Bezpieczeństwo w sieci: technologia I2P

Michał Palwal/Karol Gosławski/Filip Kuliński

03.02.2020

Sieć Invisible Internet Project(w skrócie I2P)powstała z modyfikacji sieci Freenet. Jest to sieć peer-to-peer(w skrócie P2P)czyli taki model komunikacji, który zapewnia wszystkim hostom te same uprawnienia.
Podstawę I2P stanowią węzły, które biorą udział w trasowaniu połączeń.
W I2P węzłem jest każdy użytkownik sieci Brak centralnego węzła sprawia, że szyfrowanie przesyłanych paczek danych odbywa się przez każdy z węzłów pośredniczących w transmisji. W sieci I2P transmisja danych realizowana jest poprzez jednokierunkowe tunele (nadawcze oraz odbiorcze).

Tunele nadawcze	ruch odbywa się w kierunku od sieci do węzła tworzącego tunel
Tunele odbiorcze	obsługujące ruch wychodzący od twórcy tunelu do sieci.

Rysunek 1: Sieć I2P

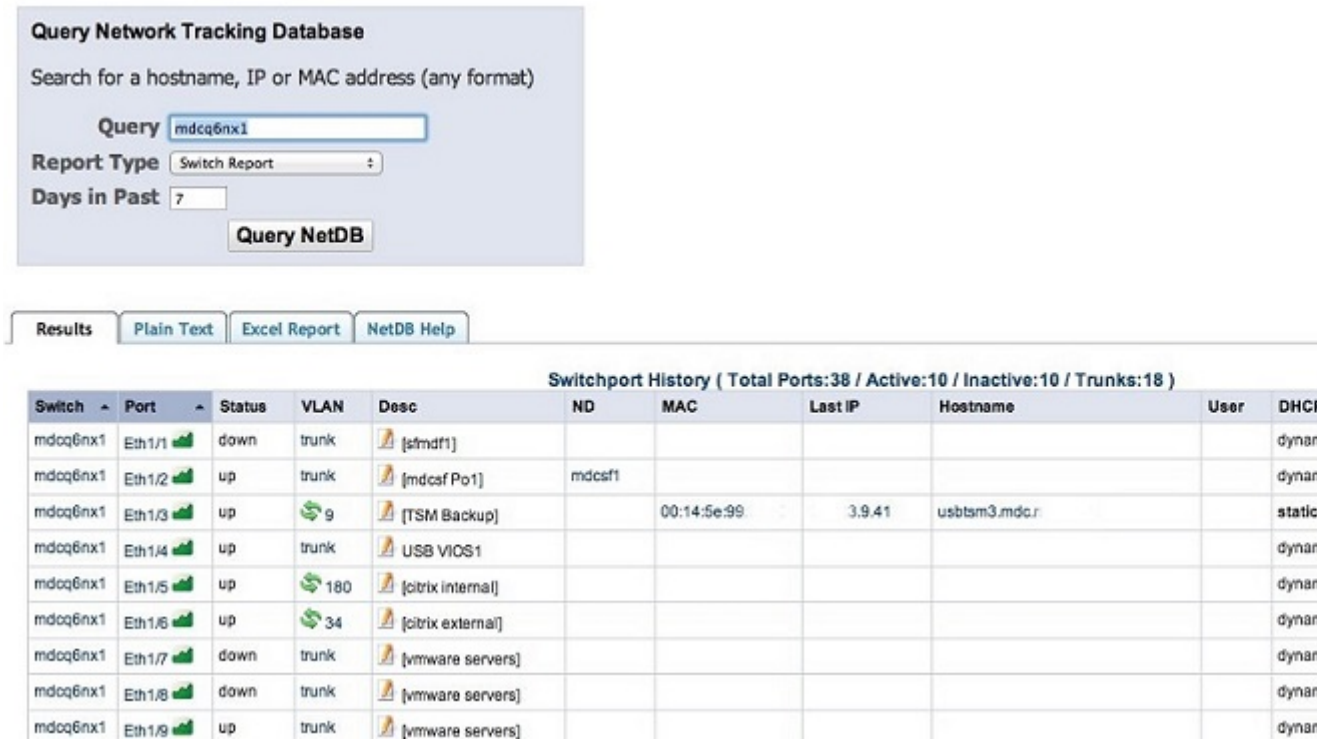
Dane o przekaźnikach I2P znajdują się w rozproszonej bazie danych o nazwie netDb.
Jeżeli podłączamy się do I2P, my także stajemy się częścią netDb, a program do obsługi sieci utworzy na komputerze dwa zestawy informacji:

1 routerInfo:

Etykieta węzła I2P, zawierająca klucze kryptograficzne do automatycznego szyfrowania połączeń odbieranych i szyfrowanych, adres IP oraz cyfrową sygnaturę potwierdzającą tożsamość.

2 leaseSet:

Informacje o otwartych tunelach danego komputera. Użytkownicy I2P odbierają i wysyłają pakiety dwoma osobnymi, wirtualnymi tunelami.



Rysunek 2: NetDb

Przykład: Chcemy podłączyć z serwerem użytkownika X wykorzystując mechanizm I2P.

1) Nasz komputer wyszukuje w netDb kryptograficzne klucze użytkownika X oraz dane o bramie wejściowej do jego tunelu odbierającego.

2) Szyfrujemy poszczególne żądania do witryny użytkownika X, a następnie wiążemy je w zakodowany pakiet. Szyfrowanie to odbywa się za pomocą jego 2048-bitowego klucza publicznego utworzonego algorytmem ElGamal.

3) Nasz komputer wybiera trzy losowe węzły sieci I2P i tworzy za ich pomocą tunel wysyłający. Zakodowany pakiet szyfrowany jest kolejnymi jednosesyjnymi kluczami publicznymi AES węzłów.

4) Kolejne węzły dekodują pakiet swoimi kluczami prywatnymi do momentu, w którym ostatni z nich, brama wyjściowa, otrzyma zakodowany pakiet.

5) W momencie gdy zakodowany pakiet opuszcza tunel wysyłający, brama wyjściowa tworzy na niej specjalną, międzytunelową warstwę szyfrowania.

6) Komputer użytkownika X tworzy tunel odbierający między trzema innymi losowymi węzłami sieci I2P. zakodowany pakiet trafia do bramy wejściowej, czyli pierwszego węzła tunelu odbierającego. Tunel odbierający dekoduje międzytunelową warstwę szyfrowania i przekazuje wiadomość dalej, w kierunku użytkownika X.

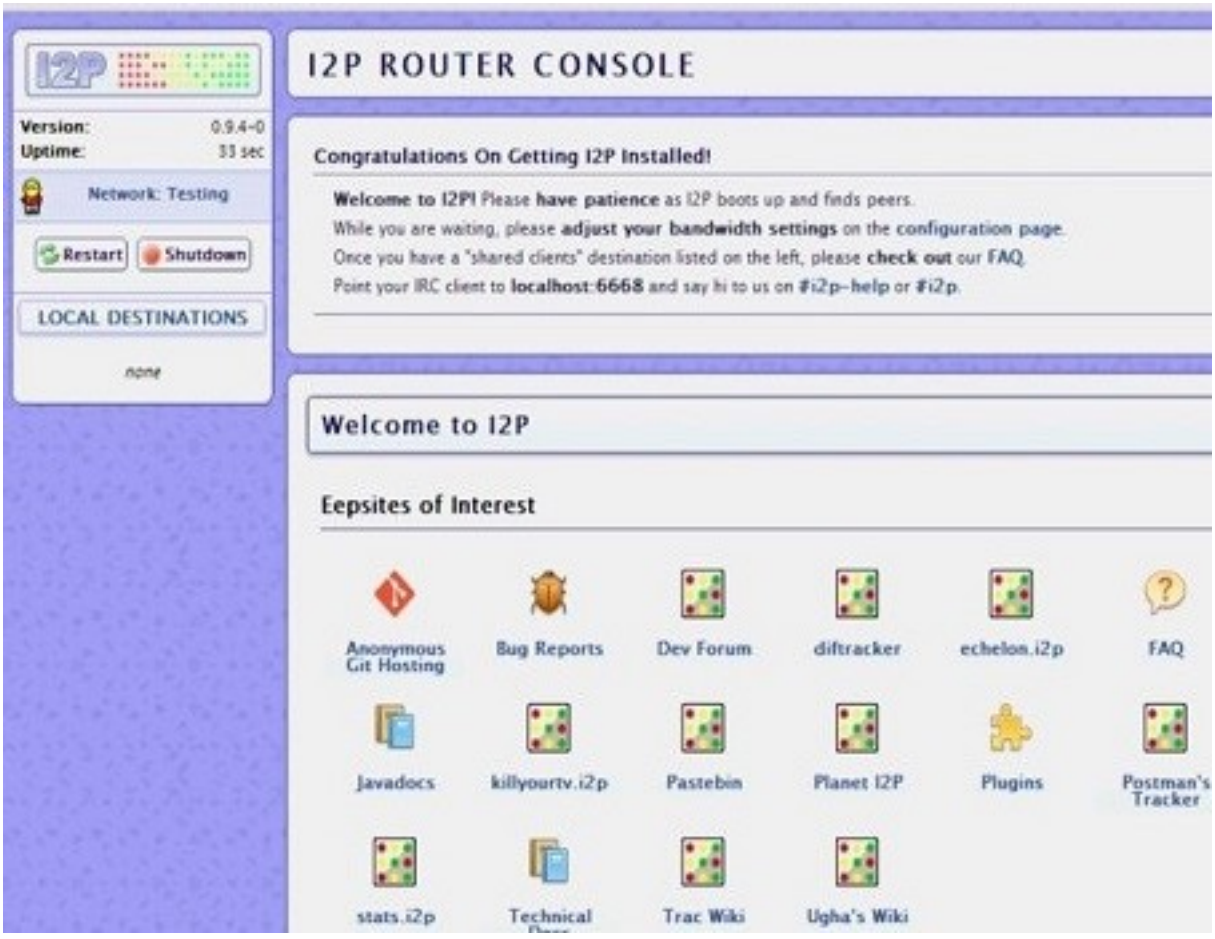
7) Węzły tunelu odbierającego użytkownika X szyfrują przekaz swoimi jednosesyjnymi kluczami publicznymi AES, a prywatne klucze przekazują użytkownikowi X. Za ich pomocą użytkownik X zdejmuje warstwy szyfrowania. Dzieje się tak do chwili, w której otrzyma „goły" pakiet. Wówczas za pomocą własnego klucza prywatnego ElGamal otrzymuje właściwą treść naszego żądania. Jeżeli witryna użytkownika X odpowie na nasz sygnał, jego komputer będzie musiał wykonać analogiczne czynności.

Instalacja i korzystanie z I2P:

Do przeglądania zasobów I2P potrzeba oficjalnego klienta tej sieci, którego łatwo ściągnąć z jego witryny https://geti2p.net/pl/

Paczka jest dostępna dla systemów BSD, Linux, Windows, OS X, a także w wersji przenośnej dla Androida. Aby program zadziałał poprawnie, na naszym komputerze musi się znajdować klient Javy w wersji 1.6 lub nowszej.

W panelu kontrolnym znajdziemy wszystkie najważniejsze informacje techniczne o połączeniu, a także linki do najbardziej użytecznych ukrytych usług sieci I2P.



Rysunek 3: I2P Router console

Jak dokonać wyboru pomiędzy Tor oraz I2P?

Niewątpliwą zaletą Tora jest większa liczba użytkowników niż jest to w przypadku I2P, szersze wsparcie ze strony profesjonalistów, pokaźne wsparcie finansowe, a także nakierowanie na w pełni bezpieczne przeglądanie internetu. Wiele znaczy także i to, że jest napisany w języku programowania C, a nie w Javie.

I2P, mimo że jest mniejszy, także posiada swoje mocne strony: w pełni zdecentralizowaną architekturę peer-to-peer, traktowanie wszystkich użytkowników jako węzły, nakierowanie na organizację darknetu, szersze wsparcie dla protokołów sieciowych, a także szybszy przepływ danych wewnątrz sieci (w I2P każdy komputer przyjmuje jednocześnie określoną liczbę tuneli, na przykład dwa odbierające i dwa wysyłające; w Torze każdy komputer, który łączy się z serwerem, ma własną trasę).

Rysunek 4: