# SNI 정보를 활용한 Zoom 사용자 행위 탐지

김주성, 박지태, 호태규*, 홍윤환*, 김명섭
고려대학교, *닥터소프트
{jsung0514, pjj5846, tsmkim}@korea.ac.kr, *{tghui92, hong}@doctorsoft.co.kr

# Identification of Zoom User Behaviors using SNI Information

Ju-Sung Kim, Jee-Tae Park, Tae-Gyu Ho*, Youn-Hwan Hong*, Myung-Sub Kim
Korea Univ., *Doctorsoft

요 약

SaaS는 클라우드 기반으로 소프트웨어 제공 모델이다. 최근 많은 기업들에서 SaaS의 사용이 증가하고 있다. 기업의 효과적인 자산 관리를 위해서는 관리 부서에서 SaaS의 구매 및 사용을 관리해야 한다. 하지만 승인하지 않은 클라우드 소프트웨어를 구매하여 사용하는 Shadow IT 현상이 발생하면서 문제가 발생하고 있다. 이러한 리스크를 관리하면서 효율적인 자산 운용을 위하여 SaaS 사용 모니터링이 필요하다. 따라서 본 논문에서는 Zoom을 사용한 트래픽을 IP / Port 기반 분석 방법과 SNI 정보를 활용한 분석 방법을 사용하여 사용자의 행위를 탐지하는 방법론에 대해 제안한다.

## Ⅰ. 서론[1)]

SaaS(Software as a Service)란, 소프트웨어를 인터넷을 통해 제공하는 모델로서, 고객은 인터넷을 통해 소프트웨어를 사용하고 유지보수를 제공하는 공급자는 클라우드를 통해 소프트웨어를 제공하고 관리하는 형태를 말한다[1]. SaaS 서비스는 초기 비용이 상대적으로 적고 사용자의 필요에 따라서 선택적으로 사용할 수 있다는 장점으로 인해 최근 기업이나 단체에서의 사용이 많아졌고 효율적인 자산 운용을 하기 위해 모니터링을 통한 관리를 필요로 하게 됐다.

모니터링을 통한 관리가 중요한 이유는 Shadow IT 때문이다. Shadow IT란 조직 내에서 IT 부서의 승인 없이 구매, 배포 또는 사용되는 IT 서비스 또는 솔루션을 의미한다[2]. 기업에서 SaaS 애플리케이션을 사용할 때 관리가 제대로 이루어지지 않는 경우가 발생하게 되며, 이는 보안 위험성을 포함하여 조직 내부에서의 IT 부서의 통제 및 관리 능력을 저해할 수 있는 문제를 야기할 수 있다. 따라서 이러한 문제를 해결하고 기업의 손해를 줄이기 위해서 SaaS 사용 모니터링의 필요성이 대두되고 있다.

트래픽 분석에 사용되는 방법론으로는 IP / Port 기반 분석 방법, 통계 정보를 활용한 분석 방법, 머신 러닝을 활용한 분석 방법, SNI 정보를 활용한 분석 방법 등이 있다[3]. 본 논문에서는 헤더 기반 분석 방법과 SNI 정보를 활용한 분석 방법을 사용해서 Zoom의 사용자 행위를 탐지하는 방법을 제안한다.

Zoom은 화상회의 솔루션 업체인 ZOOM Video Communications가 개발한 화상회의 프로그램이며[4] 최근 코로나19의 유행으로 비대면으로 활동하면서 우리가 가장 많이 사용한 SaaS 응용프로그램이다. 따라서 본 논문에서는 Zoom을 사용한 트래픽을 분석하여 사용자의 행위를 탐지하여 사용자가 어떤 행위(로그인, 로그아웃 등)를 했는지에 대한 정보를 제공할 수 있는 방법을 제안하고자 한다.

본 논문의 구성은 본 장의 서론에 이어 2장 본론에서 Zoom 사용자의 행위를 정의하고, Zoom 사용자의 행위를 탐지하는 방법론에 대해 언급한다. 3장 결론 및 향후 연구에서는 해당 연구를 정리하고 향후 연구에 진행할 내용에 대해 언급하는 순서로 진행한다.

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).

## Ⅱ. 본론

본 논문에서는 Zoom 트래픽을 분석하여 사용자가 Zoom을 사용할 때의 행위를 탐지하는 방법론에 대해 기술한다. 트래픽 분석은 SNI 정보를 활용한 분석 방법과 헤더 기반 분석 방법을 사용하였다.

Zoom 사용자의 행위 분석을 위하여 소프트웨어를 사용하기 위해 필수적으로 진행해야 하는 행위를 정의하였다. Zoom을 사용하면서 여러 가지 공통된 행위를 진행하여 플로우를 분석하였으며, 분석 시 공통적으로 발생한 플로우를 바탕으로 행위를 정의하였다.

트래픽 분석 방법으로는 각 행위 별 SNI 시그니처를 정의하여 각 4가지 행위를 탐지하였다. Zoom을 사용하게 되면 SSL/TLS 기반으로 암호화된 패킷으로 이루어진 플로우가 발생한다. 암호화된 패킷은 443 Port를 사용하여 통신하기 때문에 443 Port에서 발생한 플로우를 기준으로 플로우를 모아 SNI 정보를 확인해서 해당 행위에 대한 시그니처를 정의하였다. 이후, 정의된 시그니처를 포함하는 플로우가 발생하면 해당 행위가 탐지되었다고 판단한다. 다음 표 1은 정의한 사용자의 행위, 행위의 시점과 시그니처를 정리한 것이다.

표 1. Zoom 사용자 행위 및 시그니처 정의

| 행위 정의 | 정의 시점 | 행위 시그니처 |
|---|---|---|
| 로그인 | ID, Password 입력 | xmpp(\d{3}).zoom.us |
| 회의 참여 | 화상 회의 시작 | zoom([a-z]{5}\d{3})mmr.([a-z]{3}).zoom.us |
| 회의 종료 | 화상 회의 종료 | evt-us.ds.corp.zoom.us |
| 로그아웃 | 애플리케이션에서 계정 로그아웃 | logfiles.zoom.us |

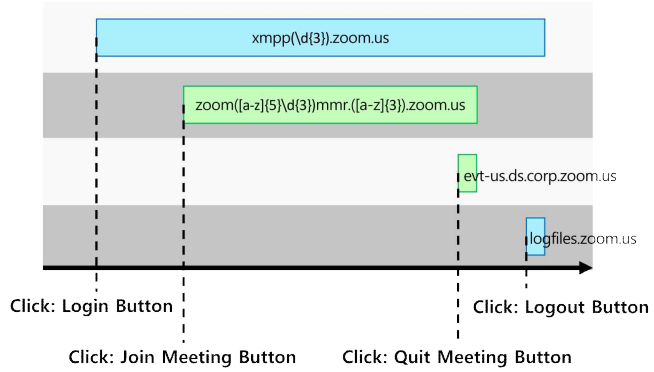


그림 1. Zoom 사용자 행위 탐지 알고리즘

그림 1은 Zoom의 사용자 행위 탐지 알고리즘을 나타낸다. 사전에 정의한 행위 중에 로그인, 회의 참여와 같은 시작과 관련된 행위 별로 정의된 탐지 시점에 해당 행위를 수행하면 탐지 시그니처를 포함한 플로우가 발생하게 된다. 발생한 시그니처 플로우는 탐지 시점으로부터 통신을 수행하여 행위의 종료 때까지 유지된다. 예를 들어 로그인 버튼을 누르면 로그인 행위에 대한 시그니처 플로우가 발생하고, 해당 시그니처 플로우는 로그아웃이 발생 할 때까지 통신을 유지한다.

최종적으로 수행되었던 로그인, 회의 참여 행위 이후에 종료 버튼을 클릭하면 로그아웃, 회의 종료 행위의 탐지 시그니처를 포함한 플로우가 발생하고, 유지되던 통신이 종료된다.

**Algorithm**: User Behavior Detection
**Input**: Entire Flow
**Output**: Behavior
**[Notation]**
$PN_F$ : Port Number of the Flow / $SNI_F$ : SNI of the Flow / $S_{1\sim4}$ : Signature of the (Login/Join Meeting/Quit Meeting/Logout) Flow / $T_{FO}$ : Time of the Flow Occurred / $T_{LI}$ : Time of the 'Login' Flow / $T_{JM}$ : Time of the 'Join Meeting' Flow

```
// User Behavior Detection
    for i=1 to Numbers of PN_F 443 Flow in Entire Flows
        if SNI_F == S_1
            state = "Login"
            T_LI = T_FO
            if SNI_F == S_2
                state = "Join Meeting"
                T_JM = T_FO
                if SNI_F == S_3
                    if T_FO > T_JM
                        state = "Quit Meeting"
            else if SNI_F == S_4
                if T_FO > T_LI
                    state = "Logout"
        else
            continue
```

그림 2. Zoom 행위 탐지 의사코드

그림 2는 Zoom 사용자 행위 탐지 알고리즘을 의사코드로 나타낸 것이다. 로그인 시 발생하는 [xmpp(\d{3})..zoom.us] 시그니처를 포함한 플로우가 발생하게 되면 로그인이 탐지되었다고 판단한다. 로그인이 탐지 될 경우, 해당 시그니처를 포함한 플로우의 발생 시간을 도출하고 이를 저장한다. 저장된 시간은 추후 로그아웃을 탐지할 때 사용된다. 회의 참여 행위는 [zoom([a-z]{5}\d{3})mmr.([a-z]{3}).zoom.us], [nws.zoom.us] 시그니처들을 포함한 플로우가 발생하게 되면 회의 참여를 탐지한다. 그리고 해당 시그니처를 포함한 플로우가 발생하면 해당 시간을 저장한다. 저장된 시간은 추후 회의 종료를 탐지할 때 사용된다. 회의 종료는 [evt-us.ds.corp.zoom.us] 시그니처를 가진 플로우가 발생하고 해당 플로우 발생 시간이 이전에 [zoom([a-z]{5}\d{3})mmr.([a-z]{3}).zoom.us]을 포함한 플로우로 회의 참여를 탐지했을 때 저장했던 시간과 비교해 회의 참여가 탐지된 시간보다 뒤의 시간이면 회의 종료가 탐지되었다고 판단한다. 로그아웃 행위는 [logfiles.zoom.us] 시그니처를 포함한 플로우가 발생하고 해당 플로우 발생 시간이 이전에 [xmpp(\d{3}).zoom.us]을 포함한 플로우로 로그인을 탐지했을 때 저장했던 시간과 비교해 로그인이 탐지된 시간보다 뒤의 시간이면 로그아웃 탐지되었다고 판단할 수 있다.

알고리즘 구현 후 검증을 하기 위해 교내외 여러 환경에서 Wireshark를 통해 수집한 트래픽을 대상으로 실험을 진행했고 플로우 발생 시간과 호스트 IP, 사용자 행위를 정확하게 도출하는 것을 확인하였다.

## Ⅲ. 결론 및 향후 연구

클라우드 서비스가 사용이 되면서, 대부분의 기업들이 적은 비용을 통해 SaaS 어플리케이션을 사용하게 되었다. 하지만 기업에서 관리하지 못하는 비승인 클라우드 서비스가 발생하게 되고, 이는 곧 기업의 효율적인 자산 운용에 영향을 미치게 된다. 이러한 Shadow IT 문제를 해결하기 위해 SaaS 모니터링 기술이 필요하다.

본 논문은 SaaS 서비스 중에서도 우리가 많이 사용하는 Zoom을 대상으로 트래픽 분석을 진행하였다. IP / Port 기반 분석 방법과 플로우의 SNI 정보를 바탕으로 트래픽을 분석하였으며, 분석된 정보를 기반으로 시그니처를 정의해 로그인, 회의 참여, 회의 종료, 로그아웃에 대한 사용자 행위를 탐지하는 방법을 제안하였다.

하지만, 사용자가 회의 종료 과정이나 로그아웃 과정을 생략하고 바로 응용프로그램을 종료할 경우, 행위 정의의 기준이 되었던 플로우가 발생하지 않을 수 있으므로 모든 경우에서 행위를 탐지할 수 없다는 한계가 있다. 향후 연구로 일반적이지 않은 행위의 흐름이 발생하더라도 정확한 행위 탐지할 수 있도록 알고리즘을 수정하여 보완할 예정이다.

## 참 고 문 헌

[1] Lowery, Craig, and Mark Armstrong. "Software as a Service." IEEE Internet Computing, vol. 9, no. 6, Nov./Dec. 2005, pp. 96-101.

[2] Kaplan, Charles, and David Norton. "The Challenges of Shadow IT Governance in the Age of Digital Transformation." Sloan Management Review, vol. 50, no. 3, 2009, pp. 21-31.

[3] 이민성, 박지태, 최정우, 김명섭, "페이로드 시그니처를 이용한 마이크로소프트 Office 365 서비스 탐지", 2020년도 한국통신학회 추계종합학술발표회, Nov. 13, 2020

[4] 하두진, 박민준. "ZOOM을 활용한 스마트 e-러닝 적용 시고" 한국중국어교육학회 학술대회, June. 2021, pp. 15-45.