Základní informace o síti Tor

Technická zpráva FIT VUT v Brně

Libor Polčák

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Technická zpráva č. FIT-TR-2017-01
Fakulta informačních technologií, Vysoké učení technické v Brně

Last modified: 20. prosince 2017

Základní informace o síti Tor

Libor Polčák

Vysoké učení technické v Brně, email: ipolcak@fit.vutbr.cz

Abstrakt Síť Tor nabízí svým uživatelům anonymitu nad rámec poskytovaný běžně využívanými protokoly Internetu. Tato technická zpráva obsahuje základní seznámení s fungováním sítě Tor a možnostmi prolomení anonymity poskytované síti Tor. Tato práce poskytuje souhrn dříve publikovaných informací a je primárně určená čtenářům s nízkým, nebo žádným povědomím o fungování sítě Tor.

1 Úvod

Anonymizační sítě, jako je například síť Tor, umožňují uživatelům Internetu přistupovat ke službám, aniž by prozrazovali své identifikační údaje, jako je IP adresa. Síť Tor se sestává z tisíců uzlů[1] rozmístěných po celém světě. Tyto uzly umožňují klientům sítě Tor zasílat zprávy z odlišné IP adresy, než která je klientovi aktuálně přidělena.

Pokud se uživatel rozhodne přistupovat skrze síť Tor do Internetu, pak nejdříve musí sestavit okruh vedoucí přes několik uzlů sítě Tor. Informace od uživatele jsou předávány postupně mezi uzly sítě Tor až k tzv. výstupnímu uzlu. Výstupní uzel vytvoří běžné spojení TCP k serveru umístěnému v Internetu. Odpovědi od serveru jsou předávány po stejné cestě zpět směrem k uživateli. Server na Internetu nevidí v požadavcích IP adresu uživatele, ale IP adresu výstupního uzlu sítě Tor. Veškerá komunikace uvnitř sítě Tor je šifrovaná a uzly sítě Tor mimo výstupního neznají skutečný cíl komunikace. Pouze vstupní uzel sítě Tor zná IP adresu uživatele.

Cílem několikanásobného předávání zpráv v síti Tor je promíchání provozu všech uživatelů sítě Tor. Promícháním provozu dává síť Tor každému z uživatelů možnost popření autorství dat, protože není jednoduše zjistitelné, kdo která data vytvořil.

Projekt Tor vznikl v USA především za přispění vládních grantů a dodnes je částečně podporován z veřejných i soukromých darů[2].

Primárními uživateli sítě Tor jsou:

– osoby snažící se překonat restriktivní omezení k přístupu k zahraničním informacím, které platí v některých státech v různých koutech světa,

[1] 31.7.2017 bylo v síti Tor dostupných 6851 uzlů, aktuální statistiky jsou dostupné např. na http://torstatus.blutmagie.de.

[2] https://www.torproject.org/about/sponsors.html.en

– osoby snažící se o omezení sledování webovými servery např. za účelem cílení reklamy,
– oběti trestných činů a nemocné osoby, které se nechtějí o svém stavu svěřovat veřejně,
– novináři při vyhledávání informací do článků pro zajištění anonymity,
– zaměstnanci neziskových organizací při připojování k infrastruktuře své organizace aniž by dávali monitorovacím nástrojům vědět, že jsou zaměstnanci dané neziskové organizace,
– firmy monitorující svou konkurenci, aniž by dávali svému konkurentovi informaci o svých aktivitách na jejich webových stránkách,
– agenti a jiné složky úřadů činných v trestním řízení při vyšetřování a práci v terénu,
– zločinci pro výměnu informací, či páchání trestné činnosti.

Cílem této práce je vytvořit dokument poskytující základní informace o možnosti identifikace uživatelů používajících síť Tor. Hlavním smyslem této práce je poskytnutí základního přehledového materiálu pro vyšetřovatele pachatelů trestné činnosti související se sítí Tor. Práce však může také sloužit uživatelům sítě Tor, pro které obsahuje informace o ochraně poskytované sítí Tor.

Tato práce má následující členění. Sekce 2 stručně představuje protokoly rodiny TCP/IP používaných sítí Tor. Sekce 3 se zabývá uzly v síti Tor. Sekce 4 popisuje vytváření okruhu v síti Tor, jak při komunikaci do veřejného internetu, tak ke skrytým službám sítě Tor. Bezpečnostní model sítě Tor, jeho slabiny a riziková chování ukazuje sekce 5. Sekce 6 shrnuje možné scénáře detekce uživatelů používající síť Tor. Sekce 7 uzavírá tuto technickou zprávu.

2 Komunikační protokoly Internetu

Tato sekce obsahuje základní informace o protokolech používaných v prostředí Internetu, které jsou využívané i protokolem Tor.

2.1 Internetový protokol

Internetový protokol (IP) umožňuje předávání zpráv mezi koncovými stanicemi připojenými k Internetu. V současné době je využíván protokol verze 4 – IPv4 [15] a verze 6 – IPv6 [8]. Obě verze adresují koncové stanice adresou IP. V případě verze 4 je adresa IP 32 bitová, verze 6 používá 128 bitové adresy. Nicméně v důsledku vyčerpání adres IPv4 může v současné době sdílet více počítačů jednu, nebo i několik adres IPv4 (tzv. překlad adres, *network address translation* – NAT).

V případě komunikace mezi dvěma počítači připojenými k Internetu jsou jednotlivé zprávy přenášeny datagramy. Každý datagram obsahuje zdrojovou a cílovou adresu IP. Jednotlivé datagramy jsou směrovány Internetem na základě cílové adresy a doručeny cílovému uzlu. Cílový uzel pozná odesílatele datagramu podle zdrojové adresy.

Z uvedených informací tedy vyplývá, že libovolný uzel na cestě datagramu v rámci Internetu zná u každého datagramu jak adresu zdrojového uzlu, tak adresu cílového uzlu.

2.2 Protokol TCP

Transmission Control Protocol (TCP) [16] umožňuje spolehlivé přenášení proudu informaci mezi konkrétními aplikacemi bežícími na koncových stanicích. TCP segmentuje proud dat získaný od aplikace do částí přenášených datagramy IP. Přenos dat mezi koncovými stanicemi je úkolem IP.

TCP používá 16 bitová čísla portu pro adresování aplikací bežících na koncových stanicích. V každém ze segmentů TCP se přenáší jak číslo zdrojového portu, tak číslo cílového portu TCP.

Libovolný uzel na cestě v rámci Internetu vidí u každého datagramu IP obsahující segment TCP čtveřici zdrojová adresa IP, zdrojový port, cílová adresa IP, cílový port. Na základě těchto informací je možné často dohledat jak koncové stanice, tak běžící aplikace. Např. cílový port 80 je obvykle používán webovým serverem pro nešifrovaný přenos webových stránek.

2.3 Šifrování dat

TLS [9] (*Tranport Layer Security*) umožňuje šifrování dat přenášených v proudu TCP. Při ustanovení spojení si obě strany spojení mohou ověřit identitu druhé komunikující strany na základě certifikátů. V praxi však nejčastěji ověřuje identitu pouze klient.

Během vytváření spojení se využívá asymetrické kryptografie postavené na existenci soukromého a příslušného veřejného klíče. Veřejný klíč je součástí certifikátu, kterým prokazuje stanice svou identitu. Všechna data zašifrovaná veřejným klíčem mohou být dešifrovaná pouze párovým soukromým klíčem. Bez odpovídajícího soukromého klíče je dešifrování komunikace TLS velmi obtížné a obecně nerealizovatelné se současnou úrovni poznání.

3 Uzly sítě Tor

Síť Tor využívá stávající linky a, pokud je to možné, protokoly sítě Internet. Veškerá komunikace mezi jednotlivými prvky sítě probíhá za vyžití protokolů IP [8, 15], TCP [16] a TLS [9]. Síť Tor tedy tvoří virtuální síť postavenou nad Internetovou infrastrukturou, tzv. síť typu *overlay*.

Síť Tor se sestává z uzlů, prvků plnících konkrétní úlohy popsané níže. Software využívaný síti Tor je volně dostupný včetně zdrojového kódu[3]. V případě potřeby je tedy možné jednotlivé programy upravovat.

Uzly sítě Tor se dělí do následujících skupin:

[3] https://www.torproject.org/dist/tor-0.3.0.10.tar.gz

Směrovače (*relays, routers*) přeposílají data v rámci sítě Tor. Umožňují uživatelům sítě Tor vytváření okruhů. Některé z uzlů mohou mít následující význačné vlastnosti (jednu i více):

- **Výstupní uzly** (exit nodes) umožňují komunikaci ze sítě Tor do Internetu. Každý z výstupních uzlů může aplikovat specifickou politiku povolující jen některý provoz (např. omezení na úrovni portů TCP).
- **Stabilní uzly** (*stable*) jsou provozovány dlouhodobě.
- **Strážci** (*guards*) jsou dlouho stabilně běžící uzly. Ze strážců si typicky klienti vybírají počáteční uzly v okruhu v síti Tor.
- **Mosty** (*bridges*) [12] jsou speciální vstupní směrovače, které nejsou veřejně inzerované. Jsou využívané uživateli připojující se do sítě Tor v oblastech, kde jsou veřejně známé uzly Tor blokované.

Směrovače sítě Tor může provozovat kdokoliv, např. neziskové organizace zabývající se svobodou na Internetu, dobrovolníci, výzkumníci, ale i zpravodajské agentury.

Adresářové servery (*directory servers*) udržují seznam aktivních uzlů v síti Tor a jejich stav.

Uživatelské proxy (*onion proxies*) běží na počítačích uživatelů přistupujících do sítě Tor. Z adresářových serverů získávají aktuální informace o stavu sítě Tor, na základě kterých vytváří virtuální okruhy.

Skryté služby (*hidden services*) jsou servery dostupné jen ze sítě Tor. Tor poskytuje možnost anonymního vytvoření okruhu ke skrytým službám pomocí doménového jména s koncovkou *.onion*. Při komunikaci se skrytou službou nezná klient IP adresu skryté služby, ani skrytá služba IP adresu klienta.
Skrytých služeb existují desetitisíce [2]. I když existují legitimní služby jako je vyhledávač DuckDuckGo[4] a Facebook[5], často jde o nelegální činnost, jako je ovládání botnetů, databáze kradených čísel platebních karet, nelegální tržiště, gambling a jiné [2, 3]. Mezi skrytými službami jsou i webové stránky v češtině [2].

Uživatelské proxy přistupují do sítě Tor přes strážce, či mosty. Aplikace komunikují s uživatelskou proxy pomocí rozhraní *SOCKS* [19, 21]. Libovolná aplikace podporující toto rozhraní může komunikovat skrze Tor. Překlad doménových jmen zajišťuje výstupní uzel.

Jedním z nejobvyklejších využití Toru je prohlížení webových stránek. Jako prohlížeč je doporučený *Torbrowser*[6] – prohlížeč postavený nad zdrojovým kódem prohlížeče Firefox[7] s modifikacemi zaměřenými na zajištění anonymity.

Z předchozího textu vyplývá, že uzly v síti (kromě mostů) jsou veřejně známé. *Torstatus*[8] zobrazuje přehled aktuálně běžících uzlů, jejich stavu, adresy IP, země umístění a dalších parametrů. Informace o jednotlivých uzlech v síti je

[4] https://3g2upl4pq6kufc4m.onion
[5] https://facebookcorewwwi.onion
[6] https://www.torproject.org/projects/torbrowser.html.en
[7] https://www.mozilla.org/cs/firefox/
[8] http://torstatus.blutmagie.de/

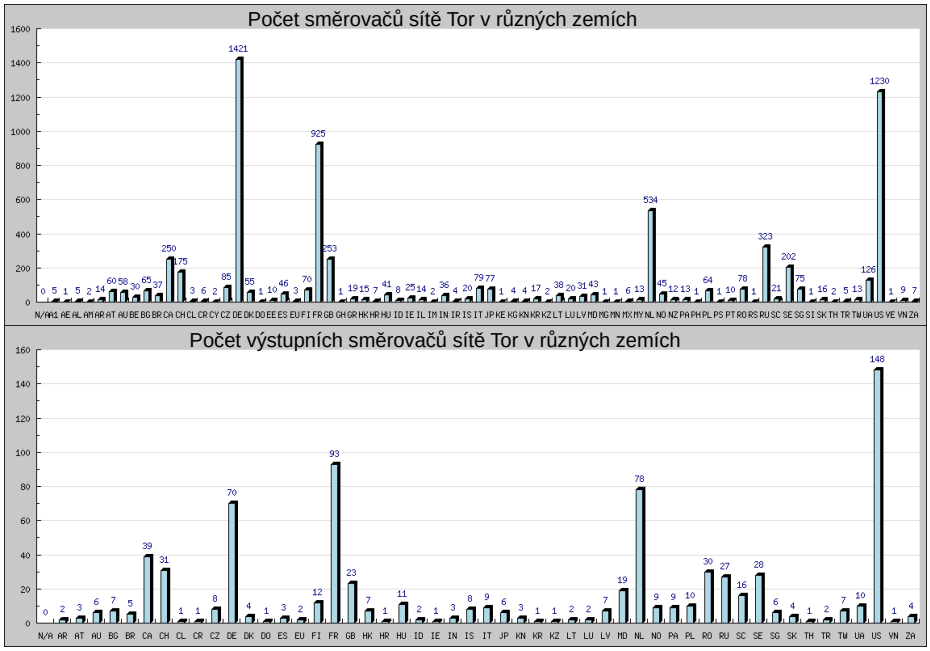
také možné získat ze služby Atlas[9], či Compass[10]. Historické informace nabízí služba Exonerator[11].

Z veřejně dostupných zdrojů je také možné získat přehled o rozmístění směrovačů sítě Tor (mimo mostů). Obrázek 1 ukazuje celosvětový přehled uzlů sítě Tor včetně stavu uzlů. Obrázek 1 byl vytvořen službou *Tormap*[12]. Mapováním uzlů v síti Tor se zabývají i další služby[13].

Obrázek 1. Rozmístění směrovačů sítě Tor ve světě. Různé barvy rozlišují role uzlů popsané výše, více informací je k nalezení na službě *Tormap*[12].

Pro lepší představu o počtu uzlů sítě Tor v jednotlivých zemích je možné využít službu *Metrics*[14], nebo *TorStatus*[15]. Obrázek 2 ukazuje počty směrovačů sítě Tor v různých zemích získaný ze služby *TorStatus*. Vrchní graf zobrazuje všechny směrovače, dolní graf jen výstupní směrovače sítě Tor. V době generování obrázků se v České republice nacházelo 85 směrovačů sítě Tor, osm z nich umožňovalo zasílání dat do veřejné sítě Internet.

[9] https://atlas.torproject.org
[10] https://compass.torproject.org/
[11] https://exonerator.torproject.org/
[12] https://tormap.void.gr/
[13] Např. https://fusiontables.googleusercontent.com/embedviz?q=select+col11+from+1y20sGGfeFToP4yIiCic5wuXaNS7VEXBfqa1YF8o&viz=MAP&h=false&lat=54.39465933303901&lng=27.20015753749999&t=1&z=5&l=col11&y=3&tmplt=3&hml=TWO_COL_LAT_LNG
[14] https://metrics.torproject.org/bubbles.html#country
[15] http://torstatus.blutmagie.de/network_detail.php



Obrázek 2. Rozmístění směrovačů sítě Tor podle zemí[15].

4 Stavba okruhu v síti Tor

Každý uzel sítě Tor, který může vystupovat v roli prostředníka na cestě síti Tor, si generuje dlouhodobý pár veřejného a soukromého *identifikačního klíče* sloužícího pro koordinaci činnosti sítě Tor. Pro autentizaci vůči klientům sítě Tor se používá pár veřejného a soukromého klíče; nový pár se generuje přibližně jednou týdně. Tento pár klíčů se používá během ustanovení spojení protokolem TLS [9]. Dočasné klíče použité protokolem TLS nejsou uchovávány.

Komunikace uvnitř sítě Tor probíhá pomocí buněk o pevné velikosti 512 B, či 514 B, v závislosti na použité verzi protokolu [11].

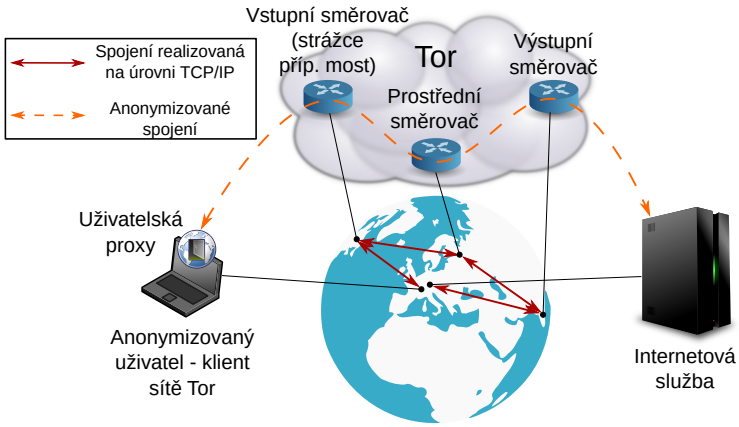
4.1 Vytvoření cesty sítí Tor

Před započetím komunikace skrze síť Tor si klient vybírá směrovače na cestě. Na cestě přitom nesmí být několik směrovačů, u kterých je podezření, že mohou být spravovány stejnou autoritou (na základě adresy směrovačů a dobrovolně sdělených informací). Ve výchozím stavu se volí cesta délky tři[16].

Při navazování spojení pak klient nejdříve ustanoví spojení s prvním směrovačem na cestě. Po ustanovení spojení požádá klient o prodloužení cesty na další

[16] https://www.torproject.org/docs/faq.html.en#ChoosePathLength

uzel a takto postupuje stejně, dokud se nedostane na požadovanou délku cesty. Obrázek 3 ukazuje příklad cesty skrze síť Tor do Internetu. Přestože ve skutečnosti komunikuje anonymizovaný uživatel s Internetovou službou, na úrovni protokolů TCP/IP se komunikace odehrává ve čtyřech různých spojeních.



Obrázek 3. Klient sítě Tor posílá data skrze několik uzlů rozmístěných různě ve světě.

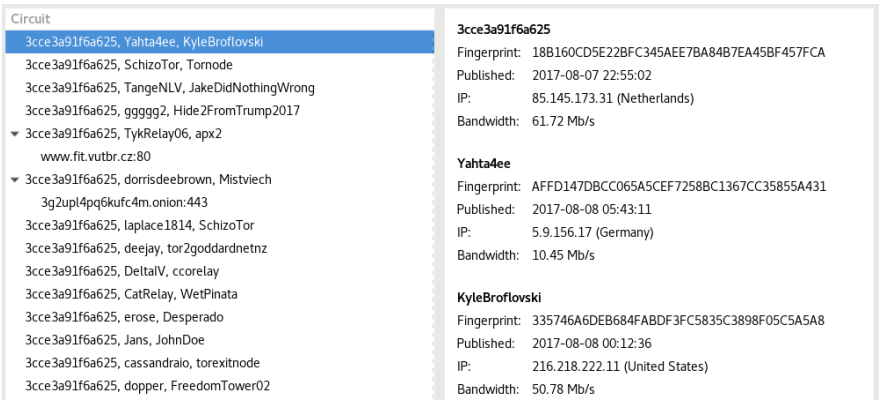
Data odesílaná uživatelskou proxy anonymizovaného uživatele určená pro Internetovou službu jsou několikanásobně šifrovaná: (1) klíčem používaným při komunikaci s výstupním směrovačem, (2) klíčem používaným při komunikaci s prostředním směrovačem a (3) klíčem používaným při komunikaci se vstupním směrovačem. Směrovače na cestě tedy nevidí obsah přenášené komunikace. Pouze výstupní směrovač je schopen dešifrovat data určená Internetové službě. Tato data však mohou být také šifrovaná.

Obrázek 4 zobrazuje výstup aplikace *Onion Circuits* běžící na počítači připojenému k Toru. V levé části okna jsou zobrazeny aktuálně otevřené okruhy z tohoto počítače. Na obrázku je vidět, kterými okruhy jsou přenášena data aktuálně otevřených spojení k `www.fit.vutbr.cz` a `https://3g2upl4pq6kufc4m.onion`. V pravé části okna jsou zobrazeny detaily k aktuálně vybranému okruhu v levé části.

Skryté služby

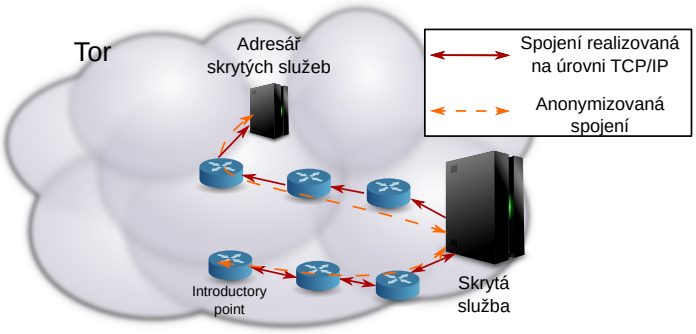
Jak již bylo zmíněno, Tor umožňuje vytvoření tzv. skrytých služeb – serverů, které je možné kontaktovat bez znalosti adresy IP, která u skrytých služeb není veřejná.

Při vytváření skryté služby vytvoří správce veřejný a soukromý klíč, který se používá při autentizaci skryté služby vůči návštěvníkům. Zároveň si skrytá služba



Obrázek 4. Na počítači připojeném k síti Tor, je možné přehledně zobrazit seznam aktuálně otevřených okruhů.

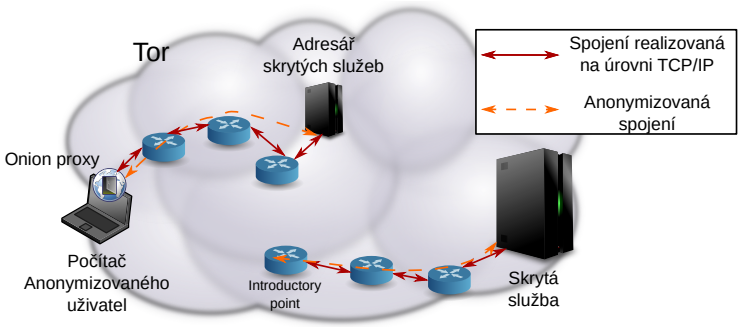
vytvoří okruhy k několika uzlům označovaným jako *introductory point*. Okruhy ponechává aktivní po nějaký čas. Informace o všech *introductory points* skrytá služba podepíše a publikuje v rámci adresářových serverů. Žádný z adresářových však nezná všechny skryté služby. Obrázek 5 ukazuje okruh vytvořený skrytou službou k jednomu z *introductory point*. Druhým (krátkodobým okruhem) skrytá službá publikuje informace o své přítomnosti v adresářových serverech.



Obrázek 5. Skrytá služba publikuje informace o svých *introductory points* v adresáři.

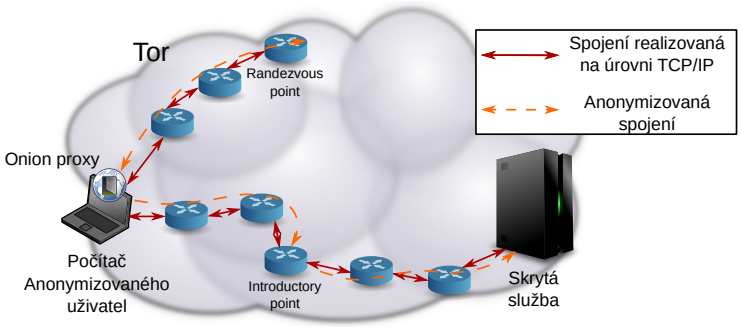
V případě, že se chce anonymizovaný uživatel připojit ke skryté službě musí se nějakým způsobem dozvědět o její existenci. Tuto informaci může získat od správce skryté služby, na webové službě běžící na Internetu nebo jiné skryté službě, či jakýmkoliv jiným způsobem. Pro zjištění aktuálních *introductory points*

skryté služby kontaktuje anonymizovaný uživatel adresářové služby Tor. Obrázek 6 ukazuje okruh vytvořený k adresářové službě a okruh mezi skrytou službou a jedním *introductory point* této služby.



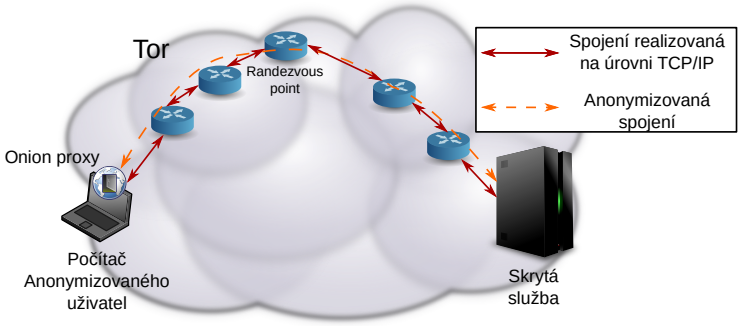
Obrázek 6. Anonymizovaný uživatel sítě Tor zjišťuje *introductory points* požadované skryté služby.

Dříve než počítač anonymizovaného uživatele sítě Tor kontaktuje vybraný *introductory point*, vybere si jeden ze směrovačů a požádá jej o roli prostředníka ve vytváření okruhu ke skryté službě, tzv. *randezvous point*. S tímto uzlem se také dohodne na tajné informaci potřebné pro úplné vytvoření okruhu. Následně počítač anonymizovaného uživatele sítě Tor předá tajnou informaci a požádá jej o předání skryté službě. Obrázek 7 zobrazuje vytvořenou část okruhu mezi anonymizovaným uživatelem a *randezvous point* a dočasně vytvořený okruh k *introductory point*, který je prostředníkem skryté služby.



Obrázek 7. Anonymizovaný uživatel sítě Tor vytvořil okruh k *randezvous point* a zasílá požadavek skryté službě.

Skrytá služba vytvoří anonymizovanou cestu k *randezvous point* a autentizuje se vůči uživateli sítě Tor. Vytvořeným okruhem skrze *randezvous point* poté probíhá vlastní komunikace mezi klientem a skrytou službou. Obrázek 8 zobrazuje výsledný okruh.



Obrázek 8. Komunikace mezi anonymním klientem a skrytou službou probíhá okruhem přes *randezvous point*.

5 Bezpečnostní model sítě Tor

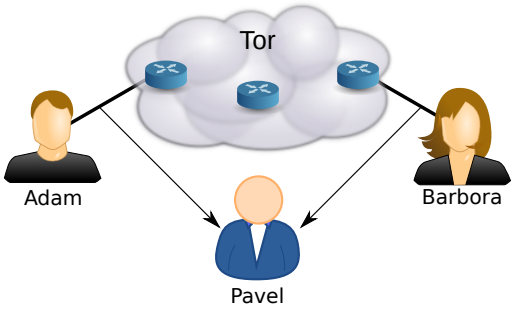
Tor poskytuje služby uživatelům po celém světě [12, 13]. Primárním smyslem použití jsou interaktivní protokoly jako je instantní přenos zpráv, nebo prohlížení webových stránek. Takže je nutný přenos dat s co nejnižším zpožděním při průchodu síti.

5.1 Možnosti lokálního pozorovatele sítě Tor

Bezpečnostní model sítě Tor chrání před pozorovateli schopnými monitorovat pouze část sítě [12, 13]. Uvažovaný pozorovatel může vytvářet, upravovat, mazat, či zpožďovat provoz, či dokonce provozovat vlastní uzly sítě Tor, nebo část uzlů kompromitovat.

Zvolený bezpečnostní model cíleně nechrání před pozorovateli dvou potenciálních komunikujících stran. Uvažujme následující příklad na obrázku 9. Adam komunikuje s Barborou přes síť Tor. Pozorovatel Pavel monitoruje provoz na linkách, kterými jsou připojeni Adam i Barbora k Internetu (a tudíž i k síti Tor).

Pavel může sledovat množství přijatých a odeslaných dat na obou linkách v čase. Při vhodné struktuře provozu je možné s určitou pravděpodobností prokázat, že Adam komunikoval s Barborou [5, 12, 17]. Kromě pasivního pozorování může Pavel část provozu zahazovat, či zdržovat a pozorovat vliv na přenos



Obrázek 9. Pavel monitoruje linky připojující Adama a Barboru k Internetu.

dat u druhého sledovaného. Adam i Barbora mohou pozorovateli ztížit situaci provozováním vlastního směrovače sítě Tor. V takovém případě by uživateli provozujícímu uzel sítě Tor skutečně patřila pouze část provozu protékající po jeho lince k Internetu.

Coufal [6] ve své diplomové práci navrhl a otestoval metodu pro korelaci odpovědí od webového serveru na vstupu a výstupu ze sítě Tor. Navržená metoda porovnává objem datových toků v časových oknech. Nejdříve je nutné nalézt vhodnou pozici okna, aby byl interpretovaný vzor v počtu přenášených buněk Toru za určitý čas na vstupu a výstupu sítě v korelaci. V rámci testování metody se ukázaly velmi dobré možnosti navržené metody.

Výše uvedené vlastnosti sítě Tor by bylo možné využít policejními, bezpečnostními, či zpravodajskými složkami v roli Pavla při pozorování dvou uživatelů, nebo uživatele a služby, pokud jsou oba připojeni k Internetu v České republice. Pozorovatel však musí provoz sledovat v okamžiku aktivní komunikace. Pozorování nelze uplatnit zpětně.

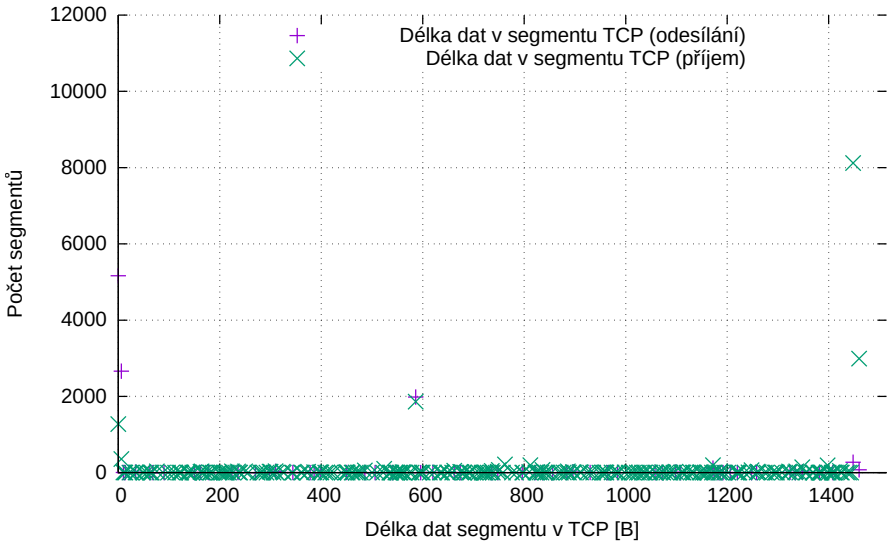
5.2 Detekce komunikace v síti Tor

Bezpečnostní model sítě Tor se nesnaží zastírat, že konkrétní uživatel komunikuje v rámci sítě Tor. Jak již bylo zmíněno, síť Tor používá pro svou komunikaci buňky pevné velikosti. Toho je možné využít pro analýzu síťového provozu bez znalosti dešifrované komunikace na základě četnosti délek přenášených paketů. Pakety přenášející jednu buňku Toru mají velikost 586 B [18].

Protože se tyto buňky přenášejí protokolem TCP, může se v jednom segmentu objevit více zpráv, nebo i jen část zprávy. V běžném nastavení uzly sítě Tor přenos buňky nijak nemaskují a provoz sítě Tor se vyznačuje specifickou charakteristikou zobrazenou na obrázku 10.

Na obrázku lze vidět tři nejpočetněji zastoupené délky segmentů:

- 0 B: Potvrzovací segmenty TCP, nenesou žádná data.
- 586 B: Odpovídá hodnotě typické pro Tor [18].



Obrázek 10. Příklad histogramu rozložení velikosti segmentů TCP při komunikaci v síti Tor.

– 1448 B, respektive 1460 B: Maximální velikost segmentu, přesná velikost závisí na volitelných parametrech v hlavičkách TCP a IP, které mohou být ovlivněny operačním systémem, či jeho nastavením. Pro IPv6 by byly hodnoty o 20 B nižší v důsledku větší hlavičky IPv6.

Jako obranu před výše popsanou analýzou délek paketů je možné nasadit transformátory charakteristik síťového provozu (*pluggable transports*) [18]. Ve výchozím stavu nejsou transformátory aktivní. Aby byly transformátory účinné, je nutné jejich nasazení na obou stranách komunikace. Vzhledem k tomu, že transformátory nejsou obvykle nasazovány na směrovače sítě Tor, nasazení na klientovi by chránilo pouze jeden směr komunikace. Transformátory charakteristik síťového provozu však bývají nasazené na mostech[17].

5.3 Neopatrné chování uživatelů

Někteří uživatelé si myslí, že použití sítě Tor je dostačující pro získání anonymity v prostředí Internetu. Pokud si nebudou dávat pozor, mohou se prozradit svým chováním. Projekt Tor dává uživatelům některé rady, jak se při používání Toru chovat[18]. Uživatele, kteří uvedené rady porušují je možné vystopovat.

[17] https://www.torproject.org/docs/bridges.html.en
[18] https://www.torproject.org/download/download-easy.html.en

Jak již bylo zmíněno, při prohlížení webu je doporučeno využívat prohlížeč *Torbrowser*. Pokud uživatel použije jiný prohlížeč, může navštívený server aplikovat některou z metod identifikace prohlížeče, tzv. *browser fingerprinting* [4, 14, 20, 22]. *Panopticlick*[19] obsahuje databázi více než 500 000 dobrovolně poskytnutých testu prohlížečů zaměřených na obsah hlaviček HTTP a informací dostupných pomocí JavaScriptu jako je identifikační řetězec prohlížeče, velikost obrazovky, preferovaný jazyk, časová zóna a nainstalovaná písma. *AmIUnique*[20] nabízí obdobný test, ke kterému navíc přidává testování generování obrázku na koncovém počítači, který je ovlivněný grafickou kartou a nainstalovanými písmy.

Pluginy v prohlížeči, jako je Flash, RealPlayer, Quicktime, umožňují zjistit skutečnou adresu IP počítače. Uživatelé používající tyto pluginy je možné deanonymizovat pomocí skriptů vložených Internetovým serverem, nebo výstupním uzlem sítě Tor (viz níže).

Při použití nešifrovaného protokolu, jako je HTTP, je možné na cestě od výstupního uzlu sítě Tor k Internetovému serveru pozorovat nešifrovaný obsah uživatelských dat. V takovém případě je možné zjistit například uživatelské jméno při přihlašování. Další možností je upravení odpovědi. Odpověď může upravovat také kompromitovaný výstupní uzel sítě Tor. Do odpovědi je možné vložit například skript zjišťující skutečnou adresu uživatele (viz výše) nebo jinak přizpůsobit odpověď. Např. je možné upravit obsah stahovaných souborů, či využít chování prohlížeče, který automaticky stahuje soubory[21].

Některé aplikační protokoly, jako je např. BitTorrent přenášejí informace o IP adrese. Takováto adresa IP může být přenesena skrze Tor, čímž dochází k deanonymizaci uživatele[22].

Uživatel může mít nakonfigurovaný počítač tak, že prohlížeč sice komunikuje skrze Tor, ale ostatní aplikace Tor nevyužívají. Pokud uživatel stáhne přes Tor nějaký dokument, otevře jej jinou aplikací a tento dokument obsahuje externí obsah a aplikace jej stáhne mimo síť Tor, uživatel může být deanonymizován.

5.4 Další zdroje informací

Základy sítě Tor jsou popsané ve vědeckém článku [13], který byl později aktualizován [12]. Tento článek obsahuje podrobnější informace o bezpečnostním modelu sítě Tor, o cílech projektu, návrhu sítě a mechanismech, na jejichž základě síť funguje. Specifikační dokumenty použitých protokolů jsou volně dostupné [1, 10, 11].

Problematikou sítě Tor, i anonymitou na Internetu, se zabývá velké množství vědeckých publikací. Stránky *Free Haven*[23] obsahují databázi přibližně 450 vědeckých článků věnující se této tématice, více než 50 z nich obsahuje ve svém názvu slovo Tor.

[19] https://panopticlick.eff.org/
[20] https://AmIUnique.org/
[21] http://gynvael.coldwind.pl/?id=55
[22] https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea
[23] https://www.freehaven.net/anonbib/topic.html

6 Shrnutí možností detekce uživatelů sítě Tor

Tato sekce popisuje vybrané činnosti, které se dotýkají uživatelů počítačových sítí v kontextu využití sítě Tor. U každého případu je popsaná ochrana poskytovaná síti Tor a možnosti jejího prolomení.

6.1 Identifikace uživatele sítě Tor

Např. při vyšetřování bezpečnostních incidentů může být úkolem identifikace útočníka. Pokud je útok spáchán za využití sítě Tor, je potřeba identifikovat konkrétního uživatele sítě. Tor maskuje adresy IP připojených uživatelů za adresy IP výstupních uzlů sítě Tor. V jeden okamžik může jeden uživatel využívat libovolné množství dostupných výstupních uzlů a každý uživatel výstupní uzly v čase mění.

Obecně uživatele sítě Tor není snadné identifikovat, pokud nemůžeme sledovat všechen provoz v síti Tor, tedy monitorovat většinu Internetu. Např. výše popsaný *Torbrowser* se snaží, aby metadata uživatelů vypadala uniformě.

Při identifikaci je možné využít neopatrnosti uživatelů popsané v podsekci 5.3. Pro vyšetřování přístupů uskutečněných v minulosti je však potřeba mít k dispozici dostatek informací, např. pro identifikaci prohlížeče. Často však dostatek informací k dispozici není. Následující výpis ukazuje příklad záznamu ve formátu *Combined Log Format* používaným webovými servery:

```
1.2.3.4 - frank [01/Aug/2017:08:46:46 +0200] "GET /myadmin/
    scripts/setup.php HTTP/1.1 HTTP/1.1" 403 209 "http://www.
    example.com/" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit
    /537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari
    /537.36"
```

V záznamu je uloženo:

- adresa IP přistupující ke konkrétní stránce: *1.2.3.4*,
- jméno autentizovaného uživatele (pokud proběhla autentizace): *frank*,
- čas přístupu: *01/Aug/2017:08:46:46 +0200*,
- požadovaná stránka: `/myadmin/scripts/setup.php`,
- typ požadavku a verze protokolu: *GET HTTP/1.1 HTTP/1.1*,
- návratový kód: *403*,
- velikost dat odeslaných v odpovědi: *2*09,
- předešlá navštívená stránka: `http://www.example.com/`,
- identifikátor prohlížeče poskytnutý samotným prohlížečem – tzv. *user agent string* (UAS): *Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36*

Uložené informace nejsou dostačující k identifikaci skutečného uživatele. Uchovaná adresa IP pro přístupy skrze Tor je adresa použitého výstupního uzlu. Vodítkem by mohl být UAS, který je však v případě použití *Torbrowseru* unifikovaný a mění se pouze verze, např. *Mozilla/5.0 (Windows NT 6.1; rv:52.0)*

Gecko/20100101 Firefox/52.0. I při použití jiného prohlížeče obvykle není UAS unikátní.

V případě identifikace uživatele v reálném čase, mohou být využity metody korelace dat na vstupu a výstupu sítě Tor, v případě, že existuje podezřelý uživatel. Metody korelace popisuje podsekce 5.1.

6.2 Odposlech všech dat konkrétního uživatele

V případě zákonných odposlechů [23] je soudně povoleno odposlouchávat provoz konkrétního uživatele. Pokud tento uživatel využívá síť Tor, jsou veškerá data uživatele vyměňovaná přes síť Tor několikanásobně šifrovaná (viz podsekci 4.1). Navíc data uživatele opouštějí síť Tor na různých výstupních uzlech rozmístěných po celém světě.

Pro odposlech obsahu všech dat uživatele sítě Tor by tedy bylo nutné:

1. Odposlouchávat všechny výstupní uzly sítě Tor. V současné době je však provozováno více než 750 uzlů umožňujících přístup ze sítě Tor do veřejného Internetu[24].
2. V zachyceném provozu identifikovat provoz sledovaného uživatele a odlišit jej od ostatního provozu, viz podsekci 6.1.

6.3 Detekce přístupu ze sítě Tor

Služby provozované v rámci Internetu mohou detekovat skutečnost, že uživatel používá k přístupu síť Tor na základě adresy IP přicházejícího požadavku.

Síť Tor před veřejným Internetem nijak neskrývá skutečnost, že provoz pochází ze sítě Tor. Naopak existuje několik služeb umožňujících určit zda adresa IP patří do sítě Tor, včetně historických informací. Přehled služeb je uveden v sekci 3.

6.4 Detekce zapojení stroje do sítě Tor

Adresy IP uzlů poskytující služby ostatním členům sítě Tor jsou veřejně přístupné s výjimkou skrytých služeb a mostů, viz sekci 3.

I když většina uživatelů neprovozuje vlastní směrovač sítě Tor, při monitorování provozu je možné detekovat, že konkrétní stroj komunikuje se vstupním uzlem sítě Tor uvedeným ve veřejném seznamu. Alternativně je možné detekovat provoz sítě Tor na základě charakteristických délek paketů, viz podsekci 5.2. Transformátory charakteristik síťového provozu (*pluggable transports*) [18] umožňují dynamicky měnit délky paketů, tyto transformátory však nejsou ve výchozím stavu aktivní.

[24] https://metrics.torproject.org/relayflags.html

7 Závěr

Tato technická zpráva popisuje fungování anonymizační sítě Tor, zvolený bezpečnostní model a jeho slabiny. Cílem této technické zprávy je podat základní informace o síti Tor čtenáři s žádnými, nebo malými informacemi o síti Tor. Technická zpráva může sloužit také jako rozcestník k dalším zdrojům dostupných na webu i ve vědeckých publikacích.

Tato technická zpráva navazuje na naši dřívější technickou zprávu [7], která obsahuje detailnější informace o technických podrobnostech souvisejících s anonymizační síti Tor.

Literatura

[1] TC: A Tor control protocol (Version 1). [online], [cit. 2017-08-10].
URL https://gitweb.torproject.org/torspec.git/tree/control-spec.txt

[2] Biryukov, A.; Pustogarov, I.; Thill, F.; aj.: Content and Popularity Analysis of Tor Hidden Services. In *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2014, ISSN 1545-0678, s. 188–193.

[3] Biryukov, A.; Pustogarov, I.; Weinmann, R.-P.: Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. In *2013 IEEE Symposium on Security and Privacy*, 2013, ISSN 1081-6011, s. 80–94.

[4] Cao, Y.; Li, S.; Wijmans, E.: (Cross-)Browser Fingerprinting via OS and Hardware Level Features. In *Proceedings of Network & Distributed System Security Symposium (NDSS)*, 2017.

[5] Chakravarty, S.; Barbera, M. V.; Portokalidis, G.; aj.: On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records. In *Proceedings of the 15th International Conference on Passive and Active Measurement - Volume 8362*, PAM 2014, New York, NY, USA: Springer-Verlag New York, Inc., 2014, ISBN 978-3-319-04917-5, s. 247–257.

[6] Coufal, Z.: Korelace dat na vstupu a výstupu sítě Tor. 2014, diplomová práce, Vysoké učení technické v Brně.

[7] Coufal, Z.; Polčák, L.: Anonymizační síť Tor. Technická zpráva, 2014.
URL http://www.fit.vutbr.cz/research/view_pub.php?id=10626

[8] Deering, S.; Hinden, R.: *Internet Protocol, Version 6 (IPv6) Specification.* IETF, 2017, RFC 8200 (Internet Standard).

[9] Dierks, T.; Rescorla, E.: *The Transport Layer Security (TLS) Protocol Version 1.2.* IETF, 2008, RFC 5246 (Proposed Standard).

[10] Dingledine, R.; Mathewson, N.: Tor Directory Protocol Specification. [online], [cit. 2017-08-10].
URL
https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

[11] Dingledine, R.; Mathewson, N.: Tor Protocol Specification. [online], [cit. 2017-08-04].
URL
https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

[12] Dingledine, R.; Mathewson, N.; Murdoch, S.; aj.: Tor: The Second-Generation Onion Router (2014 DRAFT v1), 2014.
URL http://www.cl.cam.ac.uk/~sjm217/papers/tor14design.pdf

[13] Dingledine, R.; Mathewson, N.; Syverson, P.: Tor: the second-generation onion router. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13*, SSYM'04, Berkeley, CA, USA: USENIX Association, 2004.

[14] Eckersley, P.: How Unique Is Your Web Browser? In *Privacy Enhancing Technologies*, *Lecture Notes in Computer Science*, ročník 6205, Springer Berlin Heidelberg, DE, 2010, ISBN 978-3-642-14526-1, s. 1–18.

[15] Information Sciences Institute University of Southern California, IETF: *Internet Protocol*. 1981, RFC 791 (Internet Standard).

[16] Information Sciences Institute University of Southern California, IETF: *Transmission Control Protocol*. 1981, RFC 793 (Internet Standard).

[17] Johnson, A.; Wacek, C.; Jansen, R.; aj.: Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer; Communications Security*, New York, NY, USA: ACM, 2013, ISBN 978-1-4503-2477-9, s. 337–348.

[18] Kadianakis, G.: Packet Size Pluggable Transport and Traffic Morphing. Technická Zpráva 2012-03-004, The Tor Project, 2012.
URL https://research.torproject.org/techreports/morpher-2012-03-13.pdf

[19] Koblas, D.; Koblas, M. R.: Socks. In *Proceedings of the UNIX Security III Symposium*, 1992, s. 77–83.

[20] Laperdrix, P.; Rudametkin, W.; Baudry, B.: Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints. In *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, s. 878–894.

[21] Leech, M.; Ganis, M.; Lee, Y.; aj.: SOCKS Protocol Version 5. 1996, rFC 1928 (Proposed Standard).

[22] Mowery, K.; Shacham, H.: Pixel Perfect: Fingerprinting Canvas in HTML5. In *Proceedings of W2SP*, 2012.

[23] Právní řád České republiky: Zákon č. 127/2005 Sb. ve znění pozdějších předpisů (*Zákon o elektronických komunikacích*) doplněný o vyhlášku č. 336/2005 Sb. (*Vyhláška o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv*).