Rule 기반 트래픽 분석을 통한 사용자 행위 탐지 시스템 설계

박지태, 이민성, 김보선, 신창의, 김명섭

고려대학교

{pjj5846, min0764, boseon12, realmine, tmskim}@korea.ac.kr

A Design of User Behavior Detection System through Rule-based Traffic Analysis

Jee-Tae Park, Min-Seong Lee, Boseon Kim, Chang-Yui Shin, Myung-Sup Kim

Korea Univ.

요 약

최근 다양한 응용 서비스가 발생하고 있으며, 특히 네트워크 기술의 발전에 따라 기존의 설치 형태의 응용 서비스뿐만 아니라 구독 형태의 응용 서비스(SaaS)의 사용량이 증가하고 있다. 구독 형태의 응용 서비스는 체계적으로 관리 할 수 있으며, 단체가 사용하기 편리하지만, 실제 사용자보다 더 많은 인원의 라이선스를 구독 할 경우, 불필요한 지출이 발생 할 수 있다. 따라서 SaaS 응용 서비스를 대상으로 다양한 연구가 수행되고 있으며, 그 중에서 가장 널리 알려진 분석 방법은 페이로드 시그니처를 활용한 방법이다. 하지만 페이로드 시그니처를 활용한 분석 방법은, 각 SW마다 정의되는 시그니처가 다르기 때문에 SW 별로 분석 시스템을 따로 만들어야하며, 분석 대상 SaaS SW 수가 많아 질 경우 상당히 비효율적이다. 따라서 본 논문에서는 기존 방법의 문제점을 해결하기 위하여 Rule 기반 사용자 행위 탐지 방법을 제안한다. 먼저 SaaS 서비스를 대상으로 사용자 행위에 대해 정의하고, 제안하는 방법의 시스템 구조와 정의한 Rule 구조에 대해 설명하고 논문을 마친다.

Ⅰ. 서 론

최근 네트워크 기술의 발전에 따라 설치 형태의 응용 서비스와 함께 구독 형태의 응용 서비스(SaaS)의 사용량이 증가하고 있다. SaaS 응용 서비스는 클라우드 기반 소프트웨어 제공 모델로 개인, 혹은 특정 기업 및 단체에서 사용 인원, 기간, 사용 라이선스에 따라 구매하여 사용하며, 기간이 만료 될 경우, 신문 구독처럼 기간을 연장하거나 폐지 할 수 있는 구독 형태로 서비스가 제공된다. SaaS 서비스는 점차적으로 사용이 증가하고 있으며, 기존에 설치 형태의 응용 서비스도 구독 형태의 응용 서비스로 전환되고 있는 추세이다. 가장 대표적으로 널리 알려진 SaaS 서비스는 Office 365, Adobe Creative Cloud가 있으며, 필요에 따라 사용을 조정 할 수 있기 때문에 많은 기업 및 단체에서 사용하고 있다[1-2]. 또한 기업 내에서 사용하는 비율과 필요한 서비스에 따라 적절한 금액만을 지불하여 효율적인 자산 관리도 할 수 있다. 하지만 반대로 실제로 서비스를 사용하는 비율에 대한 모니터링이 제대로 이루어지지 않는다면 불필요한 지출이 발생할 수 있다. 따라서 SaaS 응용 서비스와 사용량에 대한 정확한 모니터링이 필요하며, 특히, 기업 내 사용자의 사용 행위에 대한 탐지를 통해 실제 사용량과 구입한 라이선스를 비교하여 불필요한 지출을 확인 할 수 있다.

이러한 추세에 따라 SaaS 응용 서비스에 대해 다양한 연구가 수행되어 왔으며, 가장 널리 알려진 방법은 페이로드 시그니처를 활용하여 사용자 행위 탐지 방법이 있다[1]. SaaS 응용 서비스는 기본적으로 SSL/TLS 기반의 암호화 트래픽을 사용하기 때문에 암호화 된 페이로드 전체 내용 대신 SNI(Server Name Indication)을 사용하며, 각각의 SW 별로 공통으로 도출되는 SNI 정보를 시그니처로 정의 한다. 하지만 기본적으로 SaaS SW 별로 도출되는 SNI 정보가 다르기 때문에, 각 SW 별로 정의된 탐지 시그니처는 달라진다. 따라서 각 SW 별로 탐지 시스템과 알고리즘에 따라 매번 새로운 탐지 시스템을 구축해야하기 때문에 비효율적이다. 따라서 본 논문에서는 이러한 비효율적인 문제를 해결하기 위해 기존의 방법 대신 SaaS 서비스 대상으로 Rule 기반의 사용자 행위 탐지 방법을 제안한다.

본 논문의 구성은 본 장의 서론에 이어 2장 관련 연구에서 기존에 수행된 rule 기반의 분석 방법인 Snort Rule에 대해 설명한다. 3장 본론에서 제안하는 Rule 기반의 사용자 행위 탐지 방법에 대해 설명하며, 4장에서 결론 및 향후 연구에 대해 기술한 후 마친다.

Ⅱ. 관련 연구

Rule 기반의 분석 방법은 정의 된 특정 규칙을 활용하여 트래픽을 분석하는 방법으로, 주로 IDS(Intrusion Detection System)에서 Snort Rule이 사용된다. 정의 된 규칙을 사용하여 대응되는 패킷을 탐지하고, 탐지 된 패킷에 대하여 정의 된 규칙대로 행동(Action)을 수행한다[3-4]. 규칙은 패킷 단위로 적용되며, 패킷의 헤더 및 통계, 페이로드 정보 등을 주로 사용한다. Snort Rule의 구조에 대한 예시는 표 1에 나타나있으며, Header, Body(Option)로 구성되어 있다. Header는 대상 패킷을 판단하는 기준을 명시하며, body는 패킷을 처리하는 규칙을 나타낸다.

표 1 Snort Rule 구조 예시

Action	Prot.	SRC IP	SRC Port	->	DST IP	DST Port	Option
alert	tcp	any	any	->	any	any	...

본 논문은 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발) 이며, 2021년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2021S1A5C2A03097574).

Snort Rule 기반의 분석 방법은 규칙을 정의하기 위해 분석 대상 트래픽을 수집하여 해당 트래픽에서만 발견되는 공통 특징을 우선적으로 찾아야 한다. 이 때, 공통 특징을 찾으려면 많은 양의 대상 트래픽을 수집하고, 분석해야하기 때문에 많은 시간이 걸리며, 발견된 공통 특징에 따라 정확도가 달라진다.

Ⅲ. 본론

본 논문에서는 SaaS SW에 대한 사용자 행위 탐지를 목적으로 한다. 사용자 행위는 분석 대상 SW 별로 공통으로 발생하는 행위로 SW 시작, 로그인, SW 종료, 로그아웃으로 구성되며, 그림 1에 나타나있다. 사용자의 관점에서 각각의 행위는 서로 연관되어 있다. 예를 들어 SW 시작이 수행되어야 로그인, SW 종료와 같은 다른 행위가 발생 할 수 있으며, 로그인이 발생해야 로그아웃 행위가 발생 할 수 있다. 이러한 행위 간의 관계는 정확하게 사용자 행위 탐지 시 중요하기 때문에, 제안하는 방법에서는 행위 간의 관계를 Rule로 정의 하였다.

그림 1 사용자 행위 정의

제안하는 방법은 네트워크 패킷을 확인하고 정의 된 규칙에 의하여 탐지되는 패킷일 경우 정의 된 규칙대로 처리한다는 점에서 Snort Rule과 유사하다. 기존의 시그니처 기반 분석 시스템과 Rule 기반의 분석 시스템에 대한 구조는 그림 2에 나타나 있다. 시그니처 기반의 탐지 시스템은 SW 별로 시그니처와 알고리즘이 다르기 때문에 SW 별로 별개의 분석 프로그램이 필요하지만, Rule 기반의 분석 시스템의 경우 여러 개의 분석 프로그램 대신 각 SW 별로 Rule만 정의 하면 쉽고 간편하게 적용 가능하다.

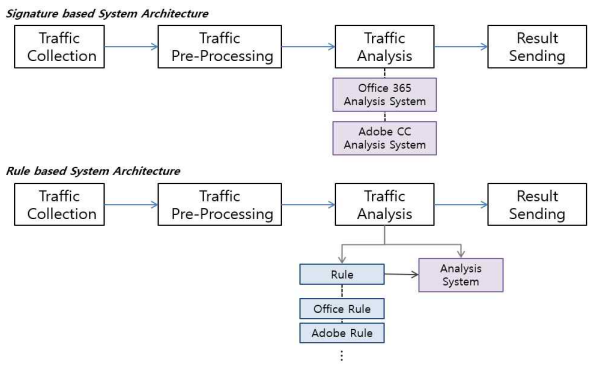

그림 2 시그니처, Rule 기반 사용자 행위 탐지 시스템 구조

본 논문에서 제안하는 방법에서 정의한 Rule은 Snort Rule의 구조와 다른 구조를 지니며, 표 2에 나타나 있다. Snort Rule은 패킷 단위로 규칙을 정의 하지만, 제안하는 방법에서는 플로우, 패킷 단위로 규칙을 정의한다. 이 때, 사용되는 Rule은 총 9가지로 구성되며, 플로우 단위에서 5가지, 패킷 단위에서 3가지, 기타 1가지로 구성된다. 플로우 단위에서의 Client IP, Port, Protocol, Server IP, Port는 플로우의 5-tuples 정보를 나타낸다.

패킷 단위에서의 방향성(Direction)은 플로우 내에서 확인 할 패킷의 방향을 나타내며, 패킷의 방향에 따라 Client to Server (C->S), Server to Client (S->C)로 구성된다. Packet Number는 확인 할 패킷이 몇 번째 패킷인지 나타내며, SNI는 확인 할 패킷에서 존재하는 String 정보를 나타낸다. Behavior는 사용 행위 간의 관계를 고려하여 대상 행동이 발생하기 위해 이전에 발생해야 하는 행동을 나타낸다. 예를 들어, 로그인 행위를 탐지 할 경우, Behavior는 SW 시작으로 정의된다.

표 2 정의 된 Rule 예시

단위	정보	Description	Example
플로우	Client IP	클라이언트 IP	any
	Client Port	클라이언트 포트	any
	Protocol	프로토콜	tcp
	Server IP	서버 IP	13.107.6.156
	Server Port	서버 포트	443
패킷	Direction	플로우 내 패킷 방향	C->S
	Packet Number	확인 할 패킷 번호	4
	SNI	SNI 정보	www.office.com
기타	Behavior	이전 발생 행위	None

Ⅳ. 결론 및 향후 연구

최근 SaaS 서비스의 사용이 증가하고 있으며, 기업에서는 불필요한 지출을 줄이기 위해 SaaS 서비스에 대한 정확한 모니터링이 필요하며, 이를 위해 실제 사용자의 정확한 행위 탐지가 필요하다. 가장 널리 알려진 SaaS 서비스 사용자 행위 탐지 방법은 페이로드 시그니처를 활용한 방법으로, 높은 정확도로 사용자 행위를 탐지 할 수 있지만, SW 별로 포함하는 SNI 정보가 다르기 때문에 SW 별로 별개의 분석 프로그램을 만들어야 한다. 점차적으로 증가하는 SaaS SW 종류를 감안하면 이는 매우 비효율적이며, 분석 프로그램이 많아질수록 과부하가 걸릴 가능성이 높아진다.

따라서 본 논문에서는 기존의 문제점을 해결하기 위해 Rule 기반의 사용자 행위 탐지 방법과 탐지에 사용되는 새로운 Rule 포맷을 제안한다. 제안하는 방법은 기존 방법과 다르게 하나의 분석 프로그램에서 각 SW 별로 정의 된 Rule을 읽고, 수집 된 패킷에 대하여 Rule에서 정의한 절차를 거친 후, 최종적으로 사용자 행위를 탐지하게 된다.

향후 연구로 Office 365의 전체 행위를 대상으로 Rule 기반 사용자 행위 탐지 시스템을 구현 할 예정이다. 또한, Adobe Creative Cloud와 같은 다른 SaaS SW를 대상으로도 Rule을 정의 할 예정이다.

참 고 문 헌

[1] 박준상, 박진완, 윤성호, 오영성, 김명섭. "응용 레벨 트래픽 분류를 위한 시그니쳐 생성 시스템 및 검증 네트워크의 개발." 한국정보처리학회 학술대회논문집 16(1) pp. 1288-1291, 2009.

[2] Dalmazo, Bruno L., J. P. Vilela, and Marilia Curado. "Performance analysis of network traffic predictors in the cloud." Journal of Network and Systems Management 25(2) pp. 290-320, 2017.

[3] 심규석, 윤성호, 이수강, 김성민, 정우석, 김명섭. "네트워크 트래픽 분석을 위한 Snort Content 규칙 자동 생성." 한국통신학회논문지 40(4) pp. 666-677, 2015

[4] A. Garg and P. Maheshwari, "Performance analysis of Snort-based Intrusion Detection System," 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), 2016, pp. 1-5,