

УДК 004.056.5, 004.7

КАЛАНЧА АНДРІЙ АНДРІЙОВИЧ

курсант 1 курсу факультету №4

Харківського національного університету внутрішніх справ;

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ

ЗАСОБИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В МЕРЕЖІ

Згідно статті 11 і 21 Закону України «Про інформацію» до конфіденційної інформації про фізичну особу, зокрема, належать дані про її національність, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Хоча сьогодні інформація про інтереси користувача - гарячий товар. Її збирають про кожного, хто спілкується в цифровому світі, використовують самі та/або перепродують. Таргетована реклама, відстеження усієї мережевої активності інтернет-провайдерів, стеження зі сторони держави та інші негативні соціальні явища, що порушують нашу конфіденційність вже стали буденними для кожного. Забезпечити власну безпеку (анонімність) в мережі - тяжка праця, що вимагає масивного обсягу знань. Навіть кращі знавці у цій сфері не завжди можуть впоратися. Перше що потрібно розуміти, так це те, що 100% анонімність - це міф, бо повна анонімність може бути тільки при відсутності пристрою взагалі [0].

Проксі-сервери

Глобально, коли говорять «проксі-сервер», то мають на увазі щось, що виступає посередником між клієнтом і адресатом.

У розрізі забезпечення анонімності проксі-сервери бувають:

- HTTP-(веб)-проксі-сервери. Такі сервери пропускають через себе тільки HTTP-трафік;
- SOCKS-проксі-сервери. На відміну від HTTP-проксі-серверів, SOCKS передає всю інформацію, нічого не додаючи від себе;
- окремо варто згадати CGI-проксі або «анонімайзери», які по суті становлять собою web-сервер з формою, де клієнт вводить адресу потрібного

сайту. Після чого відкривається сторінка запитаного ресурсу, але в адресному рядку браузера видно адресу CGI-проксі. CGI-проксі, як і будь-який web-сервер може використовувати https для захисту каналу зв'язку між собою і клієнтом [2].

Схему роботи проксі-серверу ви бачите на рисунку 1.

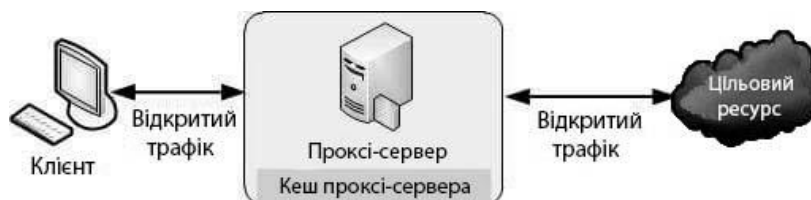


Рисунок 1. — Схема роботи проксі-сервера

Переваги проксі-серверів:

- проксі дешеві, в мережі можна знайти багато безкоштовних проксі.

Недоліки проксі-серверів:

- треба довіряти проксі-серверу;
- для http-проксі треба фільтрувати HTTP-заголовки;
- необхідність налаштування проксі-сервера для кожної програми або використання окремих програм-соксифікаторів, наприклад, Proxifier.

VPN/SSH

Йдеться про VPN, маючи на увазі також і SSH-тунелі. Оскільки, не зважаючи на деякі відмінності, основний принцип у них однаковий. Схема роботи VPN показана на рисунку 2.



Рисунок 2. — Схема роботи VPN

Наразі комерційними провайдерами пропонуються такі протоколи VPN:

- PPTP - використовується найбільш широко, швидкий, легко налаштовується, проте вважається «найменш захищеним» порівняно з іншими;

- L2TP + IPSec. L2TP забезпечує транспорт, а IPSec відповідає за шифрування. Ця зв'язка має більш сильне шифрування, ніж PPTP, стійка до вразливостей PPTP, забезпечує також цілісність повідомлень і автентифікацію сторін;

- OpenVPN - безпечний, відкритий, а отже, поширений, дозволяє обходити блокування, але вимагає окремого програмного клієнта;

- SSTP - такий же безпечний, як і OpenVPN, окремого клієнта не вимагає, проте сильно обмежений у платформах: Vista SP1, Win7, Win8.

Окремо варто відзначити сервіси, що надають «DoubleVPN», коли перед тим, як вийти в Інтернет, трафік проходить 2 різних VPN-сервери в різних країнах, або навіть «QuadVPN», коли використовується 4 сервери, які користувач може вибрати сам і розташувати в довільному порядку [2].

Переваги VPN/SSH:

- швидко і зручно, не треба окремо налаштовувати програми.

Недоліки VPN/SSH:

- потрібно довіряти VPN/SSH-серверу/провайдеру.

Tor

Це система маршрутизаторів, в якій клієнт з'єднується з Інтернетом через ланцюжок вузлів. Як правило, ланцюжок складається з трьох вузлів, кожному з них невідомі адреси клієнта і ресурсу одночасно. Крім того, Тор шифрує повідомлення окремо для кожного вузла, а відкритий трафік видно тільки вихідному роутеру [2]. Схема роботи Тор показана на рисунку 3.

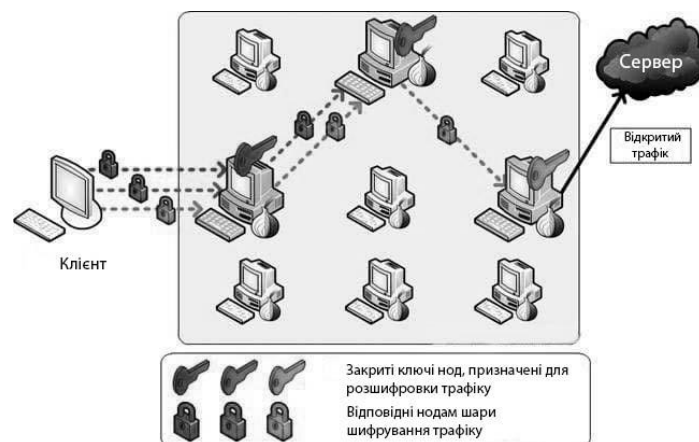


Рисунок 3. — Схема роботи Тор

Переваги Tor:

- високий ступінь анонімності клієнта при дотриманні всіх правил;
- простота використання (завантажив Tor Browser Bundle, запустив і користуйся).

Недоліки Tor:

- вихідний трафік прослуховується;
- низька швидкість;
- наявність керуючих серверів.

Висновки. Анонімність - соціокультурне явище, що побудоване довкола поняття приватності та свободи кожної людини в Мережі. Зараз інформація про інтереси користувача – це гарячий товар. Її збирають про кожного, хто спілкується в цифровому світі, використовують самі та/або перепродують. Як збирають інформацію і кому це може бути цікаво – нікому не відомо, оскільки ними може бути як продавець таргетованої реклами, так і правління, яке активно відслідковує кожен наш крок в житті за допомогою геолокації і пошуковий запит в мережі Інтернет; інформація про те, хто і про що говорив, яку думку має. Тож дотримуватися анонімності в мережі, можливо, наш єдиний спосіб уберегтися від «Великого Брата», тобто від паноптикуму, і хоча б у кіберпросторі залишатися тими, ким ми є справді і не боятися переслідувань за власну думку, інтереси та бажання. Інтернет – місце, де кожен може бути вільним у всіх розуміннях цього слова.

Список використаних джерел:

1. Практичний посібник з анонімності в онлайні [Електронний ресурс]. – Режим доступу : <https://habr.com/ru/company/vdsina/blog/556914/>
2. Методи анонімності у мережі [Електронний ресурс]. – Режим доступу : <https://blog.agronavtika.ru/2016/03/18/metodyi-anonimnosti-v-seti-chast-1-pros/>