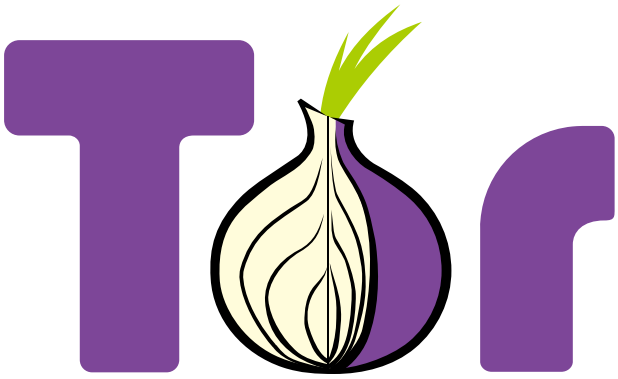
Wojciech Myszka

Laboratorium 4: Przeglądarka TOR (sieci TOR) wer. 27 z drobnymi modyfikacjami!

2020-03-26 10:37:38 +0100

1. Cel laboratorium



Celem zajęć jest zapoznanie się z ideą sieci TOR i przeglądarką TOR Browser.

Jak już wszyscy mogli się przekonać zwykłe połączenia sieciowe nie są w żadens posób zabezpieczone prze różnego rodzaju „podsłuchem”:

1. Transmisja przesyłana w wielu rodzajach medium nie jest w żaden sposób szyfrowana (dziś nie dotyczy to już praktycznie transmisji radiowej WiFi).
2. Zarówno „drugi koniec” transmisji jak i ewentualni podsłuchujący mogą (stosunkowo) łatwo zdobyć informacje o adresie po-

czątkowym, adresie końcowym i dokładnym czasie nawiązania połączenia.[1]

Użycie protokołu HTTPS/TLS chroni przed podglądaniem przesyłanych informacji. VPN w jakimś zakresie może ukrywać adres źródłowy. Zazwyczaj jeden serwer VPN obsługuje wielu klientów więc o ile można zaobserwować fakt nawiązania połączenia z nim wobec szyfrowania informacji nie da się później (łatwo) powiązać ruchu wychodzącego z serwera VPN z ruchem przychodzącym.

Sieć TOR stara się połączyć obie powyższe cechy w sposób zapewniający użytkownikowi sporo prywatności. System nie jest **absolutnie** pewny. W przypadku transmisji nieszyfrowanej węzeł końcowy ma dostęp do zawartości pakietów. Użycie protokołu HTTPS częściowo problem poprawia.

Prace nad systemem zapoczątkowało U.S. Naval Research Laboratory, był rozwijany przez Defense Advanced Research Projects Agency (DARPA) i opatentowany przez Marynarkę Wojenną w 1998 roku. Głównym zadaniem systemu było umożliwienia przesyłania informacji (wywiadowczych) z wykorzystaniem jak najprostszych środków. Na pewny etapie kod oprogramowania został opublikowany na otwartej licencji.

2. Zasada działania sieci TOR

Aby zapewnić maksimum prywatności używa się trasowania cebulowego[2]

Do działania sieci TOR potrzebne jest istnienie węzła katalogowego, który przekazuje nadawcy listę węzłów, które mogą być wykorzystane do transmisji. Wybierana jest z nich (losowo) trasa pakietu. Wiadomość jest szyfrowana i żaden węzeł (za wyjątkiem ostatniego) nie wie na której pozycji się znajduje.

[1] Informacje te nazywane bywają „metadanymi”, stosunkowo łatwo można je gromadzić (nie zawsze wymagane są odpowiednie zezwolenia sądowe). Nawet jeżeli ich przydatność jest ograniczona — użytkownik sieci może czuć się skrępowany.

[2] Istnieje również trasowanie czosnkowe.

Każdy pakiet danych jest wielokrotnie zaszyfrowany. Każdy kolejny węzeł „zdejmuje koleją warstwę szyfrowania" dowiaduje się o punkcie docelowym i przekazuje pakiet dalej.

Podobnie następuje przekazanie pakietu „powrotnego".

Podczas transmisji żaden z węzłów pośrednich nie zna ani punktu początkowego, ani końcowego transmisji. Wie jedynie o dwu sąsiadach.

3. Zadania do wykonania

Najprostszym sposobem skorzystania z sieci TOR jest użycie specjalnej przeglądarki (TOR Browser). Jest na dostępna dla praktycznie wszystkich najważniejszych systemów operacyjnych (Windows, Linux, Mac, Android). Można również zapoznać się z jej kodem źródłowym. Instalacja nie wymaga praw administratora.

Tor Browser to specjalnie spreparowana przeglądarka Firefox (prac ująca w trybie prywatnym) wraz z oprogramowaniem pozwalającym korzystać z sieci

1. Zainstalować przeglądarkę (w odpowiedniej wersji)
2. Sprawdzić (kilkakrotnie) z jakiego adresu przeglądarka łączy się z innymi serwerami (na przykład korzystając z serwera `https://whatismyipaddress.com/`). Porównać z wynikami dla „zwykłej przeglądarki".
3. Zapoznać się z kontrolkami w polu adresu (ikonka ). Zwłaszcza zwrócić uwagę na ścieżkę Tor (Tor Circuit).
4. Zapoznać się z ustawieniami dotyczącymi prywatności przeglądarki Tor Browser.

4. Uwaga końcowa

Generalnie Tor Browser poprawia bezpieczeństwo w sieci, ale należy pamiętać, że jest to program, więc nie jest wolny od błędów. I całkiem niedawno (pisanie tej instrukcji rozpocząłem 12 marca 2020, kończę 23) wykryto błąd powodujący uruchamianie skryptów java tam gdzie

nie powinny być one uruchamiane. Wersja łatająca tę dziurę została opublikowana 18 marca.

5. Instrukcja w postaci jednego pliku...

...jest również dostępna.