Ciemna strona Internetu

Internet to bez wątpienia jedno z najważniejszych osiągnięć ludzkości w XX wieku. Jest to ogromna sieć komputerów z całego świata, która umożliwia szybką komunikację. Co więcej, jest tak zaprojektowana, aby uzyskać bardzo dużą niezawodność. To znaczy, jeśli jakiś węzeł w sieci, jakiś kabel łączący pewne węzły, czy nawet spora część wszystkich węzłów i kabli, ulegnie awarii, to i tak reszta sieci będzie potrafiła się komunikować, znajdując *ad hoc* nowe ścieżki między nieuszkodzonymi węzłami.

Powyższa własność (niezawodność) była głównym założeniem Internetu i została zrealizowana naprawdę znakomicie (technicznie ten model nazwano TCP/IP). Natomiast projektanci zupełnie pominęli inny aspekt – prywatność komunikacji. W samym czystym Internecie nie ma wbudowanych żadnych mechanizmów szyfrowania. Innymi słowy, każda porcja wysyłanej informacji (czyli tak zwany *pakiet* TCP/IP) biegnie po sieci jawnym tekstem, co oznacza, że każdy po drodze może odczytać jej treść, nadawcę, odbiorcę. Naturalnie to nie jest tak, że o bezpieczeństwie nikt nie pomyślał. Po prostu uznano, że ten element (jeśli będzie potrzebny) załatwi się – jak to się żargonowo mówi – *w wyższej warstwie abstrakcji*.

I rzeczywiście – tajność *treści* wiadomości użytkownicy mogą sobie stosunkowo łatwo zapewnić. Wystarczy, że sami będą (albo zrobi to za nich jakieś oprogramowanie czy protokół warstwy wyższej, np. TLS) szyfrować wiadomości lokalnie na swoich komputerach i wysyłać do Internetu już tylko szyfrogramy.

Schody zaczynają się gdzie indziej. Znacznie trudniej ukryć jest sam fakt *odbycia* komunikacji w Internecie między węzłem sieci X a węzłem Y. Z tym problemem stara się sobie radzić społeczność projektu TOR (*The Onion Router*, czyli „trasowanie cebulowe"). Pomysł polega na tym, aby wysyłanie bezpośrednie wspomóc obecnością trzech (wylosowanych ze społeczności!) pośredników. Zamiast pakietów $[X \to Y]$ po Internecie będą się więc kręciły wyłącznie pakiety $[X \to P_1]$, $[P_1 \to P_2]$, $[P_2 \to P_3]$ oraz $[P_3 \to Y]$. Co więcej, odpowiednio szyfrowane są również adresy węzłów, z czego wynika, że adres X-a zna tylko (zakładając jego uczciwość względem społeczności TOR) P_1, a adres Y-a – tylko P_3.

TOR jest więc swoistą siecią w sieci, gdzie węzły przede wszystkim pośredniczą w komunikacji między innymi węzłami. Gdy ruch jest duży, to ścieżki komunikacji często na siebie nachodzą, co sprawia, że z zewnątrz (spoza TORa) w zasadzie nie jest możliwe odczytanie, kto z kim *naprawdę* się komunikuje.

Oczywiście, jak zawsze w kryptologii, należy się zastanowić, co się stanie, gdy kontrolę nad częścią węzłów TORa przejmie *ten zły* (albo ten dobry, w zależności od miejsca siedzenia względem barykady). Jest jasne, że ktoś, kto jednocześnie kontroluje P_1, P_2 oraz P_3, wie, że X rozmawia z Y. Z drugiej strony – szyfrowanie adresów zapewnia, że nawet kontrola nad dwoma spośród trzech pośredników pozwala co najwyżej stwierdzić, że zarówno X, jak i Y korzystają z TORa, ale w żaden sposób nie umożliwia ich wzajemnego skojarzenia. (Oczywiście oznacza to, że bezpieczeństwo TORa musi opierać się na założeniu, że procent *przejętych* węzłów jest niski).

TOR umożliwia jeszcze więcej, konkretnie – tworzenie tak zwanych *serwisów ukrytych*. Polega to na tym, że można stworzyć jakiś serwis (powiedzmy stronę www) w taki sposób, aby nikt nie mógł go zamknąć ani nie mógł odkryć, kto go stworzył. To zadanie nie jest wcale dużo trudniejsze od ukrytej komunikacji. Autor serwisu wybiera (losuje) w sieci TOR kilka węzłów, odzywa się do nich (oczywiście anonimowo, za pomocą opisanego wyżej systemu trzech pośredników) i prosi, aby pełnili rolę ukrytych wejść do jego serwisu. Klienci serwisu nigdy nie będą odzywać się do niego bezpośrednio, a jedynie właśnie poprzez te ukryte wejścia (a i do nich tylko za pomocą trzech pośredników). Ostatecznie, po zakończeniu protokołu wejścia do serwisu od klienta do serwera jest aż sześciu pośredników.

Anonimowość, którą oferuje TOR, jest niezwykle duża. Aby się o tym przekonać, zacytujmy fragment z tajnego raportu amerykańskiej agencji NSA, który został upubliczniony przez Edwarda Snowdena. NSA pisze w nim, że TOR jest „królem superbezpiecznych i szybkich sieci anonimizujących". Opisuje też pomysły na pewne ataki na cyberprzestępców (operacja pod kryptonimem Egoistyczna Żyrafa). Z dokumentu wynika, że NSA ma z TORem poważny problem i odnosi tylko drobne sukcesy w walce z nim. TOR sam w sobie nie został nigdy skutecznie zaatakowany. Natomiast udało się zamknąć niektóre serwisy ukryte wewnątrz TORa, na przykład portal Silk Road (`http://silkroadvb5piz3r.onion`), na którym handlowano przede wszystkim substancjami psychoaktywnymi.

Co pewnie oczywiste, płatności w serwisach ukrytych dokonuje się zwykle za pomocą bitcoinów. Dla pełnej anonimowości pozostaje jednak problem, jak niepostrzeżenie je zdobyć. Ale i tutaj ludzkość sobie poradziła. Poniżej przykład prawdziwego ogłoszenia (jak podał `satoshi.pl` za `localbitcoins.com`), które można było znaleźć w „tradycyjnym" Internecie:

Jesteś z Trójmiasta i chcesz kupić bitcoiny za gotówkę, aby być całkowicie anonimowym posiadaczem najpopularniejszej kryptowaluty? Żadnych przelewów, osobista sprzedaż za gotówkę, koszt całkowity = 1,05 x (cena BTC po aktualnym kursie z `pln.bitcurex.com`) + 20 PLN. Jak to działa? Cała komunikacja z mojej strony odbywa się za pośrednictwem TORa, co i Tobie radzę zrobić. Maile proszę wysyłać jedynie z poczty Tor Mail. Po ustaleniu warunków transakcji, już jako osoba fizyczna, zakupię odpowiednią ilość BTC na giełdzie bitcurex, po czym w ustalonym miejscu i czasie dokonamy wymiany. Tym sposobem WIELKI BRAT będzie tylko wiedział, że ktoś gdzieś kupił kiedyś jakąś ilość bitcoinów, ale już nie będzie w stanie powiązać tej kwoty z Tobą.

Każda nowoczesna technologia ma dwa końce.

Tomasz KAZANA