СИСТЕМИ ОБФУСКАЦІЇ ТРАФІКУ ДЛЯ ЗАХИСТУ ВІД ГЛИБОКОЇ ІНСПЕКЦІЇ ПАКЕТІВ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Обфускація мережевого трафіку є методом захисту від перехоплення і аналізу вмісту трафіку в інформаційно-комунікаційних системах, завдяки чому цей метод широко застосовується для уникнення блокування мережевих протоколів DPI-системами і мережевими фільтрами [1].

Сучасні системи глибокої інспекції трафіку набули значного розвитку і активно застосовують методи машинного навчання, які дозволяють виявляти протоколи обфускації по статистичних характеристиках, ентропії, часових інтервалах між пакетами та по інших паттернах трафіку. У зв'язку з цим актуальним є пошук адаптивних комбінованих рішень [2, 3], які забезпечують високий рівень стійкості до атак та до аналізу обфускованого трафіку при збереженні продуктивності мережі.

Метою доповіді є розгляд сучасних підходів до обфускації трафіку, методів розрізнення обфускованого трафіку, а також визначення критеріїв та порівняння за ними сучасних систем, що реалізують різні підходи до обфускації трафіку.

В доповіді наводяться результати практичного порівняння систем обфускації трафіку Shadowsocks, V2Ray, obfs4 та Rosen за наступними критеріями: стійкість до DPI, стійкість до атак (активного втручання в протокол обфускації) та статистичного аналізу, а також ефективність, продуктивність і ресурсоємність обфускації. Наведені дані показують, що кожна з розглянутих систем має свої переваги та недоліки, і тому найбільш ефективним підходом є комбіноване застосування одночасно декількох рішень, зокрема стеку систем обфускації трафіку Shadowsocks + V2Ray + Cloudflare CDN [4].

Список літератури

1. Wu, M., Sippe, J., Sivakumar, D., Burg, J., Anderson, P., Wang, X., ... & Wustrow, E. How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic. In 32nd USENIX Security Symposium (USENIX Security 23). 2023. С. 2653-2670. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/wu-mingshi.

2. Alwhbi, I. A., Zou, C. C., & Alharbi, R. N. Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning. Sensors. 2024. 24. №11:3509. DOI: https://doi.org/10.3390/s24113509.

3. Zhou, J.; Fu, W.; Hu, W.; Sun, Z.; He, T.; Zhang, Z. Challenges and Advances in Analyzing TLS 1.3-Encrypted Traffic: A Comprehensive Survey. Electronics. 2024. 13. №20:4000. DOI: https://doi.org/10.3390/electronics13204000.

4. Umar, A. Obfuscating Network Traffic to Circumvent Censorship. 2021. URL: https://sy.st/archive/Paper/obfuscating-network-traffic.pdf.