УДК 004.03 (043.2)

А.В. Ільєнко, к.т.н.
С.С. Ільєнко, к.т.н.
О.О. Вертиполох
Національний авіаційний університет, Київ

ПІДХІД ЩОДО ВИКОРИСТАННЯ DOH ТА DOT ПРОТОКОЛІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

При проектуванні сучасних інформаційно-телекомунікаційних систем та мереж одним з найважливіших є завдання забезпечення захисту інформації з використанням новітніх методів та підходів. До найбільш ефективних методів рішення даного завдання варто віднести застосування підходу щодо захисту трафіку від втручання DPI систем, як забезпечення конфіденційності та цілісності інформаційних повідомлень.

Враховуючи аналіз останніх досліджень і публікацій, актуальним є питання захисту мережевого трафіку від втручання DPI систем, принцип дії якого ґрунтується на дослідженні вразливих місць стандартів, а саме DNS-запитів з врахуванням особливостей функціонування типових мережевих протоколів, з якими має справу переважна більшість користувачів мережі Інтернет.

Під поняттям DPI система будемо розуміти таку систему, яка виконує, так званий, глибокий аналіз мережевих пакетів на верхніх рівнях моделі OSI. Традиційний аналіз пакетів зазвичай перевіряє інформацію в заголовках пакетів мережевого та транспортного рівнів, DPI спрямований також на поведінковий аналіз трафіку прикладного рівня у режимі реального часу, тобто такий, що дозволяє розпізнавати користувацькі програми, для яких заздалегідь не визначено відомі заголовки протоколів та структури даних.

Використовуючи особливості мережевих протоколів можна виділити такі способи обходу DPI блокувань: додавання пробілів або інших символів табуляції між методом HTTP (GET, POST тощо) та URI; змішування літер регістру значення заголовка хоста; видалення пробілу між назвою заголовка та значенням у заголовку хосту; фрагментація на рівня TCP для першого пакету даних; фрагментація на рівні TCP для постійних сеансів HTTP; надсилання підроблених пакетів HTTP з низьким значенням часу

життя або неправильною контрольною сумою.

Сучасний веб та деякі інші мережеві протоколи захищені за допомогою TLS, але DNS-запити всю свою історію передають в незашифрованому вигляді. Компанії або держави використовують це в своїх інтересах, наприклад, для збору інформації про відвідувані сайти або фільтрації трафіку або навіть проводити атаки на DNS трафік, так званий спуфінг запитів з метою перенаправлення їх на власний сервер. Тому з метою вирішення проблеми шифрування DNS пропонуються такі протоколи: DNSCrypt; DNS-over-TLS (DoT); DNS-over-HTTPS (DoH); DNS-over-SSH (DoS); DNS-over-QUIC (DoQ).

Відповідно до проведеного аналізу авторами пропонується використання поєднаних методів DoT та DoH, які дозволяють одразу, без впровадження нових протоколів, із забезпеченням зворотної сумісності реалізувати захищену передачу трафіку. Перший метод більшого розповсюдження набуває на мобільних пристроях, наприклад, входить до реалізації Android 9. У той же час другий метод більшого поширення набув в системах, що вже реалізують використання HTTPS, наприклад, браузери.

Авторами реалізовано власний комплекс локального проксуючого серверу мовою програмування Python 3.8, та проведено його тестування на реальній системі. Цей комплекс дозволяє встановлювати захищене з’єднання з іншими довіреними серверами на базі використання протоколів DoH та DoT, та унеможливлює або значно ускладнює можливість використання DPI систем на межі звичайних місць їх встановлювання. Зважаючи на досягнення мети роботи практична цінність цих рішень є актуальною та необхідною для більшості користувачів та систем. Запропоноване рішення локального проксуючого серверу може бути розвинуто і далі. Наприклад, впроваджено реалізацію локального кешування або додано можливість створювати точніші правила для певних доменів та їх піддоменів, а реалізований тестовий DoH сервер може бути розгорнуто на довіреному виділеному сервері за межами можливих точок встановлення фільтруючого обладнання, що дасть змогу повністю контролювати власний трафік для резолвінгу доменних імен. Така реалізація дасть змогу повністю контролювати власний трафік для резолвінгу доменних імен.