea

Open Access http://doi.org/10.6109/jkiice.2021.25.3.449 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

본 논문에서는 웹애플리케이션 모니터링 시스템을 활용하여 암호화 웹트래픽을 경로로 이용하는 지능적 사이버공격에 대한 명확한 탐지가 가능한 웹애플리케이션 모니터링 기반 암호화 웹트랜잭션 공격 탐지 시스템에 대해 연구를 하였다. 웹방화벽 등 기존 보안 시스템은 네트워크 영역에서 암호화된 패킷을 수집할 때 복호화 및 L7 계층 디코딩 과정이 필요하였지만 웹애플리케이션 모니터링 시스템을 활용하면 복호화가 이미 되어 있는 웹애플리케이션 서버의 메모리 내에서 웹트랜잭션 정보를 수집하게 되므로 부하가 거의 없이 웹트랜잭션 정보 전수 수집 및 저장, 정확한 사용자 식별, 통계기반의 탐지 등을 통하여 다양한 지능적 사이버 공격에 대응이 가능하다.

Ⅱ. 관련연구

본 장에서는 암호화 트래픽으로 인한 해킹에 대응하기 위한 기존 웹애플리케이션 시스템에 대해 설명한다.

2.1. 웹애플리케이션 모니터링 시스템

웹애플리케이션 모니터링 시스템은 1998년 북미에서 Willy라는 업체가 처음으로 선보였고 웹서비스 사용이 확대됨에 따라 서비스의 성능 모니터링 및 개선이 중요해지면서 빠르게 성장하였다. 그림 1은 웹애플리케이션 모니터링 시스템을 나타낸다. 웹애플리케이션 모니터링 시스템은 애플리케이션 서버에 플러그인 형태로 구동되며 웹애플리케이션 서버가 기동되고 모니터링 대상 클래스가 메모리에 로딩 될 때 바이트 코드를 동적으로 조작하여 모니터링 코드를 삽입하고, 이후 삽입된 모니터링 코드를 통하여 원하는 정보를 다양하게 수집하여 실시간 모니터링과 분석 기능을 제공한다. 웹애플리케이션 모니터링 시스템은 요청된 트랜잭션 정보가 이미 복호화된 상태에서 비즈니스 로직 처리를 시작할 때 수집하게 되므로 부하가 거의 없고 요청 트랜잭션 정보 전체를 수집할 수 있다[1-4].

2.2. 보안시스템 요구사항

기존 보안 시스템은 네트워크 영역에서 수집한 패킷 정보에 의존하여 웹트랜잭션에 대한 공격을 탐지한다. 패킷이 암호화 되어 있을 경우 이를 복호화 해야 하고 복호화로 인한 성능저하가 발생되어 패킷 전수 조사가 사실상 불가능하다. 모든 패킷을 복호화 하였다 하더라도 수집된 정보를 저장하지 않는다. 암호화 웹트래픽을 이용하는 지능적 사이버 공격은 통계 기반이 아니면 탐지하기 어렵다. 이에 따라, 부하 없는 웹트래픽 전수 수집 및 저장과 저장된 데이터를 바탕으로 통계 기반의 탐지 기능이 요구되고 있다[5-7]. 이와 같은 요구사항을 해결하기 위한 시스템을 제안한다.

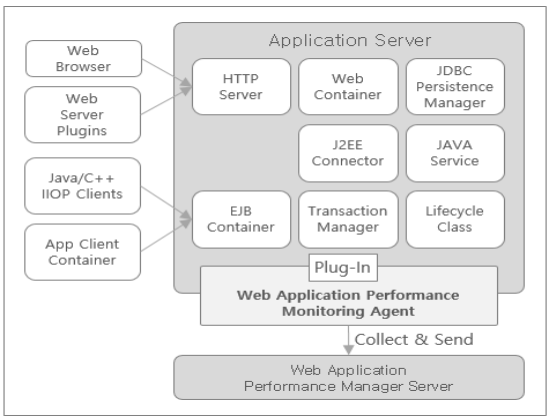

Fig. 1 Web Application Monitoring System

Ⅲ. 시스템 설계

본 장에서는 웹애플리케이션 모니터링 시스템을 통해 수집한 웹트랜잭션 정보를 기반으로 다양한 공격을 탐지 할 수 있는 시그니처 기반 탐지와 통계기반 탐지 및 데이터 액세스 기반 탐지 등을 위한 시스템 설계를 설명한다.

3.1. 탐지 시스템 설계

3.1.1. 시스템 구축 환경

본 논문에서는 HTTP 요청 정보 중에 요청한 클라이언트의 웹브라우저 및 OS의 종류와 버전 정보를 담고 있는 user-agent 정보에서 이미 공격 패턴으로 알려진 user-agent 블랙리스트 정보와 매칭 하여 탐지하도록 설계 하였다.

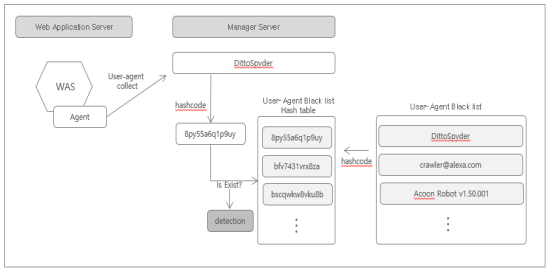

Fig. 2 User-agent blacklist detection system configuration diagram

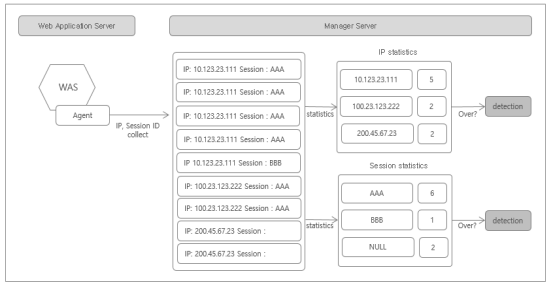

Fig. 3 Configuration of statistics-based detection system

그림 2는 user-agent 블랙리스트 탐지 시스템의 구성도를 나타낸다. 웹애플리케이션 서버에 설치된 에이전트가 user-agent 정보를 포함하고 있는 사용자가 요청한 웹트랜잭션 정보를 수집하여 매니저 서버로 전송한다. 전송된 user-agent 정보를 user-agent 블랙리스트에 등록된 텍스트와 하나하나 텍스트 비교를 하여 user-agent 블랙리스트에 존재하는지 확인하여 공격에 대한 탐지가 가능하다. 하지만, user-agent 블랙리스트가 많아질 경우 일일이 텍스트 비교를 하는데 시스템 리소스를 많이 소요하게 되므로 성능 문제를 발생시킬 수 있다. 이러한 성능 문제를 해결하기 위하여 해시테이블을 통한 탐지 방식으로 설계하였다.

3.1.2. 통계기반 탐지 시스템 설계

본 논문에서는 이미 복호화 되어 있는 웹트랜잭션 호출 정보를 수집하기 때문에 클라이언트 IP이외에도 애플리케이션 세션 아이디를 활용하여 사용자를 정확히 식별할 수 있다. 또한 수집된 정보를 모두 저장하여 클라이언트 IP 및 애플리케이션 세션 아이디로 통계화를 통해 다양한 공격을 탐지 할 수 있게 된다.

그림 3은 에이전트로부터 수집되는 클라이언트 IP와 애플리케이션 세션 아이디 정보를 통계화 하는 구성도를 보여주고 있다. IP 통계는 수집되는 클라이언트 IP별로 호출건수를 카운트 하게 되고, 애플리케이션 세션 아이디 통계는 수집되는 애플리케이션 세션 아이디 별로 호출건수를 카운트 하게 된다. 카운트를 하다가 설정된 통계 기간을 넘어가게 되면 값이 0으로 초기화 된다. 만약 카운트 도중 관리자가 설정한 임계값을 초과하게 되면 탐지되는 방식이다. 이에 본 논문에서는 DDoS 공격 탐지, IP 변조공격 탐지, 대량의 웹트랜잭션 호출 사용자 탐지 등의 기능을 구현하였다.

3.1.3. 데이터 액세스 기반 탐지 시스템 설계

본 논문에서는 웹애플리케이션 모니터링 시스템에서 수집하는 데이터 조회건수, 입력건수, 수정건수, 삭제건수 등의 데이터 액세스 정보를 수집하여 실제 데이터베이스에 발생된 비정상 행위에 대한 탐지가 가능하다.

3.2. 전체 시스템 설계

3.2.1. 시스템 구조도

기존 웹애플리케이션 모니터링 시스템을 활용하여 본 논문에 필요한 기능들을 추가하여 시스템을 구성하였다. 그림 4는 시스템 전체 구성도를 나타낸다. 탐지를 위한 이벤트 설정 및 user-agent 블랙리스트 관리 및 저장 기능과 각 탐지 항목별 탐지 이벤트 발생시 텔레그램(telegram)을 통해 이벤트 전송 및 이벤트 전송 설정을 위한 환경 설정 부분으로 나뉜다.

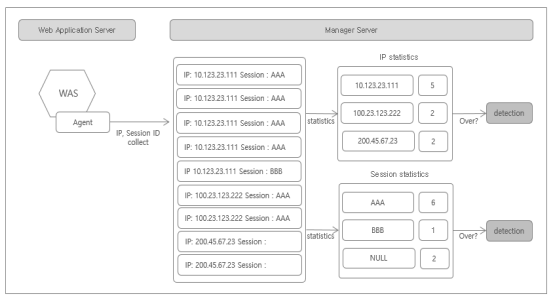

Fig. 4 System configuration diagram

3.2.2. 탐지 이벤트 텔레그램 연동

탐지 이벤트가 발생되면 보안 관리자에게 탐지 메시지를 전송하기 위하여 텔레그램 API를 사용할 수 있다.

텔레그램 봇을 생성하면 봇 API 토큰을 받을 수 있고, 웹훅 방식으로 봇 API 토큰을 포함하여 호출하게 되면 탐지 이벤트를 보안 관리자에게 전송할 수 있다. 텔레그

램을 통한 이벤트 전송의 장점은 과금되지 않는 무료 메시지 서비스란 것이다. 또한 그룹 채팅 방을 만들어 Group ID를 설정하게 되면 해당 그룹 채팅 방으로 이벤트가 전송된다. 이벤트를 받을 사용자는 텔레그램 모바일 어플에서 해당 그룹 채팅 방에 들어가는 것만으로도 이벤트를 받을 수 있다.

3.2.3. 데이터베이스 스키마 설계

관리 및 탐지, 이벤트 발송을 위한 데이터와 에이전트로부터 수집한 웹트랜잭션 정보를 데이터베이스에 적재한다. 표 1은 시스템에서 사용하는 데이터베이스의 구조를 나타낸다.

Table. 1 Database structure

Table_Name	Description
user_agent_blacklist	Storing the data of user-agent blacklist
event_code	Storing the each item event setting value
event_history	Storing the data of event history
parameter	Storing the data event send setting value
user	Storing the each user or manager information
transaction	Storing the data collect of web traffic information

Ⅳ. 시스템 구현

본 장에서는 웹애플리케이션 모니터링 시스템을 기반으로 한 암호화 웹트랜잭션 공격 탐지 시스템의 구현을 다룬다.

4.1. 구현 환경

표 2는 구현 환경을 나타낸다.

Table. 2. System implementation environment

Type	Composition
Web Application Monitoring System	Elevisor for J2EE
Tool	IntelliJ, Eclipse, Derby, Elasticsearch, Jetty, Tomcat, JDK, K*Proxy, JMeter, Telegram
PC	Windows 7 Enterprise Intel(R) Core(TM) i5-6700k, 32GB RAM

4.2. 시스템 구현

4.2.1. 탐지 설정 구현

탐지 항목별 탐지 기준을 설정할 수 있는 화면 구현하였다. 탐지 항목은 User-Agent 블랙리스트 탐지, DDoS 공격 탐지, IP 변조 공격탐지, 대량의 웹트랜잭션 호출 사용자 탐지, 대량의 데이터 액세스 탐지 등이 있다. 그림 5는 탐지 이벤트 설정 화면을 구현한 웹페이지를 나타낸 것이다.

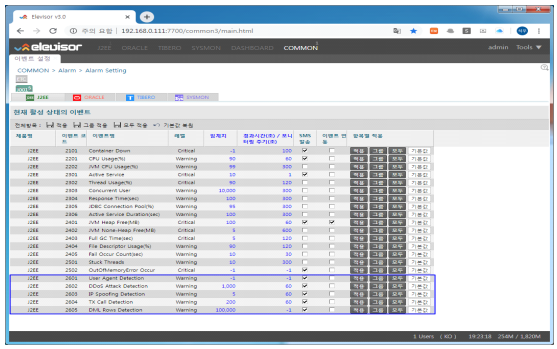

Fig. 5 Detection event setting screen

4.2.2. User-Agent 블랙리스트 탐지 기능 구현

그림 6은 User-Agent 블랙리스트 관리 화면을 구현한 웹페이지를 나타낸 것이다. User-Agent 블랙리스트 탐지를 위해서 User-Agent 블랙리스트를 관리하는 화면을 구현하였다. 기존에 알려진 다양한 User-Agent 블랙리스트를 기본 값으로 데이터베이스에 등록하였으며 User-Agent 블랙리스트의 타입을 Browser, Link, Bookmark, Checking, Download, Proxy, Web Filter, Robot, Crawler, Spider, Spam, Bed bot 등으로 구분하도록 하였다. 추가적으로 User-Agent 블랙리스트를 등록하거나, 삭제할 수 있으며 특정 항목만 일시적으로 제외시킬 수 있는 기능을 포함한다.

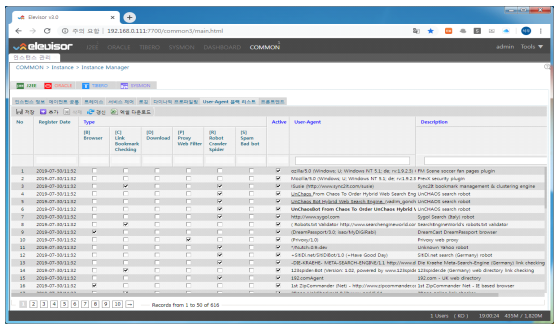

Fig. 6 User-Agent blacklist management screen

4.2.3. DDoS 공격 탐지 기능 구현

DDoS 공격 탐지는 웹클라이언트에서 애플리케이션 세션 아이디를 유지하지 않고 요청되는 클라이언트 IP를 카운트함으로서 탐지할 수 있도록 구현하였다. 이를 통하여 웹애플리케이션 세션 아이디를 유지하지 않고 요청하는 클라이언트 IP 별로 호출건수를 집계 할 수 있도록 구현하였다.

4.2.4. IP 변조 공격 탐지 기능 구현

IP 변조 공격은 동일 애플리케이션 세션 아이디에 대한 클라이언트 IP 종류를 카운트함으로써 IP 변조 공격을 하는 애플리케이션 세션 아이디를 탐지할 수 있도록 구현하였다. 이를 통하여 동일 웹애플리케이션 세션 아이디별로 클라이언트 IP 변경 건수를 집계 할 수 있도록 구현하였다.

4.2.5. 대량의 트랜잭션 요청 사용자 탐지 기능 구현

대량의 트랜잭션을 요청하는 사용자를 탐지하기 위해서는 클라이언트 IP가 아닌 애플리케이션 세션 아이디를 통하여 정확한 사용자 식별이 필수적인 요소이며, 지정된 단위 시간동안 요청한 웹트랜잭션 건수를 애플리케이션 세션 아이디별로 카운트하여 임계치를 넘었을 경우 탐지하는 방식으로 구현하였다. 이를 통하여 웹애플리케이션 세션 아이디별로 호출건수를 집계 할 수 있도록 구현하였다.

4.2.6. 대량의 데이터 액세스 탐지 기능 구현

대량의 데이터 액세스 탐지 기능은 웹애플리케이션 모니터링 시스템에서 수집한 DML 정보를 기반으로 탐지하도록 구현하였다. select, insert, update, delete 건수가 수집될 때, 보안관리자가 지정한 임계치를 넘는 트랜잭션을 식별하게 되고, 해당 트랜잭션을 유발시킨 애플리케이션 세션 아이디를 탐지하도록 구현하였다.

4.2.7. 탐지 이벤트 관리 기능 구현

탐지 이벤트 관리 기능은 기존 웹애플리케이션 모니터링 시스템의 이벤트 관리 기능에 암호화 웹트랜잭션 공격 탐지 이벤트를 추가하는 방식으로 구현하였다. 현재 발생 이벤트 관리 기능과 이벤트 이력 관리 기능으로 구분된다. 이벤트 종류별 이벤트 레벨과 발생시각 및 임계치 설정 정보, 지속시간 이벤트 메시지 등의 정보를 실시간으로 보여준다.

4.2.8. 탐지 이벤트 전송 기능 구현

탐지 이벤트가 발생되었을 때 이를 보안 관리자에게 전송하여 알려주는 기능을 텔레그램 API를 통하여 구현하였다. 그림 7은 텔레그램 봇 생성 및 검색 화면을 나타낸 것이다.

4.3. 고찰

본 논문에서는 웹애플리케이션 모니터링 시스템에서 수집한 웹트랜잭션 정보를 통하여 문자열 매칭 기반의 User Agent 블랙리스트 탐지와 통계 기반의 DDoS공격 탐지, IP변조 공격 탐지, 대량의 웹트랜잭션 호출 사용자 탐지와 DML 정보 기반의 대량의 데이터 액세스 탐지 등 총 5가지의 탐지 기능을 구현 및 각 탐지 기능별 10회의 테스트를 진행하였다.

표 3은 공격 유형별 테스트 시나리오를 나타낸다. User Agent 블랙리스트는 user agent 헤더값에서 “123spider-Bot”이 존재할 경우 탐지한다. DDoS 공격은 세션을 유지하지 않고 요청되는 클라이언트IP가 1분 동안 100회 이상일 경우 탐지한다. IP 변조공격은 동일 세션 아이디로 클라이언트 IP가 1분 동안 3회 이상 변경되었을 경우 탐지한다. 대량의 웹트랜잭션 호출은 동일 세션 아이디로 1분 동안 100회 이상 요청되었을 경우 탐지한다. 대량의 데이터 엑세스는 DML 건수가 100,000회 이상일 경우 탐지하도록 하였다.

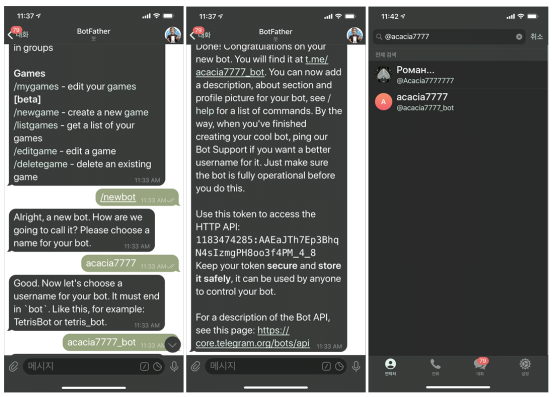

Fig. 7 Telegram bot creation and search screen

표 4는 탐지 항목별 오탐률을 나타낸 표이다. 모든 항목에서 오탐률이 0%로서 매우 정확하게 탐지되는 것으로 확인되었다. 또한 본 제안 시스템은 웹애플리케이션 모니터링 시스템이 수집한 웹트랜잭션 정보를 별도의 매니저 서버로 전송한 정보를 활용하였고, 탐지를 위한

통계 프로세싱은 매니저 서버에서 수행하기 때문에 본 시스템 적용으로 인한 운영서버에 대한 추가적인 부하가 전혀 없었다. 또한 클라이언트 IP가 아닌 애플리케이션 세션 아이디를 통하여 사용자를 식별하므로 정확한 사용자 식별 및 통계를 기반으로 한 사용자 행위 기반 탐지가 가능해 졌다. 이를 통해 기존 보안 시스템에서의 암호화 웹트랜잭션 복호화, 사용자 식별, 통계기반 탐지 등의 문제점을 해결할 수 있게 되었다.

Ⅴ. 결 론

웹서비스의 대부분은 HTTP 및 HTTPS 프로토콜을 사용한다. HTTPS 프로토콜은 암호화 통신 프로토콜로서 암호화로 인하여 기존 네트워크 기반의 보안시스템에서 웹트래픽을 점검하기 어렵게 되었으며 이를 악용하여 암호화 웹트래픽에 숨어 들어오는 공격이 증가하고 있어 정보 유출이나 해킹 등의 공격에 상당히 취약하다.

Table. 3 Test scenario

Item	Statistics Time(Min)	Count	Description
User Agent Black List Detection	-	-	Detect “123spider-Bot”
DDoS Attack Detection	1	100	
IP Spoofing Detection	1	3	
TX Call Detection	1	100	
DML Rows Detection	-	100,000	Detect DML

Table. 4 False positive rate by detection item

Item	False positive	Description
User Agent Black List Detection	0%	Detected when the requested user agent value is included in the user agent blacklist
DDoS Attack Detection	0%	Detected as the number of requests without application session ID for a specified time per client IP
IP Spoofing Detection	0%	Detects the number of times the client IP is changed during the specified time within the same application session ID
TX Call Detection	0%	Detects the number of calls during a specified time within the same application session ID
DML Rows Detection	0%	Detect when a large amount of DML(Select, Insert, Update) occurs

이를 위해 본 논문에서는 웹애플리케이션 모니터링 시스템에서 수집한 웹트랜잭션 정보를 기반으로 문자열 매칭 기반의 User Agent 블랙리스트 탐지와 통계 기반의 DDoS공격 탐지, IP변조 탐지, 대량의 웹트랜잭션 호출 사용자 탐지와 DML 정보 기반의 대량의 데이터 액세스 탐지 등 총 5가지의 탐지 기능을 구현 및 각 탐지 기능별 10회의 테스트를 진행한 결과 오탐률이 0%로서 매우 신뢰할 수 있는 암호화 웹트랜잭션 공격 탐지 시스템을 구축할 수 있었다. 또한 웹애플리케이션 모니터링 시스템 기반으로 개발하여 본 시스템 적용으로 인한 운영서버에 대한 부하가 전혀 없었고, 기존 보안 시스템에서 암호화 웹트랜잭션 복호화, 사용자 식별, 통계기반 탐지 등의 문제점을 해결할 수 있었다.

향후 연구로는 보다 다양한 탐지를 위한 연구를 해야 할 것이다. 또한 탐지의 정확도가 100%에 달하기 때문에 탐지 후 자동으로 차단하는 기능 통하여 기존에 보안 담당자가 탐지 이벤트를 수작업으로 분석 및 차단하던 부분을 자동화 할 수 있을 것으로 사료된다.

ACKNOWLEDGEMENT

This work was supported by the research grant of Pai Chai University in 2021.

References

[1] HUSTON III and B. Lawrence, “IEKEL-JOHNSON, Scott. Scalable DDoS protection of SSL-encrypted services,” U.S. Patent No 10,116,692, 2018.

[2] W. Chen, S. H. Jeong, and H. K. Jung, “WiFi-Based Home IoT Communication System,” *Journal of Information and Communication Convergence Engineering*, vol. 18, no. 1, pp. 8-15, Mar. 2020.

[3] S. E. Yang, K. Y. Park, and H. K. Jung, “A convergence

implementation of realtime traffic shapping and IPS on small integrated security router for IDC," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 23, no. 7, pp. 861-868, 2019.

[4] T. Junwei, "Detecting SSL security vulnerabilities of android applications based on a novel automatic traversal method," *Security and Communication Networks*, 2019.

[5] T. Adrian, "Decrypting SSL traffic: best practices for security, compliance and productivity," *NETWORK SECURITY*, vol. 2019, no. 8, pp. 17-19, Aug. 2019.

[6] J. H. Hyun and H. J. Kim, "Security operation implementation through big data analysis by using open source ELK stack," *Journal of Digital Contents Society*, vol. 19, no. 1, pp. 181-191, Jan. 2018.

[7] D. K. Kim, S. B. Pyo, and C. H. Kim, "Study on APT attack response techniques based on big data analysis," *The Society of Convergence Knowledge Transactions*, vol. 4, no. 1, pp. 29-34, Jan. 2016.

이석우(Seokwoo Lee)

2004년 한밭대학교 전자공학과(공학사)
2006년 솔루션 개발 연구소 팀장
2018년 중소기업기술개발 지원사업 평가위원(중소기업기술정보진흥원)
2018년 중소기업 R&D 지원사업 평가위원(중소기업진흥공단)
2020년 배재대학교 컴퓨터공학과(공학석사)
2014년 ~ 현재 주식회사 엘리바이저 대표이사
※관심분야 : 시스템 성능관리, 웹트래픽 보안, 데이터베이스 보안, 빅데이터

박순모(Soonmo Park)

1996년 부경대학교 전자공학과(공학사)
2009년 충북대학교 전기전산공학과(공학석사)
2021년 ~ 현재 배재대학교 컴퓨터공학과 박사과정 재학
※ 관심분야 : IoT, BigData Platform

정회경(Hoekyung Jung)

1985년 광운대학교 컴퓨터공학과(공학사)
1987년 광운대학교 컴퓨터공학과(공학석사)
1993년 광운대학교 컴퓨터공학과(공학박사)
1994년 ~ 현재 배재대학교 컴퓨터공학과 교수
※관심분야 : Machine learning, Big data, Embedded system, U-Healthcare, IoT