ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2012
Seria: ORGANIZACJA I ZARZĄDZANIE z. 63a Nr kol. 1891

Jacek GRUBER, Ireneusz J. JÓŹWIAK, Łukasz ŁOZIUK
Politechnika Wrocławska
Instytut Informatyki

BEZPIECZEŃSTWO INFORMACJI W WIRTUALNEJ SIECI TOR I KRYPTOWALUTA BITCOIN

Streszczenie. W artykule omówiono stan aktualny i zastosowania wirtualnej sieci komputerowej TOR (ang. *The Onion Router*). TOR jest wirtualną siecią komputerową z oprogramowaniem implementującym infrastrukturę sieciową implementującą mechanizmy trasowania zapobiegające analizie ruchu sieciowego. Przeanalizowano ideę i wirtualny rynek waluty Bitcoin, która przyczyniła się znacząco do rozwoju sieci TOR. Dokonano oceny znaczenia TOR dla wolności przepływu informacji i wolności komunikacji społecznej w Internecie.

INFORMATION SECURITY IN THE TOR VIRTUAL NETWORK AND CRYPTO CURRENCY BITCOIN

Summary. In this article the current state and use of the TOR (*The Onion Router*) virtual network are discussed. TOR is a virtual computer network with software that implements a network infrastructure that implements the routing mechanisms to prevent traffic analysis. The paper presents the analysis of the idea and the virtual currency market Bitcoin, which contributed significantly to the development of the TOR network. An assessment of the importance of TOR for freedom of information and freedom of communication on the Internet.

1. Sieć TOR

Sieć TOR to wolne programowanie i otwarta sieć, pomagające chronić się przed inwigilacją w Internecie. Inwigilacja zagraża wolności osobistej, prywatności oraz relacjom, zarówno biznesowym, jak i międzyludzkim, a nawet bezpieczeństwu państwa.

Przedsiębiorstwa stosują sieć TOR, aby chronić się przed konkurencją i utrzymać strategie biznesowe w tajemnicy. Sieć tę wykorzystuje się też do anonimowego zgłaszania nadużyć ze

stref wojennych i do zgłaszania przypadków oraz mechanizmów korupcji w instytucjach. Dziennikarze używają sieci TOR do ochrony przebiegu śledztw dziennikarskich i źródeł pozyskiwanych informacji. Wojsko i policja używają sieć TOR do chronienia komunikacji, śledztw i zbierania informacji. Nieuprzywilejowani użytkownicy używają sieć TOR, by chronić siebie, swoich krewnych i ich godność podczas używania Internetu.

Sieć TOR została zaprojektowana, zaimplementowana i jest używana przez laboratoria amerykańskiej marynarki U.S. Naval Reaserch Laboratory. Podstawowym celem projektu było zapewnienie bezpieczeństwa rządowej komunikacji. Efektem była wirtualna sieć tuneli komunikacyjnych, pozwalająca partnerom komunikacji poprawić prywatność i bezpieczeństwo w Internecie. Sieć TOR jest również platformą programistyczną, pozwalającą tworzyć narzędzia komunikacji, wykorzystujące jej zalety. Platforma ta stanowi podstawę szerokiego zakresu aplikacji, pozwalających organizacjom i użytkownikom komunikować się przez sieć publiczną bez utraty prywatności [1].

Zastosowanie sieci TOR chroni przed pospolitą formą inwigilacji internetowej, tzw. analizą ruchu sieciowego (ang. *traffic analysis*). Analiza ruchu sieciowego może być stosowana do różnych celów. Jednym z zastosowań jest identyfikacja partnerów komunikacji rozmawiających przez sieć publiczną, którymi są systemy i użytkownicy. Znajomość źródła i celu ruchu sieciowego pozwala śledzić zachowanie użytkowników Internetu i ich zainteresowania, co może mieć wpływ na ceny towarów i usług. Przykładowo, przedsiębiorstwo e-biznesowe może różnicować oferowane ceny ze względu na miejsce zamieszkania klienta. Analiza ruchu sieciowego może zagrażać wykonywaniu działalności zawodowej poprzez ujawnianie lokalizacji aktualnego geograficznego położenia pracowników. Gdy wyjeżdżamy za granicę i łączymy się z serwerem pracodawcy, by sprawdzić pocztę, możemy zdradzić swoją narodowość i zawód każdemu kto obserwuje ruch sieciowy, nawet gdy połączenie jest szyfrowane, gdyż nagłówki pakietów nie są szyfrowane [1].

Pakiety internetowe składają się z dwóch części – danych i nagłówków potrzebnych do trasowania. Dane to wysyłana i odbierana treść, na przykład zdjęcia, treść e-maili i zawartość plików z innymi danymi. Nawet jeśli przesyłane dane zostaną zaszyfrowane, analiza ruchu i tak ujawnia znaczną część aktywności użytkowników w sieci, część tego co robimy i często tego co piszemy. Analiza ruchu skupia się na nagłówkach, które określają adresata, nadawcę, rozmiar, synchronizację i inne szczegóły komunikacji.

Podstawowym problemem jest fakt, że odbiorcy naszej komunikacji mogą zobaczyć przez spojrzenie na nagłówek, że to my wysyłaliśmy danych pakiet i dane. Mogą to również robić nieautoryzowani pośrednicy komunikacji sieciowej. Bardzo prosta forma analizy ruchu

sieciowego może polegać na ulokowaniu się pośrednika pomiędzy określonym nadawcą i konkretnym odbiorcą i przeglądaniu nagłówków pakietów w ich komunikacji. Nie ma wątpliwości, że taka działalność stanowi już atak na proces komunikacji, polegający na szpiegowaniu poczynań komunikacyjnych użytkowników.

Istnieją również znacznie silniejsze sposoby analizy ruchu. Niektórzy atakujący szpiegują w wielu częściach Internetu oraz używają wyszukanych technik statystycznych do śledzenia i identyfikacji szablonów komunikacji, różnych organizacji i jednostek [1].

Zastosowanie sieci TOR polega na redukcji zagrożenia ze strony zarówno prostej, jak i złożonej analizy ruchu sieciowego. W tym celu sieć TOR rozprasza komunikację, kierując ją w wiele miejsc w Internecie i tym samym powodując, że żaden pojedynczy węzeł nie może wskazać lokalizacji użytkownika będącego stroną komunikacji. Stosowana idea jest analogiczna do stosowanej w życiu i polega na poruszaniu się skomplikowaną, trudną do śledzenia trasą w celu zgubienia śledzącego, a także na regularnym usuwaniu śladów takiej marszruty. Zamiast obierania bezpośredniej trasy od źródła do celu, pakiety danych sieci TOR obierają ścieżkę losową, przez wiele przekaźników, a przekaźniki ukrywają ślady tak, że żaden obserwator w pojedynczym węźle nie jest w stanie powiedzieć skąd dane przyszły i dokąd są kierowane [1].

Do utworzenia prywatnej ścieżki w infrastrukturze sieci TOR, oprogramowanie użytkownika przyrostowo buduje w sieci obwód z szyfrowanych połączeń. Co niewielki odcinek czasu obwód jest zmieniany, a każdy węzeł wzdłuż drogi wie jedynie, który węzeł dostarczył mu pakiet i któremu węzłowi pakiet przekazać. Klient kreowanej ścieżki komunikacyjnej negocjuje osobny zestaw kluczy szyfrowych dla każdego węzła w obwodzie, by zagwarantować sobie, że żaden węzeł nie będzie w stanie wyśledzić tych połączeń.

Po ustanowieniu obwodu można nim wymieniać różnorodne dane, co zapewnia różnorodność oprogramowania, zarówno istniejącego, jak i możliwego do zaprojektowania, bazującego na sieci TOR. Ze względu na to, że węzeł widzi nie więcej niż jeden skok pakietu w obwodzie, ani podsłuchujący, ani węzeł ustanowiony przez szpiega nie może użyć analizy ruchu do określenia źródła i adresu docelowego komunikacji.

Ponieważ TOR działa na potrzeby strumieni TCP, może zostać użyty przez dowolną aplikację, korzystająca z gniazdek SOCKS. W celu zwiększenia wydajności, sieć TOR wykorzystuje ten sam obwód dla połączeń realizowanych w pewnym odcinku czasu, na przykład w ciągu 10 minut. Późniejszej komunikacji przypisywany jest już inny obwód. Celem tej strategii jest zapobieżenie skojarzeniu wcześniejszej działalności komunikacyjnej użytkownika z działalnością późniejszą.

Sieć TOR umożliwia również użytkownikom ukrywanie swojej pozycji sieciowej, zatem i geograficznej, przy korzystaniu z różnorodnych usług publikacyjnych i wymiany informacji oraz opinii poprzez fora internetowe. Użytkownicy sieci TOR mogą łączyć się do tych ukrytych serwisów anonimowo. Tego rodzaju funkcjonalności pozwalają użytkownikom sieci TOR budować aplikacje i serwisy internetowe do publikowania i wypowiadania się bez obawy o mniej lub bardziej zinstytucjonalizowaną cenzurę. Nikt nie byłby w stanie stwierdzić, kto oferuje stronę z forum internetowym, i nikt, kto wystawił stronę, nie byłby w stanie określić, kto napisał i zawiesił na forum lub na tablicy opinię lub post.

Sieć TOR nie może rozwiązać wszystkich problemów anonimowości, gdyż koncentruje się jedynie na ochronie transportu danych. Jeśli nie chcemy, by strony, które oglądamy, widziały dane nas identyfikujące, musimy używać oprogramowania zgodnego z protokołem TOR. Przykładowo, podczas korzystania i nawigowania w sieci można używać programu *Torbutton*. Program ten zatrzymuje cześć informacji o konfiguracji komputera. Nie ujawniajmy poufnych danych na forach internetowych i nie wykonujmy innych nierozsądnych działań osłabiających ochronę naszej tożsamości i naszych chronionych danych.

Musimy być świadomi, że TOR, jak wszystkie anonimowe sieci, które są wystarczająco szybkie do surfowania, nie zapewnia ochrony przed tzw. atakami *end-to-end timing attacks*, czyli analizą statystycznej próby domyślenia się, jakie dane były szyfrowane, na podstawie czasu, który był potrzebny by je zaszyfrować, a także przed obserwacją ruchu wejścia i wyjścia z sieci. Inaczej mówiąc, gdy są podejrzenia, że użytkownik A może zaatakować serwer B, infrastruktura bezpieczeństwa i odpowiednie służby administracyjne mogą obserwować ruch od użytkownika A. Gdy okaże się, że serwer B otrzymuje żądania wtedy, gdy użytkownik A wysyła zaszyfrowane pakiety, oznacza to, że pakiety otrzymane przez serwer B należą do użytkownika A [1].

2. Kryptowaluta Bitcoin

Bitcoin to wirtualna waluta utworzona w 2009 roku przez Satoshi Nakamoto [2]. Jest to także nazwa oprogramowania udostępnianego na zasadach open source, którego celem jest możliwość korzystania z tej waluty.

Waluta Bitcoin jest jedną z pierwszych prób implementacji koncepcji nazywanej kryptowalutą, która po raz pierwszy została opisana w 1998 roku przez Wei Dai na liście mailingowej *cypherpunks*. Waluta została wykreowana w przekonaniu, że w ogólnym pojęciu

moneta jednostkowa BTC waluty Bitcoin to dowolny przedmiot lub jakikolwiek zapis, który można zaakceptować jako zapłatę za dobra i usługi oraz jako spłatę długów w określonym kraju, lub ma ona jakieś inne socjoekonomiczne znaczenie. Waluta Bitcoin została wykreowana na podstawie idei wykorzystywania kryptologii w celu kontroli tworzenia i przekazywania pieniędzy, zamiast w tym celu polegać na centralnym wydawcy (emitencie) [4].

Bitcoin jest tzw. walutą peer-to-peer. Określenie peer-to-peer znaczy, że nie ma jednego centralnego punktu do emitowania pieniędzy czy monitorowania transakcji. Zadania te są wykonywane kolektywnie przez sieć, do której waluta jest organicznie przywiązana.

Do emitowania pieniędzy i monitorowania transakcji Bitcoin wykorzystuje kryptografię klucza publicznego. Monety mają klucz publiczny ich właściciela. Kiedy pieniądze są wysyłane od użytkownika A do użytkownika B, to użytkownik A dodaje do monet klucz publiczny użytkownika B i całość podpisuje swoim kluczem prywatnym. Od tego momentu to użytkownik B ma monety i może nimi dysponować wedle swoich życzeń. Aby użytkownik A ponownie nie wydał pieniędzy, które już do niego nie należą, wszystkie transakcje są trzymane w sieci jawnie przez wszystkich użytkowników. Przed każdą operacją ważność monet jest sprawdzana [4].

Bitcoin tworzy i dystrybuuje (emituje) porcje nowych bitmonet (ang. bitcoin – BTC), szacunkowo 6 razy na godzinę w losowych odstępach czasu, do jednego z użytkowników. Potencjalnie każdy użytkownik kryptowaluty może otrzymać taką partię bitmonet dzięki użytkowaniu aplikacji bitcoinowej lub wykorzystaniu oprogramowania równoważnego, dostosowanego do posiadanego przez użytkownika wyposażenia. Generowanie bitmonet jest często nazywane *wydobywaniem*, przez analogię do wydobywania złota. Prawdopodobieństwo tego, iż dany użytkownik otrzyma partię monet, zależy od stosunku ilości mocy obliczeniowej wniesionej do sieci za pośrednictwem tego użytkownika do sumy mocy obliczeniowej wniesionej przez wszystkie węzły. Liczba bitmonet utworzona w partii nigdy nie jest większa niż 50 BTC (dane na luty 2011 r.), a nagrody w BTC są zaprogramowane na zmniejszanie się w czasie aż do zera, tak aby mogło zaistnieć kiedykolwiek nie więcej niż 21 milionów bitmonet. Oczekuje się, że w miarę jak wypłaty będą się zmniejszać, zbieranie opłat transakcyjnych będzie dla użytkowników motywacją do uruchamiania kolejnych węzłów generujących.

Wszystkie generujące węzły sieci współzawodniczą o pierwszeństwo w znalezieniu rozwiązania problemu kryptograficznego dla przetwarzanego bloku kandydującego, co wymaga stosowania metody powtarzających się prób i błędów. Kiedy węzeł znajdzie takie rozwiązanie, ogłasza je w sieci oraz deklaruje się posiadaczem nowej partii bitmonet. Miejsca końcowe (ang. *peers*), otrzymujące nowo rozwiązany blok, sprawdzają jego poprawność

przed zaakceptowaniem i dodaniem do łańcucha. Do obliczeń węzły mogą używać standardowego oprogramowania klienta i procesorów klasycznych CPU lub wykorzystywać inne oprogramowanie, wykorzystujące procesory graficzne GPU. Użytkownicy mogą także generować bitmonety BTC grupowo [4]. Tak więc każdy blok jest generowany co 10 minut, każdy węzeł osobno, co każde 2016 bloków (co w praktyce zajmuje średnio 2 tygodnie). Jeżeli bloki są generowane zbyt szybko lub zbyt wolno, co zależy od zwiększającej lub zmniejszającej się mocy obliczeniowej całej sieci, stopień trudności odpowiednio wzrasta lub maleje.

Odmiennie niż w przypadku konwencjonalnej waluty, Bitcoin, ze względu na swoją zdecentralizowaną naturę, nie pozwala żadnemu nadzorcy kontrolować waluty. W oprogramowaniu Bitcoin zaimplementowany jest na stałe mechanizm kontroli inflacji. Mechanizm ten jest znany wszystkim uczestnikom systemu na starcie.

Transfery pieniędzy BTC w walucie Bitcoin są wykonywane bezpośrednio, bez pośrednictwa operatorów finansowych prowadzonych przez osoby trzecie. Taki typ transakcji gwarantuje niewykonalność refundacji. Klient sieci Bitcoin ogłasza transakcję do otaczających go węzłów, które propagują płatność do reszty sieci [4]. Uszkodzone lub niewłaściwe transakcje są odrzucane przez *uczciwe* węzły. Transakcje są w większości darmowe, ale w celu nadania priorytetu transakcji wobec innych węzłów może być uiszczana opłata. Całkowita liczba bitmonet w czasie dąży do 21 milionów w 2033 roku. Zasoby pieniądza rosną geometrycznie w odcinkach zwiększającego się liniowo tempa, wzrastającego co 4 lata. W 2013 roku będzie wygenerowana połowa całkowitych zasobów Bitcoin, a w 2017 roku zostanie wygenerowane 75% [3],[6] jej całkowitych zasobów.

W miarę dochodzenia do granicy podaży pieniądza w walucie Bitcoin i braku pieniądza BTC w obiegu, wartość bitmonet zacznie doświadczać wzrostu realnej wartości, czyli deflacji. Bitmonety są jednak podzielne do 8 miejsc po przecinku (co razem daje $2{,}1 \times 10^{15}$ jednostek), usuwając praktyczne limitowanie zniżkowych korekt cenowych w środowisku deflacyjnym. Oczekuje się, że w tym okresie węzły generujące (zapisujące transakcje do bloków) będą utrzymywać się z umiejętności konkurencyjnego zbierania opłat transakcyjnych, zamiast bicia nowych bitmonet.

3. Anonimowość a wolność w sieci TOR

Sieć TOR w połączeniu z kryptowalutą Bitcoin tworzy parę dającą użytkownikom wolność w Internecie. Dzięki nim użytkownik może nie tylko uniknąć sankcji gospodarczych nałożonych na dany kraj, cenzury oraz innych działań niekorzystnych i retorsji, ale również

uniknąć płacenia podatków, konsekwencji handlu narkotykami i handlu bronią – możliwości te omówiono poniżej. Wystarczy potrzebne oprogramowanie pobrać z miejsca https://www.torproject.org/. Proces instalacji jest bardzo dobrze wyjaśniony i prosty. Trzeba jednak wiedzieć, że niektóre z omówionych poniżej stron i zasobów zawierają materiały lub opisują praktyki zakazane przez polskie ustawodawstwo i prawodawstwo [5].

Przygodę z siecią TOR można zacząć od strony Torlinks, której opis znajduje się na stronie http://torlinkbgs6aabns.onion. Torlinks to wartościowa baza linków do różnych stron tematycznych, serwisów i grup dyskusyjnych z zakresu technologii TOR.

The Hidden Wiki, opisana w miejscu http://kpvz7ki2v5agwt35.onion, jest ukrytą wersją Wikipedii. Została podzielona na kategorie tematyczne. Stanowi bogaty zbiór linków i artykułów z sieci TOR.

Tor Mail, omówiony w linku http://jhiwjjlqpyawmpjx.onion, jest serwisem oferującym anonimowe konta pocztowe.

Serwis Silk Road, opisany w linku http://silkroadvb5piz3r.onion, to odpowiednik portalu aukcyjnego Allegro.pl, tyle tylko, że z produktami i towarami nielegalnymi. Można tu kupić szeroką gamę narkotyków, podróbek, fałszywych dokumentów, nielegalnie wyprodukowanych e-booków, dane ostępowe do kont w serwisach internetowych, sprzęt muzyczny i komputerowy niewiadomego pochodzenia.

W serwisie The Armory, opisanym w linku http://ayjkg6ombrsahbx2.onion, handluje się nielegalnie bronią i amunicją.

Torowisko to forum internetowe na platformie TOR. Poziom intelektualny tego forum jest wysoki w porównaniu z innymi ogólnodostępnymi w Internecie. Konieczność używania oprogramowania TOR stanowi przeszkodę na przykład dla gimnazjalistów, którzy na Torowisku pogardliwie nazywani są *gimbusami*. Interesujący na tym forum jest dział *Przekręty*. Można tam poznać techniki stosowane przez przestępców, aby móc się przed nimi bronić. Forum dysponuje obszerną bazą zeskanowanych dokumentów zawartych w linku http://vjelr2xdaqsgslzr.onion.

Strona internetowa Polish Black Market, znajdująca się w http://wcgk6z6zgem7gg2w.onion, skupia głównie rodzimych, *wyjętych spod prawa* przedsiębiorców.

4. Podsumowanie

Anonimowa sieć TOR w połączeniu z kryptowalutą Bitcoin to bardzo specyficzne i ciekawe technologicznie oraz koncepcyjnie rozwiązanie. Anonimowość komunikacji

i przesyłania danych stwarza niezwykłe możliwości dla ludzi, którzy chcieliby zmieniać świat na lepsze i bronić się przed oszustami. Jednak możliwości tych korzystają ludzie mający intencje zdecydowanie odmienne i próbujący oszukać innych, również na wielką skalę.

Tylko od czasu do czasu można usłyszeć o stosunkowo daleko posuniętej inwigilacji w Internecie i masowym podsłuchiwaniu w telefonii i innych mediach telekomunikacyjnych. Trudno orzec, czy i jak długo utrzyma się w mediach komunikacyjnych stan względnej wolności. Gdyby jednak ten stan się nie utrzymał i za jakiś czas wolność przepływu informacji i wolność komunikacji społecznej w mediach elektronicznych i telekomunikacyjnych załamałaby się, to o tę wolność nie trzeba by walczyć poprzez wystąpienia społeczne. Wystarczyłoby intensywnie rozwinąć sieć TOR, dodając do niej znacząco dużą ilość nowych węzłów sieci. Od niedawna można obserwować namiastki podobnych, alternatywnych metod zabiegania o wolność w sferze komunikacji społecznej.

Bibliografia

1. About Tor. https://www.torproject.org/about/overview.html.en, 20/04/2012.
2. Bitcoin P2P Digital Currency. http://bitcoin.org/about.html, 21/04/2012.
3. Kilka słów o bitcoin. http://bitcoin.pl/index.php/obitcoin, 19/04/2012.
4. Bitcoin, http://pl.wikipedia.org/wiki/Bitcoin. 5/05/2012.
5. Wszystko co związane z siecią Tor. http://www.wcgk6z6zgem7gg2w.onion, 6/6/2012.
6. Bitcoin P2P Digital Currency. http://bitcoin.org/about.html, 20/04/2012.

Abstract

TOR network in conjunction with a cryptocurrency Bitcoin is a revolutionary solution. In this article the current state and use of virtual network TOR (The Onion Router) are discussed. Also the paper presents the analysis of the idea and the virtual currency market Bitcoin, which contributed significantly to the development of the TOR network. Anonymity provides great opportunities for people who want to repair the world or protect themselves against fraud. On the other hand it gives the same opportunities for those who definitely do not intend to do it and are trying to harm other people. Bitcoin was created based on the idea of using cryptography to control the creation and money transfer. Bitcoin contributed to the thrive of the TOR network.