Darknet
zagrożenie czy przyszlość

Internet czy to cała sieć?

- Ze względu na ograniczenia prawne wprowadzane w sieci internet od lat rozwija się szara strefa majaca na celu wprowadzenie pełnej wolności – wolności absolutnej.

Rozmiary

- Szacuje się, że Darknet jest o kilka rządów wielkości większy, niż powszechnie znane strony na powierzchni sieci. Według niektórych szacunków, nawet 96% wszystkich danych znajduje się w szeroko rozumianej Deep Web (Głęboka sieć).

Realizacja

- ANts P2P – system wymiany plików P2P anonimizujący i szyfrujący ruch, obsługuje publikacje HTTP.
- Azureus – klient BitTorrent z dodatkową opcją użycia I2P lub Tor (open source, napisany w Javie)
- Freenet – odporny na cenzurę rozproszony system plików do anonimowej publikacji (open source, napisany w Javie)
- GNUnet – P2P framework, zawiera program do wymiany plików jako najważniejsza aplikację (projekt GNU, napisany w C)
- I2P – anonimizujaca powłoka sieciowa na której mogą być budowane aplikacje (open source, napisany w języku Java)
- Imule – modyfikacja emule działająca w sieci I2P
- MUTE – anonimizujący program do wymiany plików.
- Nodezilla – anonimizująca powłoka sieciowa o zamkniętym kodzie, na której można budować aplikacje (napisany w językach C++ oraz Java)
- Tor – Jest to jeden z największych projektów badawczych sieci anonimowych nastawiony na anonimowe przeglądanie internetu. Tor nie jest klientem P2P sam w sobie, tzn nie świadczy usług innym użytkownikom sieci.
- Winny – Klient P2P bardzo popularny w Japonii (freeware, napisany w C++ dla Windows)

Zasada działania

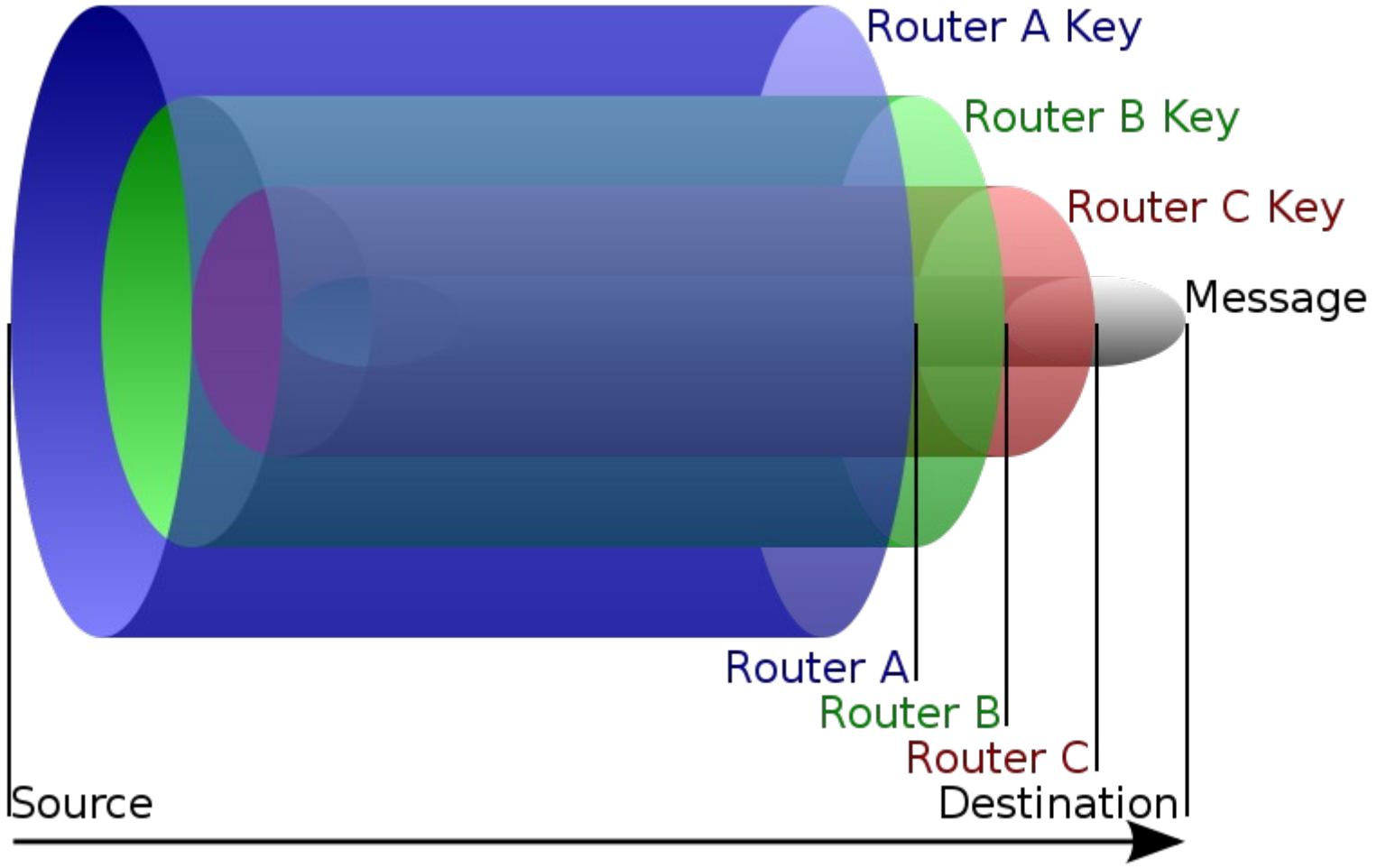
- Wszystkie te sieci oparte są na zasadzie wymiany peer2peer oraz by zagwarantować anonimowość głównie wykorzystują trasowanie cebulowe.

Trasowanie cebulowe

- Trasowanie cebulowe (ang. onion routing) - technika służąca anonimowej komunikacji w sieci komputerowej.

- Polega ona na wielokrotnym szyfrowaniu wiadomości, a następnie przesyłaniu jej przez szereg węzłów zwanych routerami cebulowymi (ang. onion routers). Każdy z nich usuwa warstwę szyfrowania w celu uzyskania informacji o dalszym trasowaniu i przesyła dane do następnego routera. Takie działanie zapobiega ujawnieniu węzłom pośredniczącym pochodzenia, odbiorcy oraz treści wiadomości. Trasowanie cebulowe opracowane zostało przez Davida Goldschlaga, Michaela Reeda oraz Paula Syversona.
- Począwszy od 2008 r. sieć Tor dominuje w wykorzystywaniu tej technologii

Trasowanie cebulowe



- Tor chroni tożsamość użytkowników oraz ich działalność w sieci przed analizą ruchu. Operatorzy utrzymują wirtualną sieć złożoną z ruterów cebulowych, zapewniającą anonimowość zarówno w sensie ukrycia lokalizacji użytkownika, jak też możliwości udostępniania anonimowych ukrytych usług.
- Wykorzystuje kryptografię, wielowarstwowo szyfrując przesyłane komunikaty (stąd określenie „trasowanie cebulowe”), zapewniając w ten sposób poufność przesyłania danych pomiędzy ruterami. Użytkownik musi mieć uruchomiony na swoim komputerze program, który łączy się z serwerem pośredniczącym sieci Tor[4]. Takie serwery, zwane węzłami, może uruchomić u siebie każdy, kto chce wspomóc rozwój Tora. Oprogramowanie łączące się z internetem może korzystać z Tora poprzez interfejs SOCKS.

- Tor nie oferuje całkowitej anonimowości i przy założeniu dostępu do odpowiednio dużych środków technicznych możliwe jest wytropienie danego użytkownika tej sieci[5]. Tor nie może i nie próbuje chronić przed monitorowaniem ruchu na granicach sieci, tzn. pakietów wchodzących i opuszczających sieć[6]. Na przykład rząd Stanów Zjednoczonych ma możliwość monitorowania dowolnego szerokopasmowego połączenia z Internetem dzięki urządzeniom wprowadzonym na podstawie Communications Assistance for Law Enforcement Act (CALEA) i dlatego może kontrolować oba punkty końcowe połączeń Tora, wykonywanych na terytorium USA. O ile Tor chroni przed analizą ruchu, nie może zapobiec potwierdzeniu komunikacji[6].

Historia

- Początkowo sponsorowany przez laboratoria badawcze Marynarki Wojennej Stanów Zjednoczonych, pod koniec 2004 r. stał się projektem firmowanym przez Electronic Frontier Foundation (EFF), która wspierała go finansowo aż do listopada 2005[7]. Obecnie rozwojem oprogramowania Tor zajmuje się Tor Project – organizacja non-profit (niedochodowa) o charakterze badawczo-edukacyjnym, z siedzibą w Stanach Zjednoczonych, otrzymująca wsparcie finansowe z różnych źróde

Trasa pakietu

- Użytkownicy uruchamiają na swoich komputerach oprogramowanie klienckie sieci Tor, które okresowo tworzy wirtualne obwody w sieci.
- Tor wielowarstwowo szyfruje przesyłane komunikaty (stąd nazwa „trasowanie cebulowe”), zapewniając doskonałą poufność przesyłania pomiędzy ruterami. Jednocześnie oprogramowanie udostępnia interfejs SOCKS klientom. Aplikacje potrafiące obsługiwać protokół SOCKS mogą być skonfigurowane tak, by łączyły się z internetem za pośrednictwem oprogramowania klienckiego Tor, pełniącego w tym wypadku funkcję proxy, które następnie multipleksuje ruch sieciowy przez wirtualny obwód sieci Tor.
- Wewnątrz sieci Tor ruch jest przekazywany pomiędzy ruterami, osiągając w końcu węzeł wyjściowy, z którego niezaszyfrowany pakiet jest przekazywany do miejsca przeznaczenia. Z punktu widzenia docelowego komputera, ruch wydaje się pochodzić z wyjściowego węzła sieci Tor.
- Schemat połączenia wygląda w następujący sposób.
  Użytkownik → węzeł1 → węzeł2 → węzeł3 → Serwer docelowy

- Sieć Tor działa na poziomie protokołu TCP i – inaczej niż większość pozostałych sieci anonimowych – nie narzuca ograniczeń co do możliwych zastosowań. Anonimizacji przy użyciu Tora poddawane są często takie aplikacje, jak IRC, komunikatory internetowe czy przeglądanie stron WWW. W przypadku WWW Tor na ogół stosuje się w parze z Privoxy, filtrującym serwerem pośredniczącym, mającym za zadanie ochronę prywatności na poziomie aplikacji.

Etykieta

- Nieodłącznie towarzysząca sieci Tor anonimowość sprawia, że tradycyjne praktyki administracyjne, zmierzające do przeciwdziałania nadużyciom, mogą być niewystarczające dla połączeń z niej wychodzących. Tor posiada funkcję, pozwalającą zredukować ten problem zarówno z perspektywy operatorów węzłów wyjściowych, jak i witryn osób trzecich.
- Węzły wyjściowe definiują swoją „politykę wyjściową”, która określa, jaki ruch jest, a jaki nie jest dopuszczalny przez ten węzeł. Większości najważniejszych nadużyć dotyczących sieci Tor można zapobiec, używając kombinacji adresu i portu. Potencjalne nadużycia obejmują:
  - Zapychanie łączy - Społeczność Tora uważa za niestosowne przesyłanie wielkich ilości danych przez sieć – rutery cebulowe są utrzymywane przez ochotników na własny koszt.
  - BitTorrent Protokół BitTorrent nie powinien być używany z siecią Tor ze względu na duże ilości przesyłanych danych. Domyślna polityka węzłów wyjściowych blokuje standardowe porty BitTorrent.
  - Spam Domyślna polityka wyjściowa blokuje połączenia z portem 25, zapobiegając rozsyłaniu spamu bezpośrednio z sieci Tor.
  - Anonimowi użytkownicy Serwisy, które chcą odmiennie traktować użytkowników odwiedzających je poprzez Tor, mają taką możliwość.

TOR

- TOR (Tor’s Onion Router Network) jest prawdopodobnie najprostszą i najpopularniejszą implementacją Darknetu.
- Technologia ta została opracowana przez wojska amerykańskie w celu umożliwienia anonimowego przesyłu informacji i do dziś nie znaleziono sposobu, aby ją złamać (niektórzy informatycy są przekonani, że nigdy to nie będzie możliwe).

TOR

- Występująca w niej domena .onion nie jest częścią rejestru ICANN i nie da się z nią połączyć bez użycia programu
- Ze względu na sposób działania routingu TOR, zarówno host obsługujący odwiedzaną stronę internetową, jak i klient zwracający, są ukryci i ich identyfikacja jest praktycznie niemożliwa.

- Kombinacja ta powoduje, że taka forma Internetu znajduje się daleko poza kontrolą jakiegokolwiek rządu lub regulacji.
- Użytkownik musi tylko kliknąć przycisk „Nowa tożsamość” („New Identity”), a program wybierze nowy węzeł, przez który będzie wysyłać zapytania – operacja ta nadaje ci nowy adres IP i całkowicie nową tożsamość, nawet w zwykłym Internecie.

- Dla systemu operacyjnego Windows istnieje też bardzo wygodna wersja Tora, która nie wymaga instalacji i zawiera w sobie skonfigurowaną przeglądarkę Firefox. Dzięki temu Tora możesz mieć zawsze przy sobie, np. na pendrive i odpalać go gdziekolwiek jesteś.

- Mając zainstalowanego TOR-a może uzyskać dostęp do wszystkich domen .onion, takich jak Hidden Wiki (adresy w domenie .onion wyglądają dosyć niekonwencjonalnie i mają niestesty nieprzyjemną dla użytkowinika formę;
- Hidden Wiki http://www.kpvz7ki2v5agwt35.onion/wiki/ która powie ci dużo o tym jak odnaleźć się w Darknecie i od czego zacząć.
- Własny hosting na Freedom Hosting (http://www.xqz3u5drneuzhaeo.onion/),
- blog na blog.masked (http://www.ms4kc75hlvnfcxgz.onion/)

- Tor to nieprzebrane bogactwo stron i informacji, po których z czasem nauczysz się swobodnie poruszać. W sieci będziesz mógł prowadzić własną pocztę e-mail, udzielać się na rozmaitych forach, przesyłać pliki, czy dokonywać transakcji handlowych z innymi użytkownikami z całego świata.

Nielegalne zastosowania

- Sieć Tor może być wykorzystywana do celów uznawanych za nielegalne w niektórych jurysdykcjach, jak na przykład krytykowanie przywódców państwowych, wymiana materiałów chronionych prawem autorskim bądź dystrybucja pornografii dziecięcej[20][21][22]. We wrześniu 2006 r. władze niemieckie, w trakcie operacji wymierzonej przeciwko pornografii dziecięcej, skonfiskowały sprzęt jednego z centrów danych, na którym uruchomione było oprogramowanie Tor

Słabości TOR

- Wycieki zapytań DNS
  - Podobnie jak w przypadku wielu innych systemów do anonimowego surfowania po internecie, część aplikacji nadal wykonuje bezpośrednie zapytania do serwerów domenowych (DNS), pomijając serwer pośredniczący Tor. Wykorzystanie Privoxy bądź polecenia „torify”, dystrybuowanego wraz z Torem, to jedne z możliwych rozwiązań tego problemu. Ponadto aplikacje używające protokołu SOCKS5, który obsługuje żądania proxy oparte na nazwach, mogą przesyłać przez Tora zapytania DNS, które zrealizuje węzeł wyjściowy, zapewniając w ten sposób anonimowość analogiczną jak dla innych danych przesyłanych przez sieć Tor

Słabości

- Analiza ruchu
  - Jak wszystkie współczesne sieci anonimowe z niewielkimi opóźnieniami (ang. low latency), Tor jest podatny na analizę ruchu przez adwersarzy, którzy mogą obserwować oba końce połączenia użytkownika
- Podsłuchiwanie przez węzły wyjściowe

Niebezpieczeństwa

- Tor może być niebezpieczny, jeśli jest niewłaściwie użyty, podobnie jak każda inna rzecz. Z Daknetu korzystają wszyscy: politycy, aktywiści, uciekinierzy, szpiedzy, detektywi, służby specjalne, rebelianci, hakerzy, spiskowcy, handlarze bronią, narkotykami, płatni mordercy, pedofile, alfonsi, złodzieje, oszuści… a także zwykli, przeciętni ludzie, którzy z jakiegoś powodu chcą skorzystać ze swojego naturalnego prawa do zachowanie prywatności i anonimowości.

- W Torze można znaleźć różne plugastwa, ale pamiętaj też, że nikt cie nie zmusza, aby tam wchodzić (dla własnego zdrowia psychicznego odradzam korzystanie z hostingów ze zdjęciami, oraz z niemoderowanych for, takich ja chany) – przy odrobinie zdrowego rozsądku, można tego wszystkiego uniknąć i cieszyć się wolnością poważnych i rzeczowych informacji, jakie można tam znaleźć.

I2P2 Network and .i2p Domains

- Inna forma Darknetu znajduje się w sieci I2P2. I2P działa w bardzo podobny sposób do Tora, choć jest nieco bardziej elastyczna i może być używana dla wielu różnych typów protokołów i różnych aplikacji, włączając w to Web access, email, IRC Chat i inne.
- Oprogramowanie to pozwala na dostęp do domeny I2P, która jest inną formą Darknetu.

Domeny namecoin .bit i alternatywny DNS

- Wiele podobnych wielkich projektów jest obecnie w fazie rozwoju.
- Namecoin jest zdecentralizowanym, rozpowszechnionych systemem DNS, zaopatrzonym w domenę najwyższego poziomu .bit, opartą na tej samej strukturze co Bitcoin (wirtualna waluta).
- Zasadniczo, należąc do „kopalni” Namecoin, w ten sama sposób można wydobywać bitcoiny.
- Jest to zatem wymienialne dla nazwy domeny .bit.
- Co ciekawe, ICANN zgłosił również niedawno zwiększenie liczby dozwolonych sufiksów internetowych.

Inne formy Darknet i Dark Web

- Należy też zauważyć, że Deep Web (Głęboka sieć) jest wszechogarniającym pojęciem, które obejmuje wszelkiego rodzaju treści, które nie są zwykle dostępne (albo ze względu na użycie niestardardowych DNS, jak Dark Internet lub podobne, nie są po prostu indeksowana i nie można ich znaleźć za pomocą zwykłej, nieskonfigurowanej przeglądarki), wyszukiwane, lub po prostu linki do tych stron są nieznane.
- Darknet jednak, zazwyczaj odnosi się do udostępniania plików na stronach (włączając w to metodę peer-to-peer), jak również do do przekaźników IRC chat, z których większość nie jest typowo indeksowana.
- Dark Internet najprawdopodobniej jest naturalną i nieuniknioną odpowiedzią na rządowe próby coraz większej kontroli, prowadzącej do zniszczenia tej wspaniałej idei.
- Można przewidzieć, że w najbliższych latach zauważymy gwałtowny wzrost i rozwój ciemnej strony Internetu.

Przydatne linki

- https://pl.wikipedia.org/wiki/Tor_(sie%C4%87_anonimowa)
- http://libertarianin.org/co-to-jest-darknet/