Fingerprinting Secure Messaging Application Network Traffic

Cristina Alarcon, Mohammad Saidur Rahman
clalarcon@miners.utep.edu, msrahman3@utep.edu
Department of Computer Science, University of Texas at El Paso

Abstract

Traffic analysis can reveal sensitive user activity even when network traffic is encrypted. This project investigates the possibility of fingerprinting encrypted TikTok traffic to detect user actions by capturing and analyzing network flows with tshark. This was done on a Raspberry Pi, configured as a Wi-Fi access point using RaspAp. Using a clean Android device connected through the Raspberry Pi, we automated scenarios that reflect average TikTok usage (scrolling, likes, and shares) while background traffic from Chrome and other apps provided environmental noise. These findings demonstrate privacy risks in modern encrypted applications.

Prior research has been largely YouTube focused and has not addressed short-form platforms, which are characterized by frequent swiping and very short watch times. The goal is to understand what behavioral signals remain visible in flow-level metadata (packet sizes, packet directions, etc.) after application payloads are protected and to assess how a passive observer could exploit those signals in real networks.

Our threat model focuses on realistic passive observers such as a compromised public Wi-Fi operator or a campus network administrator. Test scenarios were scripted with Android Debug Bridge (ADB) to automate the data collection and maintain consistency. RaspAp was used as an interface for the passive observer to view information such as the connected devices' IP addresses and the number of clients. To isolate TikTok traffic, we applied filters for DNS queries and TLS Server Name Indication (SNI) values associated with TikTok domains (tiktokv.com).

Preliminary results indicate that TikTok traffic exhibits distinctive patterns even with background noise. During TikTok viewing sessions, there are sudden increases in downstream traffic often coincided with TCP retransmissions. This suggests that TikTok's video delivery mechanism may involve preloading or buffering events that trigger retransmissions when packets are delayed or dropped. These retransmission bursts align with user interactions such as scrolling to the next video or pausing.

This behavior creates a secondary fingerprint that can be used to infer not only that a video was viewed, but also when transitions occurred between videos. Overall, our study emphasizes the need for traffic level defenses and continued attention to metadata leakage in the design of privacy preserving mobile applications.