Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: Informační studia a knihovnictví

Studijní obor: Informační studia a knihovnictví

Bakalářská práce

Pavel Schamberger

Anonymita v prostředí internetu

Anonymity in the Internet Environment

Praha, 2014

Vedoucí práce: Mgr. Vít Šisler, Ph.D.

Rád bych poděkoval vedoucímu této bakalářské práce Mgr. Vítu Šislerovi, PhD. za velikou ochotu a trpělivost při řešení všech problémů a v neposlední řadě také za velmi podnětné připomínky.

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, že jsem řádně citoval všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 30. července 2014 .....

podpis studenta

Abstrakt

Předložená bakalářská práce se zabývá současným stavem anonymity v prostředí internetu a jejím historickým vývojem. Teoretickou část zakončuje srovnání anonymity a identity v internetovém prostředí, doplněné o motivaci samotných uživatelů k využívání reálné identity na straně jedné a anonymity na straně druhé. Dále práce analyzuje v současné době používané identifikační technologie v porovnání s nástroji pro zachování si anonymity na internetu.

Klíčová slova

anonymita online, anonymita, identita, soukromí, internet, web

Abstract

This bachelor thesis deals with the current state of anonymity in the Internet environment and its historical development. The theoretical part is topped with the comparsion of anonymity and identity in the online environment, complemented by the users themselves showing theirs motivation to use real identity on the one hand and anonymity on the other. Further analyzes currently used identification technology compared with the tools for maintaining the anonymity on the Internet.

Keywords

anonymity online, anonymity, identity, privacy, internet, web,

Obsah

1 Úvod

Anonymita v prostředí internetu je aktuální, často diskutované téma. Na rozdíl od reálného světa si většinová populace často ani neuvědomuje různé technologie sloužící k identifikaci osob ve spojení s moderními technologiemi s důrazem na internetovou síť.

Cílem této bakalářské práce je zmapovat vývoj anonymity v prostředí internetu od jeho masového rozšíření do současnosti (90. léta 20. století - 2014) se zaměřením na postupný nárůst služeb a technologií pracujících s reálnou identitou uživatelů a s tím spojený úbytek anonymity. Tento virtuální prostor není zdaleka tak anonymní, jak by se na první pohled mohlo zdát, a zjednodušeně řečeno již nestačí pouze vystupovat pod pseudonymem z důvodu, že existuje mnoho technologií sloužících k identifikaci uživatelů na straně jedné – zároveň existuje i celá řada nástrojů k anonymizaci v prostředí internetu na straně druhé.

K výběru tématu mě vedl osobní zájem o tuto problematiku a debata, která se o ní aktuálně vede. Tato debata je dále částečně spojená s otázkou soukromí na internetu obecně. Virtuální prostor prošel napříč svojí historií bouřlivým vývojem a spolu s jeho masovým rozšířením se objevuje neúprosný trend směřující k identifikaci uživatelů.

Právě historickým vývojem, anonymitou obecně a porovnáním anonymního působení a vystupování pod reálnou identitou se zabývá tato práce v první, teoretické části. V úvodu první části je definována samotná anonymita v prostředí internetu. Následuje popis historického vývoje spolu se souvislostmi, které jsou důležité pro navazující části práce. Teoretickou část zakončuje srovnání anonymity a identity v internetovém prostředí doplněné o motivaci samotných uživatelů k využívání reálné identity na straně jedné a anonymity na straně druhé.

V druhé, praktické části je cílem analyzovat a poskytnout ucelený přehled identifikačních technologií, které jsou v současnosti využívány. Tuto část následuje analýza nástrojů primárně sloužících k protichůdné snaze – ke snaze o

vzdorování uvedenému trendu a o používání internetu v anonymním režimu. Tyto nástroje fungují na odlišných principech a jejich použití je často vhodné jen k určitým účelům a pro určitou cílovou skupinu. Součástí analýzy je také jejich srovnání s výčtem jejich předností a nedostatků.

Úvod praktické části popisuje technologie sloužící k identifikaci uživatelů a popisuje jejich fungování. Na úvod navazuje rozsáhlý přehled technologií dopomáhajících k větší míře anonymity od doplňků webových prohlížečů přes speciální software až po robustní linuxové distribuce. V této části je velký důraz kladen na program Tor, který je v současnosti velice oblíbený a zároveň obecně uznávaný jako jedno z nejlepších řešení pro zachování anonymity na internetu. Mimoto také tvoří základ (nebo důležitou součást) dalších významných projektů, které mají za cíl skrytí reálné identity uživatele.

Vlastní práce má rozsah 43 normostran a veškeré bibliografické záznamy jsou zpracovány dle citační normy ISO 690:2011.

2 Vývoj anonymity v prostředí internetu

2.1 Definice anonymity

Pojem anonymita vznikl z řeckého slova *anonymia* znamenajícího beze jména či bezejmenný. Ačkoli se může zdát, že se jedná o něco nového, anonymita nás provází napříč historií. Mnoho autorů v minulosti publikovalo buď zcela anonymně nebo pod pseudonymem. Lze říci, že důvody pro využití anonymity zůstávají stejné - strach z represe, nepochopení nebo jen pokus odprostit se od vnějších vlivů směrem k větší tvůrčí svobodě. S příchodem informačních technologií a jejich neustálým zdokonalování se lidem po celém světě dostává do ruky nástroj pro vyjádření vlastních myšlenek a názorů, který může představovat podobně přelomový vynález, jakým byl knihtisk. Se snižující se náročností sebevyjádření s možností oslovit velké publikum ale prudce klesá šance zachování anonymity, která, v případě nepodniknutí veskrze technických opatření, je v prostředí dnešního internetu v podstatě nulová.

Širší definice anonymity aplikovatelná jak na reálný tak i virtuální svět od Garyho Marxe (Marx 1999) předpokládá k dosažení anonymity neznalost ani jedné ze sedmi dimenzí identifikačních informací. Tyto dimenze jsou: jméno osoby, lokace, pseudonym spojitelný s reálným jménem nebo lokací, pseudonym prozrazující jiné informace, odhalující vzorce chování, členství v některé sociální skupině nebo informace, předmět či dovednost naznačující osobní charakteristiky. Těchto sedm dimenzí by se dále dalo zařadit do takzvané sociální anonymity, kterou spolu s technickou anonymitou uvádí Hayne a Rice (Hayne 1997), kteří ve své práci na základě jeho písemného projevu zkoumají identifikovatelnost autora a efektivitu technické anonymity.

Andreas Pfitzmann (Pfitzmann 2001) v průběhu let připravil terminologii zaměřenou na anonymitu, identitu, pseudonymitu a další aspekty kontextu informačních technologií. Cílem bylo tyto pojmy v rámci svých definic od sebe odlišit. V rámci definice anonymity zmiňuje množinu anonymity, tedy množinu subjektů, které působí navenek totožně a nejsou od sebe jednotlivě rozpoznatelné: „Anonymita subjektu znamená, že není identifikovatelný v rámci množiny subjektů, množiny anonymity.“ Množina anonymity je velice důležitý prvek v

rámci všech anonymizačních nástrojů a zjednodušeně se dá prohlásit, že se vzrůstající velikostí této množiny vzrůstá pomyslná anonymita subjektu. Tvrzení, že anonymita potřebuje společnost dalších subjektů, ilustruje příklad pomyslného dokonalého anonymizačního nástroje. Ten může po technické stránce bezchybně fungovat, pokud jej ale používá úzký okruh lidí, nebo pouze samotný jedinec, ravděpodobnost, že je to právě on, je vždy stoprocentní.

I to může být jeden z důvodů, proč některé státy podporují projekty zaměřené na anonymitu v prostředí internetu, i když by se to na první pohled mohlo zdát jako protichůdná snaha identifikaci uživatelů (Tor Project 2014). Bezpečnostní složky tyto nástroje samy využívají. Například americké námořnictvo v minulosti stálo u zrodu konceptu Onion Routingu (Reed 2006), na kterém je mimo jiné založen program Tor. Vzhledem k jeho využívání v úzkém okruhu lidí z jedné organizace ale nesloužil a nemohl sloužit dle představ o anonymizaci uživatelů a okolí tak mohlo snadno poznat, odkud uživatel pochází.

2.2 Vývoj anonymity v prostředí internetu

Problematiku anonymity v prostředí internetu je nutné vnímat v historických souvislostech a s ohledem na její vývoj. První zmínka o lidské interakci skrze síť se datuje do roku 1962, kdy J. C. R. Licklider z amerického MIT publikoval svůj koncept *Galactic Network* (Licklider 1962), předzvěst následujícího vývoje. Později v tom samém roce se Licklider stal vedoucím výzkumné skupiny ARPA (The Advanced Research Projects Agency), která v roce 1971 změní název na DARPA (The Defense Advanced Research Projects Agency), pod kterým působí dodnes. Během let připravila tato skupina koncept a specifikace projektu ARPANET, který v roce 1969 dosáhl milníku čtyř navzájem propojených počítačů. Pro tyto potřeby vznikl nejprve Network Control Protocol (NCP), který se choval spíše jako ovladač zařízení, a poté konečně vznikl Transmission Control Protocol/Internet Protocol (TCP/IP), který je využíván dodnes.

Při tvorbě TCP protokolu měli jeho tvůrci (Leiner 2009), Robert E. Kahn a Vinton Cerf na paměti jeho spolehlivost, otevřenost a neutralitu. I díky těmto vlastnostem pravděpodobně přetrval do dnešních dnů (i když s různými modifikacemi).

Prvotní problémy se ztrátami paketů vedli k rozštěpení TCP na dva protokoly - TCP a IP. Paket jak je v informatice označován blok přenášených dat se skládá ze dvou částí. Hlavičky, která obsahuje řídící data, na základě kterých je paket doručen a uživatelská data, tedy samotný obsah. Zatímco TCP se stará o samotný transport paketů, protokol IP zajišťuje jejich správné adresování.

Fungování tohoto protokolu lze přirovnat k pošťákovi, který pouze přenáší data mezi dvěma body a jejich výslednou interpretaci nechává na koncových aplikacích. Tento minimalistický design není náhodou. Díky odsunutí veškeré komplexnosti na okraj sítě, tedy jednotlivých aplikacím, je možné provozovat na síti mnoho rozličných služeb. Pokud je tedy nutná identifikace uživatele, je zároveň nutná externí identifikační technologie. Tento princip pojmenovali výzkumníci Jerome Saltzer, David Clarke a David Reed jako *end-to-end principle* (Saltzer 1984). Ten je považován za jeden z důvodů úspěchu internetu a jeho masivního rozšíření.

Poté začaly vznikat technologie, které jsou s internetovým prostředím provázané dodnes – File Transfer Protocol (FTP), Domain Name System (DNS), ale i takové, které již neexistují (respektive jejichž využívání je na ústupu). Takovou technologií je například USENET, který umožňuje komunikaci v rámci globálních skupin v dobách vytáčeného připojení, tedy určitý vývojový krok směrem k dnešnímu stavu, kdy je internet v podstatě všudypřítomný a komunikace skrze něj okamžitá.

K zásadnímu vývoji došlo až na přelomu 80. a 90. let 20. století, kdy Tim Berners-Lee vynalezl a představil (Berners-Lee 1989) světu World Wide Web spolu s hypertextovým přenosovým protokolem HTTP, skrze který v roce 1990 úspěšně navázal spojení mezi klientem a serverem v rámci internetu. Po tomto mezníku dochází k rychlému vývoji a v roce 1994 je již 11 milionů amerických domácností vybaveno pro jízdu na informační superdálnici (Kohut 1994). Okolo roku 1996 je možné mluvit o masovém rozšíření internetu do každodenního života, v této době převážně na území Spojených států amerických. Ruku v ruce s tímto vývojem dochází ke vzniku programů a služeb, které jsou dnes již

neodmyslitelně spjaty s prostředím internetu jako jsou vyhledávače Yahoo, Google či prohlížeč Internet Explorer.

V historickém vývoji je také důležité zmínit společnost Netscape Communications, která se mimo svůj ve své době úspěšný webový prohlížeč Netscape Navigator nesmazatelně zapsala do historie díky svému zaměstnanci Lou Montullim. Právě on vymyslel a představil koncept *HTTP cookies*, tedy mechanismu pro opětovnou identifikaci zařízení při návratu na webovou stránku (Kristol 2000). Tím se bude tato práce vzhledem k jeho citlivé povaze z pohledu soukromí (respektive anonymity) zabývat později.

V dnešní době se o internetu mluví ve spojitosti s jeho všudypřítomností, což minimálně ve vyspělejších částech světa potvrzují čísla 2,4 miliardy připojených uživatelů – tedy 34% penetrace skrze obyvatelstvo a 566% nárůst v počtu uživatelů od roku 2000 (Internet World Stats 2014).

2.2.1 Anonymita versus identita

Obrázek 1 Na Internetu nikdo neví, že jsi pes (Steiner 1993)

„Na Internetu nikdo neví, že jsi pes," (v originále „*On the Internet, nobody knows you're a dog,*" (Steiner 1993)), je známým příslovím, které bylo otištěno jako

komiks v roce 1993 v magazínu New Yorker. Toto přísloví se stalo ikonickým ve vztahu k anonymitě na internetu. Přestože je i po více než 20 letech stále používáno, už nereflektuje (a ani nemůže) skutečnou situaci, která se podstatně změnila.

Po masovém rozšíření a přechodu z výzkumného projektu do komerčního prostředí se Internet stává čím dál tím významnější součástí ekonomik jednotlivých států. Zformovala se poptávka po technologiích identifikujících jednotlivé uživatele, která existuje převážně ze dvou důvodů. Prvním a primárním důvodem je pochopitelně marketing ve snaze o lepší personifikaci a robustní obchodní model reklam na webu obecně. Nejspíš i díky známým případům podvodů s kreditními kartami a bankovními převody na přelomu tisíciletí se poškozené instituce začaly o podobné identifikační technologie zajímat. Začaly tyto pokusy včas detekovat, na základě nespárování identifikačních informací o uživatelském zařízení. Celá tato oblast nazývaná *fraud detection* je mnohem širší, s potřebou indentifikace uživatele je ale spojena od začátku. Toto lze označit za druhý hlavní důvod formování poptávky po technologiích identifikujících konkrétní uživatele vycházející ze soukromého sektoru.

Lze ale najít i další důvody, které více reflektují současné tendence o získání kontroly nad internetem ze strany státních správ po celém světě. Tyto správy si již uvědomily potenciál, který v sobě internet skrývá. Lidé, znepokojení tímto vývojem, často s mírnou nadsázkou mluví o takzvaných *Čtyřech jezdcích Infokalypsy* (Assange 2012), v jejichž jméně dochází k regulacím tohoto prostoru. Tito jezdci ztělesňují čtyři velké strašáky současného internetu. Jmenovitě se jedná o terorismus, dětskou pornografii, prodej drog a praní špinavých peněz. Příkladem boje s těmito „jezdci“ může být internetový filtr zavedený ve Velké Británii na konci roku 2013, jehož zavedení bylo obhajováno snahou o ochranu dětí před příliš brzkou sexualizací (Davides 2010) pomocí metody Opt-In. Hlavním problémem, se kterým se doteď možnost Opt-In potýká, je bohužel i blokování falešně detekovaného závadného obsahu, kterým mohou být například komunitní stránky pro homosexuály, stránky obsahující informace o pohlavních chorobách a podobně (Ward 2014).

Lawrence Lessig uvádí ve své knize Code: „Neviditelný muž se nebojí státu, protože ví, že jeho povaha jej staví mimo jeho dosah.“ Tedy pokud nevíte, o koho se jedná, kde je a co dělá, nemůžete jej regulovat. Tak to podle Lessiga fungovalo v počátcích internetu, každý byl neviditelným mužem. Kyberprostor byl postaven tak, že nikdo jednoduše nemohl identifikovat ostatní osoby. Jak ale uvádí dále, tato architektura internetu není Boží vůlí. Může být jiná a dokonce i přímo opačná – může jít o nejvíc regulovaný prostor, který kdy existoval (Lessig 2006).

Těmto snahám se dá do značné míry vyhnout prostřednictvím anonymizace přítomnosti na internetu za použití správných nástrojů. Bohužel právě i tyto nástroje jsou zneužívány k výše uvedeným trestným činnostem. Stejně tak jsou ale používány lidmi v ne zcela svobodných zemích, ve kterých je internetový prostor pod státním dohledem (Howard 2013). Bez nástrojů, které ze své podstaty umožňují bezpečnou komunikaci nebo které jsou nástrojem k vyhnutí se cenzuře v daném regionu, by tito lidé mohli být vystaveni persekuci za své názory a jednání v rozporu s režimem v dané zemi.

Důležitost anonymity se neomezuje pouze na státy, jejichž internet není svobodný (seznam těchto států lze nalézt například v ročních reportech Reporters Without Borders (Reporters Without Borders 2014)). Anonymita uživatelů má význam i při ochraně vlastního soukromí v rámci školní nebo firemní sítě.

Jak dále Lawrence Lessig uvádí, historie budoucnosti internetu se začala psát v Německu v lednu roku 1995. Na základě zákona o regulování pornografie nařídilo Bavorsko společnosti CompuServer, aby odstranila ze svých serverů pornografii, která byla dostupná německým občanům skrze USENET. Místo toho, aby společnost tento obsah smazala ze všech svých serverů, rozhodla se blokovat k danému serveru přístup na základě toho, z jaké země se uživatel připojil. Tímto aktem byl do jisté míry nastolen trend, kterým se kyberprostor začal ubírat.

Stejně jako se různí důvody pro identifikaci uživatele, mají i samotní uživatelé různé důvody zůstat v anonymitě. Jak popisuje Sherry Turkle ve své knize *Life on the Screen: Identity in the Age of the Internet*, že Internet ve své relativní anonymitě a mnohonásobných možnostech k sociální interakci dovoluje každému

experimentovat s více verzemi svého já. Tento stav přirovnává k dětským hrám, ve kterých lze experimentovat bez strachu z odmítnutí okolím (Turkle 1995).

V kvalitativním výzkumu z roku 2013 vyzpovídali vědci z Carnegie Mellon University napříč kontinenty 44 lidí, kteří již někdy usilovali o anonymitu na Internetu (Kang 2013). Z rozhovorů vyplynulo, že drtivá většina využívá anonymity pouze ke konkrétním činnostem a že nemají potřebu setrvat v tomto stavu déle. Přes polovina všech účastníků výzkumu využívá anonymity k maligním či ilegálním aktivitám, jakými jsou útočení a hackování ostatních, navštěvování stránek zobrazujících násilí či pornografii a v neposlední řadě i ilegální sdílení souborů a stalkingu ostatních uživatelů.

Téměř polovina z dotázaných aktivně tvoří textový i obrazový obsah, ale z obav před spojitostí s jejich například profesním životě raději publikuje anonymně. Právě obavy spadají podle autorů do pěti kategorií: strach z cyber zločinců, organizací, svých známých, ostatních uživatelů v rámci stránky či komunity a neznámých ostatních (unknown others). V rámci poslední kategorie se respondenti často strachovali o ztrátu kontroly nad jejich osobními údaji a dalším obsahem, což dokumentují jejich výpovědi:

- *Do značné míry, nemůžete kontrolovat, kdo vidí, přistupuje nebo užívá veškeré údaje, které dáte na internet ... Internet nikdy nezapomene.*
- *„Internet je ošemetný, stránky zůstanou, informace zůstanou a tak dále...“*
- *„Nemám ponětí co se s osobními informacemi děje. Kam až se dostanou, nebo jak je možné se k nim dostat.“*

Pravdou zůstává, že většina běžných uživatelů Internetu nemá velké povědomí o tom, jak internet vlastně funguje (Madden 2010). Přes 80 % účastníků výzkumu zaměřeného na soukromí na Internetu přiznalo, že neví, jak se pohybovat na internetu anonymně.

K vyostření konfliktu mezi příznivci anonymity na straně jedné a zastánci reálné identity na straně druhé došlo v roce 2011 takzvanými *„Nymwars“*. Příčinou byla snaha společností Facebook a hlavně Google, který na své v té době nové sociální síti Google+ zavedl striktní pravidla pro výhradně reálné identity uživatelů bez

možnosti přezdívek a pseudonymů. Zatímco Facebook spoléhá ve vymáhání podobných pravidel primárně na hlášení ostatních uživatelů, Google přišel s algoritmem pro detekci pseudonymů, který automaticky blokoval účty. Brzy se ale projevily nepřesnosti v algoritmu, špatně vyhodnocoval například cizokrajná jména. Po několika měsících Google na své sociální síti pseudonymy přeci jen povolil, stále však vyžaduje reálné jméno uživatele při registraci (Galperin 2011). Podobná situace se opakovala i v roce 2013, kdy Google integroval Google+ do své služby pro streamování videa YouTube. Tento krok opět směřoval k cíli přimět své uživatele používat reálnou identitu. Jedním z hlavních argumentů pro obhajobu těchto kroků je redukce urážlivých komentářů napříč službou za pomoci autocenzury ve vztahu k reálné identitě, pod kterou uživatel vystupuje.

Na opačném přístupu k anonymitě v interakci s ostatními uživateli fungují služby, jakými jsou Reddit nebo 4chan, komunitní portály pro diskuzi a sdílení původního obsahu. Právě 4chanu, stránce s dvaceti miliony unikátních návštěvníků měsíčně (4chan 2014), je přisuzován velký vliv na internetovou kulturu jako celek. Drtivá většina příspěvků je publikována jako „Anonymous“, „OP“ nebo zůstane kolonka autora zcela prázdná. Pro lepší představu: ve vzorku 5,5 milionů bylo přes 90 % příspěvků publikováno jako „Anonymous“. U pěti procent příspěvků byl pak použit slang, nebo speciální symboly, tedy netechnické řešení pro navození identity a identifikace uživatelé napříč příspěvky (Bernstein 2011).

Sám zakladatel 4chanu Christopher Poole je předním obhájcem anonymity na internetu. Dle něj právě anonymita zajišťuje autenticitu (Holiday 2011) a stojí tak v opozici k zakladateli Facebooku Marku Zuckerbergovi, který tvrdí pravý opak.

To, jaké výhody mezi anonymitou a reálnou identitou spatřují samotní uživatelé, ilustruje následující tabulka z práce *Why do people seek anonymity on the internet?* (Kang 2013).

Tabulka 1 Výhody mezi anonymitou a identitou

Kategorie	Výhody anonymity	Výhody identifikace
Sociální vazby	Vyhnutí se odporu ostatních Vyhnutí se závazkům vůči komunitě Odstranění bariér k novým vztahům Ochránění svých blízkých	Spojení s reálnými přáteli Silnější sociální pouto Povzbuzení k většímu zapojení
Reputace a důvěra	Upřímné hodnocení a doporučení	Dobré pro budování reputace Získání důvěry od ostatních uživatelů
Budování image	Kontrola nad vlastní image Vyhnutí se ponížení / souzení / kritiky	Vyhnutí se hrubé kritice Konzistentní image
Emoční benefit	Pocit uvolněnosti a pohodlí	Pocit opravdovosti, zapojení Větší blízkost k ostatním
Vyjádření názoru	Jednoduší vyjádření vlastních názorů	Vyhnutí se nezodpovědnému chování
Soukromí	Kontrola nad zveřejněním vlastních osobních údajů	Vypadat nevinně
Bezpečnost	Ochrana vlastního bezpečí Vyhnutí se právním důsledkům / spamu / stalkingu / ztrátě majetku	Schovat se v davu
Jednoduchost použití	Odpadá nutnost se přihlašovat	Snadno zapamatovatelný účet

3 Identifikační technologie

Následující kapitola představuje nejpoužívanější metody a technologie vedoucí k identifikaci uživatele. Jak již bylo předesláno dříve, původní protokol TCP/IP je v otázce identifikace uživatele v podstatě neutrální. Vzhledem k jeho implementaci a dalším webovým technologiím popsaným níže nicméně ve výsledku nekompromisně směřuje k identifikaci uživatelů, a to často i bez ohledu na jejich soukromí.

3.1 IP adresa

IP adresa jako základní stavební kámen dnešní internetu. Je to unikátní adresa každého zařízení připojeného do sítě a je již ze své podstaty poměrně unikátním identifikátorem. Z principu rozdělování těchto adres v blocích se dají logicky vyvodit informace například o geografické poloze. Tomu napomáhá i fakt, že oproti zamýšleným několika stovkám IP adres se nyní nacházíme v období, kdy čtvrtá revize protokolu IP (IPv4) se svými 32bitovými adresami začíná být nevyhovující a 4 miliardy adres kterými disponuje nedostačující.

Postupně dochází k jeho nahrazování šestou revizí (IPv6) tohoto protokolu, která pracuje s 128bitovými adresami a navyšuje limit do řádů stovek sextiliónů adres. S nástupem IPv6 adres se často zmiňují i obavy v souvislosti se soukromím uživatelů a jejich mnohonásobně větší unikátnost oproti v současnosti převažujícím IPv4 adresám. Jedna z hlavních obav je spojena se samotnou tvorbou IPv6 adres, která je částečně založena na MAC adrese síťového zařízení, která je sama o sobě naprosto unikátní.

Dále již nebude potřeba a údajně ani technicky možné mít připojeno více zařízení za pomoci NAT (Network Address Translation), což je technologie nejčastěji na úrovni routeru, která vznikla právě pro úsporu IPv4 adres. Při jejím použití dochází ke komunikaci všech zařízení se zbytkem internetu pod jedinou IP adresou, na kterou všechny požadavky router překládá. *„Network*

Masquerading", tedy „síťová přestrojení", se později stala synonymem pro NAT odrážejícím schopnost skrýt celé sítě za jedinou IP adresu.
Šestá generace tohoto protokolu v sobě skrývá i mnoho pozitivních změn a je otázkou, zda se vyplní obavy z i těch v současnosti negativně vnímaných. Třeba právě ty ve spojení se soukromím na internetu.

3.2 Geolokace

Pro zjištění geografické polohy zařízení se v současné době nejčastěji používají dvě techniky. Technika pasivnějšího rázu je založena na ověřování IP adres v rámci databází obsahujících jejich polohu založenou primárně na předpokladu o rozsahu adres, které danému regionu či poskytovateli připojení byly přiděleny. Tyto údaje jsou samozřejmě zpřesňovány hlavně v případě komerčně dostupných databází a ve většině případů jsou korektní. Přesto jsou ale v poslední době na vzestupu techniky s aktivnějším přístupem, které dokáží nabídnout přesnější informace, a to i při případně protichůdné snaze samotného uživatele.

Takzvaná *constraint-based geolocation* (Gueye 2006) pracuje na základě aktivního měření vzdálenosti za pomoci odezvy. Ve své podstatě jednoduché ale velice účinné je měření nejnižší možné dosažené odezvy hostitele (Katz-Bassett 2006), na jejímž základě se vyhodnocuje reálná vzdálenost. V případě sofistikovanějších algoritmů je brána v potaz i struktura sítě a další aspekty pro co nejpřesnější výsledky.

Vzhledem k vzrůstajícímu užívání mobilních zařízení obecně a jejich častějším přípojení do sítě se rozšiřují geolokační možnosti o *Global Positioning System* (GPS), kterým je dnes již většina zařízení vybavena, ale také o *Wi-Fi Positioning System* vhodný zejména při pohybu uvnitř budov či v husté zástavbě a o lokaci na základě tradiční GSM sítě v případě mobilních telefonů a tabletů.

V kontrastu s předchozími technologicky založenými postupy je možné využít i obsahovou analýzu příspěvku v případě, že se jedná o webovou stránku obsahující prvky webu 2.0: blog, diskuzi či sociální síť. Například pro sociální síť Twitter (Twitter 2014) existuje relativně velké množství výzkumů na téma určení polohy

uživatele na základě obsahu jeho příspěvků. Cheng et al. (Cheng 2010) nebo v novější práci výzkumníci z IBM (Mahmud 2014) představují algoritmy, které na základě veřejně dostupných tweetů a jejich následné analýzy určují lokaci uživatele. Spolu s obsahem příspěvku, který může zahrnovat údaje o počasí nebo v ideálním případě geografické názvy měst, se bere v potaz i aktivita uživatele z pohledu času pro určení jeho časové zóny. Toto vše lze provést s více než 50 % úspěšností určení umístění s tolerancí několika desítek kilometrů.

3.3 Cookies

Jak již bylo předesláno v úvodu práce, koncept cookies byl vymyšlen a představen v roce 1994 (Kristol 2001) Lou Montullim. Cookies slouží jako trvanlivý identifikátor mezi klientem a serverem v rámci webu, později schválen jako standard (Kristol 2000) v rámci The Internet Engineering Task Force (IETF). Technologie funguje na základě uložení malého množství dat ze strany serveru do klientova zařízení. Při opětovném navštívení daného webu dojde k odeslání uložených dat a k pokračování předešlé relace. Za 20letou existenci se cookies rozšířily a nabobtnaly do úctyhodných rozměrů. Vzniklo mnoho různých typů (*session cookie, 3rd party* cookies) a díky jejich citlivé povaze vůči soukromí se jimi ve své legislativě zabývá i Evropská unie (Evropská komise 2014).

Původní HTTP cookie (resp. *first-party cookie* neboli cookie první strany) přinesla do prostředí nově vznikajícího webu možnost nastolit určitý vztah (Kristol 2001) mezi klientem a serverem. Tento vztah byl velmi žádoucí zejména v prostředí elektronických obchodů, které by velmi složitě fungovaly, pokud by si nemohli zákazníci přidávat zboží do virtuálních košíku, tak aby tam při následném pohybu pro stránce i zůstalo. Zároveň ale HTTP cookies první strany umožňovaly sledovat pohyb uživatelů v rámci jednoho webu.

K samotnému vytvoření HTTP cookie dojde na základě zaslání HTTP hlavičky ze serveru s následujícím obsahem: *Set-Cookie: value[; expires=date][; domain=domain][; path=path][; secure]* (Kristol 2000). Vlastnosti cookie, jakými jsou název, expirační doba nebo lokální umístění si určuje původce a

uživatel je v případě přijmutí nemůže ovlivnit. Cookie může ale odmítnout nebo ji posléze smazat.

Možnost sledovat uživatele napříč více weby přichází spolu s takzvanou *third-party cookie* neboli cookie třetích stran, které se začínají objevovat v roce 1997. Tyto cookies pocházejí, jak název napovídá, od třetí strany, která většinou na konkrétní webové stránce pouze hostuje část obsahu (tradičně obrázky či reklamy). Původně mělo být přijímání těchto cookies v základním nastavení prohlížečů vypnuto. Reklamní průmysl byl nicméně pochopitelně proti tomuto rozhodnutí s argumentem o narušení celkové modelu jejich podnikání na webu. V současné době nabízí drtivá většina webových prohlížečů snadnou kontrolu a široké možnosti, jak s cookies třetích stran nakládat.

Oproti standardním HTTP cookies se pozdější začínají prosazovat i takzvané Flash cookies založené na technologii Flash od společnosti Adobe. Přesněji řečeno se jedná o *„local shared object"*, který může obsahovat až 100 KB (Soltani 2009) informací oproti HTTP cookie limitované na 4 KB. Dále se liší tím, že není přímo spravován prohlížečem, má odlišné umístění a standardně není nijak časově omezen. Znepokojující je i praxe obnovení HTTP cookie po jejím smazání na základě Flash cookie ze stejného serveru. Tyto cookies jsou trefně označovány jako *Zombie cookies*.

Pro úplnost je třeba zmínit ještě *Secure cookie*. Ta využívá výhod šifrovaného HTTPS protokolu a takzvanou *Supercookie*, která se nevztahuje na jeden konkrétní server, ale rovnou na celou doménu nejvyššího řádu (.com) umožňující ze své podstaty velká rizika z pohledu soukromí i bezpečnosti. Supercookies jsou prakticky ve všech moderních prohlížečích blokovány bez zásahu uživatele.

3.4 Fingerprinting

Oproti cookies, které jsou z větší části pod kontrolou uživatele, se stále více prosazuje nová metoda identifikace zařízení skrze webový prohlížeč, a to takzvaný *Web-based device fingerprinting*. O této technologii se začalo poprvé mluvit v roce 2009 v souvislosti s implementací *„Do Not Track"* volby do

webových prohlížečů, které tato technologie ignorovala a stejně uživatele sledovala i přes jejich explicitní nesouhlas. Po zveřejnění a následné diskuzi k tomuto etickému problému došlo ke slibu, že volbu uživatele budou brát do budoucna tvůrci těchto technologii v potaz.

Při pohledu zpátky působí začátky této technologie skoro až úsměvně, protože v současnosti komerční software založen na principech fingerprintingu využívá v případě *„Do Not Track"* volby uživatele jako jednu z mnoha informací, na jejímž základě vytvoří virtuální otisk zařízení.

Blíže se na technologii fingerprintingu podíval Peter Eckersley z Elektronic Frontier Foundation v roce 2010, kdy spolu s kolegy napsal vlastní open-source fingerprintovací software Panopticlick (EFF 2010). Díky tomu si uživatelé mohou ověřit, jaké informace jejich prohlížeč předává webovým serverům, které navštěvují, a jak je jejich prohlížeč unikátní ve vzorku ostatních uživatelů, kterých se nakonec sešlo téměř 300 tisíc.

Na základě tohoto experimentu publikoval Peter Eckersley studii příznačně nazvanou *How Unique is Your Browse*r (Eckersley 2010), který širší veřejnosti představuje fingerprinting jako takový. Tato technologie v podstatě pracuje na základně unikátního otisku každého webového prohlížeče, který se skládá ze všech dostupných informací, který fingerprintovací software dokáže o uživatelském zařízení shromáždit – rozlišení obrazovky, fonty v zařízení, verze všech doplňků a plug-inů, které moderní prohlížeče využívají. Všechny tyto informace jsou v drtivé většině ve své šíři natolik unikátní, že je možné tento otisk použít jako globální identifikátor. Ten v průměru obsahoval v rámci tohoto experimentu 18.8 bitů identifikační informace a téměř 95 % otisků bylo zcela unikátních v rámci 287 tisíc vzorků. Proti fingerprintingu se navíc daleko obtížněji brání než proti cookies.

Autorský kolektiv kolem výzkumníka Nicka Nikiforakise blíže prozkoumal ekosystém fingerprintovacího softwaru a jeho komerční implementace (Nikiforakis 2013). Ten se oproti předešlému razantně liší v šíři informací a vynalézavostí, jak tyto informace o zařízeních zjistit.

Poměrně velkou roli zde hrají populární zásuvné moduly moderních webových prohlížečů JavaScript a Adobe Flash, tedy software nutný pro využívání pokročilých webových technologií, na základě kterých fungují. Tyto dva moduly nenapomáhají k co nejvíce unikátnímu otisku pouze prozrazením svých aktuálních verzí, ale dají se využít i ke zjištění dalších informací o zařízení. Pro ilustraci: běžný webový prohlížeč nahlásí na server typ systému v následujícím tvaru „Linux x86_64“. Na podobný požadavek Flash odpoví „Linux 3.2.0-26-generic“, tedy celou verzí linuxového jádra. Flash také ochotně nahlásí seznam všech fontů, které se v zařízení nachází, což v případě jediného méně tradičního fontu vede k získání velice cenných informací pro otisk. V neposlední řadě se dá využít i ke detekci opravdové IP adresy straně uživatele pokud se jí snaží skrýt, kdy fingerprintovací software zašle požadavek skrze Javu a Flash souběžně a pokud přijde z dvou rozdílných IP adres, je zřejmé, že sklient využívá http proxy. Tato slabina, kdy Flash ignoruje jakékoliv proxy, je poměrně známá, díky čemuž je technologie Flash blokována na většině softwaru dopomáhajícímu k anonymitě na internetu.

Podobná situace panuje i u JavaScriptu, který se dá v případě vypnutého Flashe využít ke zjištění systémových fontů. To může provést skrze vytvoření neviditelného okna prohlížeče, ve kterém dojde k otestování jednotlivých fontů. Logicky by se nabízelo zablokování výše uvedených zásuvných modulů. To by ale ve výsledku nejenom zkomplikovalo využívání tradičních webových stránek, ale v důsledku by došlo díky zařazení k velice malému počtu uživatelů, kteří mají tyto dva moduly vypnuté, k ještě větší unikátnosti.

Na závěr výše zmíněného výzkumu se autoři pokusili zjistit rozšíření fingerprintingu v rámci webu na vzorku 10 000 nejpopulárnějších stránek dle žebříčku Alexa (Alexa 2014). I při limitaci jejich analýzy pouze na software třech komerčních poskytovatelů, jejichž kód se snažili u uvedených stránek detekovat, objevili 40 stránek využívající fingerpritingu. Mezi stránkami s pornografickým obsahem a různými seznamkami byl tento kód detekován i na webu (Skype 2014) populárního programu Skype od společnosti Microsoft.

Tato metoda začíná hrát stále větší roli i v případě mobilních zařízení, které s nástupem modulárních prohlížečů a a roztříštěností verzí operačních systému začínají připomínat klasické počítače. Jako nejrezistentnější se vůči fingerprintingu v minulosti ukázala třetí generace zařízení iPhone od společnosti Apple, a to díky obrovské anonymitě setu, v rámci kterého měla zařízení stejné rozlišení obrazovky, verzi operačního systému nebo jeden webový prohlížeč.

3.5 Analýza síťového provozu

Analýza síťového provozu, známá spíše jako *traffic analysis*, je nejkomplexnější z výše uvedených technik a v podstatě kombinuje něco z každé z nich. Pro každý specifický typ dat a druh protokolu je nutný specifický přístup. Všechny nicméně mají společný základ v analýze dat tekoucích mezi uživatelem a serverem. V podstatě stačí, aby byl útočník připojen na stejné bezdrátové síti – může jít o poskytovatele připojení nebo někoho, kdo je schopný se postavit mezi uživatele a server a tok dat odposlouchávat.

Vzhledem k tomu, že samotné odposlouchávání paket v případě využití stejné bezdrátové sítě je velice jednoduché (například pomocí populárního open-sourcového programu Wireshark (Wireshark 2014)), je důležité pro zachování soukromí a samozřejmě i z bezpečnostních důvodů používat šifrované verze protokolů pro prohlížení webu, elektronickou poštu a další činnosti. Bohužel ani nejpopulárnější šifrovaný protokol HTTPS chráněný pomocí SSL/TLS není vůči analýze datového toku zcela rezistentní, a to ani v případě pominutí chyby Heartbleed (CVE-2014-0160 2014), která se dva roky skrývala v open-sourcové implementaci OpenSSL a umožňovala získat privátní klíče z postiženého serveru.

Realizaci *traffic analysis* vůči protokolu HTTPS popisuje Brad Miller ve svém výstižně pojmenované publikaci *I Know Why You Went to Clinic* (Miller 2014), kde se zaměřuje i na další citlivé oblasti, jakými jsou právní a finanční služby, za využití mimo jiné lokačních dat, cookies a obsahu vyrovnávací paměti. Velice sofistikovanou metodou je také *website fingerprinting* (Herrmann 2009), při které se útočník snaží rozpoznat navštívenou stránku na základě jejího otisku - velikosti přeneseného obsahu, počtu jednotlivých elementů, externích prvků a podobně.

Pravdou ale zůstává, že ve většině případů je šifrovaný datový tok několikanásobně obtížnější nějakým způsobem prolomit a v obecné rovině může útočníka spíše odradit.

4 Soukromí podporující technologie

Tato kapitola představuje nástroje souborně označované jako soukromí podporující technologie (*Privacy-enhancing technologies*), které v ideálním případě (tedy za předpokladu jejich správného použití) mohou uživateli poskytnout anonymitu v prostředí internetu.

4.1 Doplňky prohlížečů

Přestože doplňky prohlížečů samy o sobě anonymitu na internetu svým uživatelům nezajistí, mohou k ní dopomoci v rámci jednotlivých aspektů, kterými je anonymita podmíněna.

4.1.1 AdBlock Plus/Edge

AdBlock Plus (Adblock Plus 2014) a jeho odnož AdBlock Edge (AdBlock Edge 2014), která se liší chybějícím seznamem povolených, sponzorovaných reklam, primárně blokuje reklamu na webu. Kromě zpříjemnění uživatelské komfortu při prohlížení webu i de facto blokuje sledování uživatele třetími stranami. Mimo klasických reklam dochází i k blokování tlačítek sociálních sítí vložených napříč weby a i díky těmto opatřením si tento nástroj vedl velice dobře v porovnání s dalšími doplňky prohlížečů dle Stanfordské univerzity (Mayer 2011).

4.1.2 Ghostery

Ghostery (Ghostery 2014) je doplňkem, který se výhradně zaměřuje na blokování sledovacích robotů napříč webem s databází čítající dva tisíce blokovatelných prvků. Tento doplněk dovoluje některé prvky opět ručně povolit a navíc v rámci svojí ikony v prohlížeči uživatele informuje o počtu detekovaných sledovacích softwarů, trackerů, u každé navštívené stránky, které blokuje. Ne výjimečně je toto číslo dvouciferné.

4.1.3 Disconnect Private Browsing

Doplněk Disconnect Private Browsing (Disconnect 2014) je velmi podobný svým konkurentům AdBlock a Ghostery. Největší rozdílem je opět vlastní databáze, na základě které blokuje trackery na webu. To může být výhodou i nevýhodou všech tří doplňků. Každý z nich může a nemusí některý obsah správně blokovat a uživatele přesto udržuje v přesvědčení, že je vše nežádoucí blokováno.
Řešením může být jejich kombinované použití, které ale může vést k technickým problémům se zobrazením jednotlivých stránek.

4.1.4 Disconnect Private Search

Pozoruhodným doplňkem, který je k dispozici pro většinu běžných prohlížečů, je Disconnect Private Search (Disconnect 2014). Tento doplněk je v podstatě speciálně zabudovaná VPN, skrze kterou jsou zasílány dotazy vyhledávačům (Google, Bing, Yahoo a dalším) při jejich běžném použití. Toto opatření slouží většímu soukromí uživatelů a chrání je před zaznamenáváním dotazů spolu s jejich IP adresou ze strany provozovatelů vyhledávačů nebo vlastního poskytovatele internetu. Dotazy jsou šifrovány a zasílány skrze speciální VPN pro skrytí IP adresy a samozřejmě i samotného dotazu.

Na adrese *https://search.disconnect.me/* je k dispozici webová verze této služby bez nutnosti instalace doplňku.

4.1.5 Privacy Badger

Privacy Badger (Privacy Badger 2014) je doplňkem z dílny Eletronic Frontier Foundation. Nyní je dostupný v alfa verzi. Autoři ho sami představují jako nástroj k blokování všech reklam a trackerů, které nefungují na základě souhlasu uživatele (Privacy Badger 2014). Částečně je opět založen na AdBlock Plus a dle slov autorů se nesnaží vyhranit vůči ostatním nástrojům, ale pouze vytvořit doplněk založený na jednoduchosti a funkčnosti.

4.1.6 HTTPS Everywhere

Více etablovaným doplňkem opět z dílny Electronic Frontier Foundation a Tor Project je HTTPS Everywhere (HTTPS Everywhere 2014). Jak název napovídá, toto rozšíření se snaží vynutit spojení s webovými servery skrze zabezpečený protokol HTTPS všude tam, kde je to možné. Standardně se snaží uživatele přesměrovat na šifrovaný protokol tam, kde je podporován, a to i přesto, že ve výchozím nastavení stránka používá nezabezpečené HTTP, nebo se snaží uživatele skrze odkaz ze zašifrované stránky přesměrovat zpět na nešifrovanou část webu.

4.1.7 NoScript Security Suite

Skrze doplněk NoScript (NoScript 2014) uživatel získává lepší kontrolu nad veškerým spustitelným obsahem ze strany webových stránek skrze jeho blokaci, kterou tento nástroj umožňuje. Primárně se tedy jedná o Javu, JavaScript, Flash, SilverLight a další. Díky tomu je uživatel lépe chráněn před trackováním obecně a navíc před bezpečnostními hrozbami spojenými právě s výše zmíněnými technologiemi. Konkrétně se díky zablokování JavaScriptu nemusí bát prozrazení reálné IP adresy při používání proxy, kterou má JavaScript tendenci ignorovat.

4.1.8 Self-Destructing Cookies

Doplněk prohlížeč Self-Destructing Cookies (Self-Destructing Cookies 2014) přistupuje k hrozbám spojeným s cookies tím, že je automaticky maže, jakmile přestanou být aktivně vyžadovány některou z právě otevřených webových stránek (tedy prakticky ihned po zavření záložky nebo odejití z dané stránky). Důvěryhodné služby umožňuje přidat na seznam povolených.

4.2 Technologie s vysokou latencí

Systémy pro anonymní komunikaci lze rozdělit do dvou základních kategorií: nízko a vysoko latentní. Pro lepší pochopení systémů s nízkou odezvou, které je možné využít k pohodlnému prohlížení webu a komunikaci v reálném čase, je dobré si nejprve představit ty s vysokou latencí, které zde byly historicky dříve.

Tyto systémy zpravidla poskytují velkou míru anonymity výměnou za vysokou odezvu, která bývá zpravidla v řádu hodin až dnů. Hodí se k asynchronní komunikaci typu elektronické pošty.

Koncept pravděpodobně prvního systému pro anonymní komunikaci byl představen Davidem Chaumem v roce 1981 (Chaum 1981). Ten popsal takzvaný „Mix server“, v rámci kterého dojde k promíchání jednotlivých zpráv před předáním jejich adresátům, a to tak, aby nedošlo ke spojitosti s odesílatelem. Od tohoto prvotního konceptu bylo představeno mnoho dalších a v dnešní době se v praxi používají tři typy komunikačních systémů s vysokou latencí. Zjednodušeně jsou označovány jako anonymní remailery.

4.2.1 Cypherpunk anonymous remailer

Jako první typ se uvádí takzvaný *Cypherpunk anonymous remailer*, který v podstatě odpovídá Chaumovu návrhu. Zprávy zaslané skrze tento systém jsou zpravidla šifrované veřejným klíčem remaileru a jejich adresáti jsou ukryti v jejím obsahu, který je po dešifrování doručen. Na zprávu zaslanou skrze tento systém nelze přímo odpovědět, a to z důvodu odstranění její hlavičky a dalším bezpečnostním opatřením těmi může být například řetězení několika remailerů za sebou).

4.2.2 Mixmaster

Druhým typem je *Mixmaster* (Moeller 2004), který směřuje každou zprávu skrze všechny uzly ve své síti před doručením adresátovi za použití SMTP protokolu. Mixmaster reflektuje několik nedostatků *Cypherpunk anonymous remaileru* a mimo kryptografických vylepšení přidává například kontrolu integrity jednotlivých zpráv pro zamezení jejich modifikací na cestě k adresátovi. Pro použití je nutný speciální klient, který není součástí většiny operačních systémů.

4.2.3 Mixminion

Třetím a závěrečným typem je *Mixminion* (Danezis 2003), remailer fungující na základě schránky, které se adresát dotazuje na nové zprávy. Tento systém umožňuje přímé odpovědi, které navíc nerozlišuje od jiných typů zpráv, díky čemuž sdílí stejnou množinu anonymity. Sami tvůrci uvádí, že se snažili vzít to nejlepší z předešlých verzí a vytvořit konzervativní design s ohledem na známé slabiny těchto systému. Pro jeho užití je opět nutný speciální program.

4.3 Technologie s nízkou latencí

Jak název napovídá, dále popsané technologie poskytují daleko nižší odezvu než ty předešlé a dovolují prohlížet web a komunikovat v podstatě v reálném čase.

4.3.1 Proxy

Jedním z nejjednodušších nástrojů pro skrytí IP adresy je využití proxy. Proxy server – ve své základní funkci – stojí mezi uživatelem a serverem, vůči kterému se tváří jako původce dotazu, a odpověď serveru směřuje zpět uživateli.
V případě závažnějších případů, kdy se uživatel potřebuje skrýt, není proxy doporučována, spíše naopak. Snadno může dojít k prozrazení reálné IP adresy, a to ať už díky špatné konfiguraci některého z programu či již zmiňovaným vlastnostem doplňků prohlížeče (například Flashe), který ignoruje veškeré proxy.

Druhým hlediskem může být neznámá identita provozovatele většiny volně dostupných proxy serverů a z toho plynoucí rizika. U komerčně dostupných proxy serverů platí pravidlo, že pokud dojde k platbě za tuto službu tradičními způsoby, jakými jsou převod či platba kartou, je prakticky vyloučena zpětná nedohledatelnost uživatele.

Proxy ale může sloužit také jako jednoduchý nástroj pro obejití cenzury na základě IP adres. Tak tomu bylo například při nedávných událostech v Turecku při pokusu o blokování sociální sítě Twitter (Rawlinson 2014). Mimo jiné se mezi Tureckými uživateli rozšířilo obejití blokace pomocí využití známého DNS proxy serveru "8.8.8.8"společnosti Google. Ten byl následně také zablokován, nicméně demonstroval jednu z možností, jak blokování obejít.

4.3.1.1 Flash Proxy

Komplexnějším řešením založeným na stejném principu je Flash Proxy (Fifield 2012) vyvinutá pod záštitou Stanfordské Univerzity. Navzdory svému názvu již nefunguje na technologii Adobe Flash ale JavaScript a WebSocket. V tomto případě jsou jednotlivými proxy servery dobrovolníci.

Jak uvádějí autoři, nesnaží se v rámci tohoto projektu neustále zvyšovat počet použitelných adres. Spíše usilují o rychle se měnící fond, který lépe uspěje v rámci protiopatřeních cenzorů. Jejich cíl je podpořen faktem, že se lze jednoduše připojit – buď skrze doplněk internetového prohlížeče či jen při prohlížení stránky, která obsahuje embedovaný kód Flash Proxy.

4.3.1.2 Java Anonymous Proxy (JAP)

Java Anonymous Proxy (JAP 2011) vzniká jako výzkumný projekt Drážďanské univerzity. Je to propracované řešení fungující na základě proxy, které ale přidává i prvek takzvaných mixserverů skupinám proxy podobným těm z anonymizačních remailerů popsaných v předchozí kapitole.

Zajímavostí je, že z důvodu zavedení evropského zákona o uchovávání provozních a lokalizačních údajů na konci roku 2005, přistoupili tvůrci na koncept takzvané *revocable anonymity* (Kopsell 2006). Tento systém v případě nutnosti dovolí předat identifikační údaje bezpečnostním složkám na základě soudního rozhodnutí. V současnosti je projekt rozvíjen převážně pod názvem JonDo (JonDo 2014), komerční odnoží JAP.

4.3.2 Virtual Private Network

Za pomoci technologie *Virtual Private Network* (VPN) je možné počítače propojit, a to za pomoci certifikátů a šifrovaného spojení, skrze veřejnou síť (Cisco 2006). Na tomto základě dojde k vytvoření pomyslného tunelu mezi uživatelem a serverem. Tato technologie je často využívána při externím připojení například do firemní sítě. V neposlední řadě slouží k využívání internetových služeb, které jsou geograficky blokovány, nebo ke stahování více či méně legálního obsahu. V minoritě případů to může být i nástroj k obejití cenzury a blokace internetu v určitých zemích. Vše z výše uvedeného je možné na základě použití, při kterém dojde – podobně jako u proxy serverů – ke skrytí IP adresy za adresu poskytovatele služby.

Z pohledu anonymity je VPN z technického hlediska přijatelné řešení. V případě komerčních poskytovatelů si však nemůžeme být jisti jejich úmysly – z jakých důvodů uchovávají záznamy o relacích uživatelů a do jaké míry jsou ochotní bránit svoje zákazníky v případě intervence úřadů? Mimo otázku, pod jakou jurisdikcí daný poskytovatel funguje, se portál TorrentFreak (Ernesto 2014) dotazoval i na to, na jaké typy plateb jsou akceptovány a na základě této a dalších odpovědí komerčních poskytovatelů je seřadil podle toho, jak berou anonymitu svých uživatelů vážně.

4.3.3 Peer-to-Peer

Technologie založené na architektuře *Peer-to-peer* (P2P) ve své podstatě neznají pojem server a jednotliví uživatelé (peers) mezi sebou komunikují přímo. Díky této vlastnosti nemohou být tyto sítě centrálně spravovány (na rozdíl od technologií zmíněných výše) a už z jejich podstaty je mnohonásobně složitější

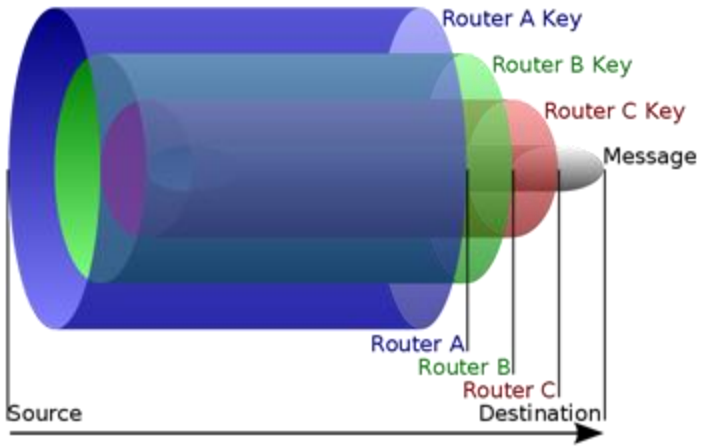
tyto sítě jednoduše vyřadit z provozu. Zpravidla i při vyřazení signifikantního uzlu v rámci sítě dojde jen k částečnému poškození, které se projevuje například sníženou rychlostí, kdy tok dat bude směřovat jinou cestou a bez odpojení části uživatelů, jak je tomu u standardních serverů. S přibývajícím počtem uživatelů zpravidla dochází k zlepšení konektivity celé sítě (za předpokladu, že uživatelé neomezují využití své linky).

Nejznámějším příkladem takové sítě je BitTorrent, nástroj ke sdílení souborů, který v dobách své největší popularity mezi roky 2004 až 2008 obstarával desítky procent ze souhrnného datového toku v rámci globálního internetu. Na rozdíl od BitTorrentu, který nikterak nezachovává anonymitu svých uživatelů a jejich IP adresu zobrazuje zbytku sítě, existují ale i technologie využívající výhod P2P právě k anonymizaci uživatelů v prostředí internetu.

4.3.3.1 Onion Routing

Koncept *Onion Routing* poprvé představil kolektiv okolo Paula Syversona z Naval Research Laboratory v roce 1996 (Goldschlag 1996). Původně se jednalo o projekt laboratoří amerického námořnictva na ochranu interní komunikace. Po ukončení první testovací fáze prošel kompletním přepsáním kódu a následně byla jeho druhá generace uvolněna pod MIT licencí do světa (Syverson 1996).

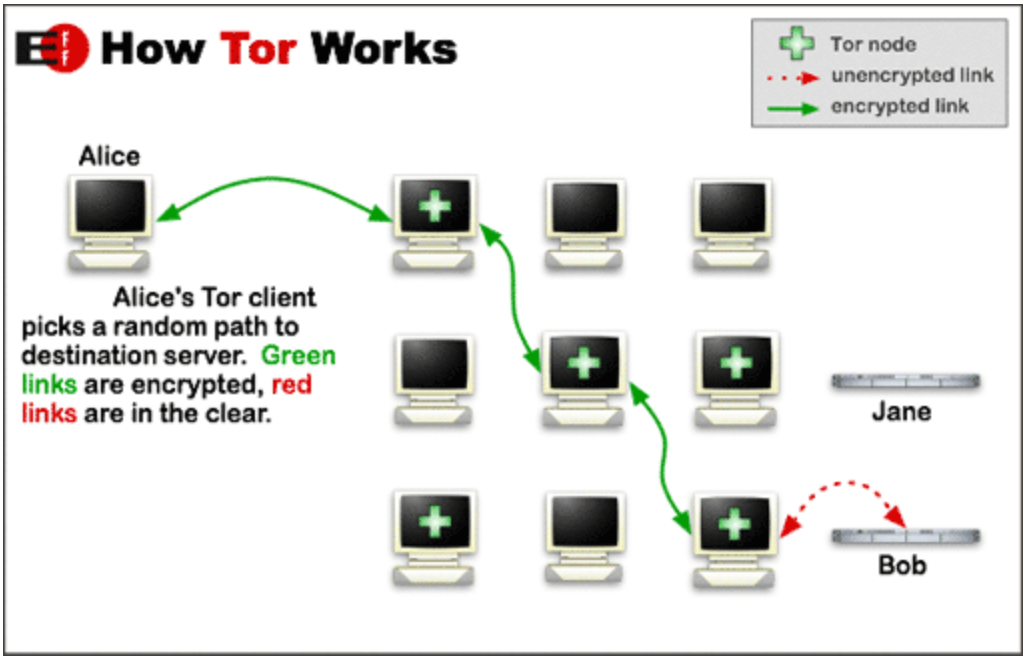
Obrázek 2 Schéma fungování Onion routingu (Wikipedia 2014)



4.3.3.2 The Onion Routing

Druhá generace byla představena Rogerem Dingledinem, Nickem Mathewsonem a Paulem Syversonem na symposiu USENIX v roce 2004 (Dingledine 2004). Po deseti letech jsou první dva jmenovaní stále v čele vývoje praktické implementace Onion Routeru druhé generace zastřešené později vzniklou neziskovou organizací *Tor Project* (Tor Project 2014a).

Obrázek 3 Jak funguje Tor (Tor Project 2014b)

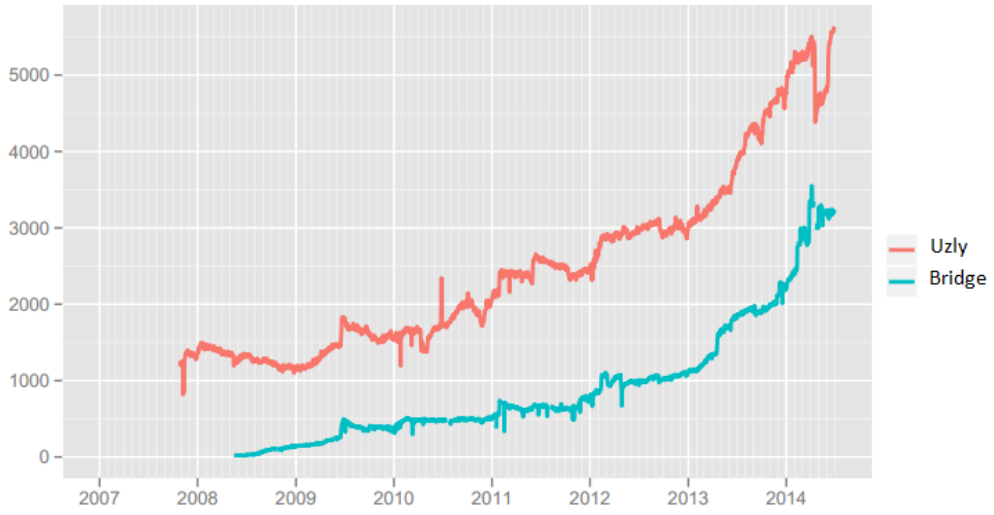


4.3.3.2.1 Tor Project

Slovo *Onion* (cibule) v názvu tohoto projektu naznačuje celý koncept fungování. V současnosti je celá síť založena na dvou typech uzlů, které buď předávají data dále v rámci sítě (*middle relay*) a nebo zajišťují komunikaci mezi sítí Tor a vnějším internetem (*exit relay*). Po připojení do této sítě se na základě algoritmu vytvoří spojení o třech vrstvách (třech slupkách cibule), které se skládá ze dvou prostředních uzlů a jednoho konečného. Komunikovaná data jsou zašifrovaná tak, že první uzel zná IP adresu uživatele, ale nezná obsah dat. Druhý uzel následně nezná původce ani obsah a až konečný uzel rozšifruje obsah a bez znalosti jeho původce jej přenáší do volného internetu.

Každý z mezičlánku pomyslně odlupuje jednu „vrstvu cibule“, tedy vrstvu šifrování. Odposlouchávat uživatele a de facto ho tak zbavit anonymity je tedy možné pouze v případě, že by útočník měl pod kontrolou všechny tři mezičlánky a zachytával jejich provoz. To je vzhledem k velikosti sítě a algoritmu, na jehož základě se spojení navazuje, málo pravděpodobné.

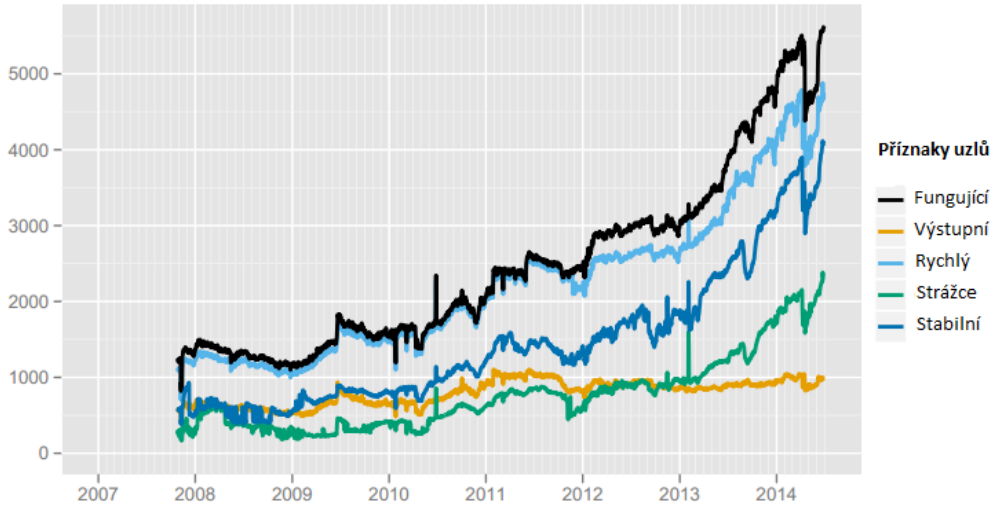
Graf 1 Počet uzlů Tor sítě (Tor Project 2014c)



Právě velikost sítě je možné vypozorovat na přiloženém grafu, který dokumentuje postupný nárůst jednotlivých uzlů, z kterých je síť složena, napříč roky fungování. Signifikantní propad v jejich počtu v první polovině roku 2014 byl způsoben odstřižením relays, jejichž operátoři včas nereagovali na kritickou chybu v OpenSSL. Společně s tímto došlo i k odpojení uzlů fungujících na zastaralé větvi verze 0.2.2.x a skokově tak bylo, v zájmu bezpečnosti celé sítě, odpojeno přes tisíc převážně menších uzlů (Dingledine 2014).

Zejména diverzita mezi jednotlivými uzly je velmi vítaný prvkem pro zabránění kompromitaci sítě. I malé body (malé co do datového toku) jsou tak z tohoto pohledu velmi přínosné. Ty velké poté samozřejmě mají pozitivní vliv na rychlost celé sítě.

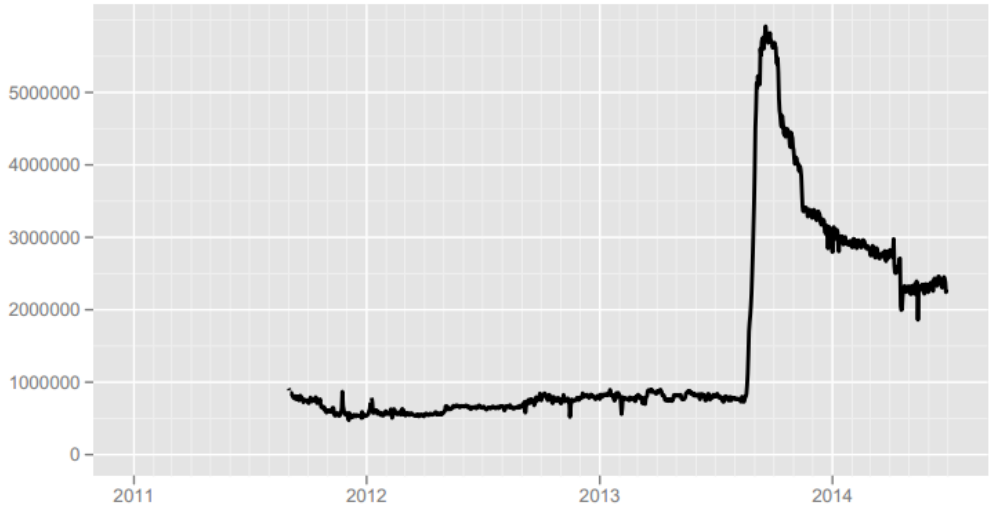
Graf 2 Typy uzlů Tor sítě (Tor Project 2014c)



V rámci celé sítě funguje několik adresářových autorit – *Directory Authority*, které shromažďují informace o všech uzlech a jejich vlastnostech. Tyto aktuální informace předávají koncovým klientům, ve kterých je seznam autorit v základu obsažen. Na základě fungování jednotlivých relays jim jsou přidělovány příznaky (*flags*) ve shodě všech autorit. Jak popisuje Roger Dingledine životní cyklus uzlů ve svém blogpostu (Dingledine 2013), k plnému zapojení do sítě dochází až po projití několika fází, které trvá přibližně deset týdnů.

Ve výše uvedeném grafu je také vidět počet relays s příznakem e*xit* – koncových uzlů, skrze které proudí data do zbytku internetu. Jejich provozování může být značně rizikové po právní stránce. Důvodem je, že se *exit relay* jeví jako původce veškerého provozu, který skrze ni proudí. Proto je důležité informovat poskytovatele připojení a reagovat na stížnosti od dalších subjektů. Pro snížení počtu hlášení má každý operátor možnost explicitně povolit nebo zakázat porty, ze kterých bude datový tok přijímat (Perry 2011). Je tedy možné pro vyhnutí se stížnostem spojeným s autorskými právy zakázat například BitTorrentové porty.

Graf 3 Počet připojených uživatelů Tor sítě (Tor Project 2014c)



Síť Tor je velká i při pohledu na uživatelskou základnu. Z dat je možné vyčíst stabilní základnu čítající téměř jeden milion připojení. Toto číslo bylo vcelku stabilní do poloviny roku 2013, kdy došlo k masivnímu nárůstu v době, kdy Edward Snowden odhalil snahy tajných služeb o monitorování internetu. Jak se ale brzy ukázalo, celou síť napadla skupina robotů, botnet Sefnit, založený na malwaru *Trojan:Win32/Sefnit.AT* pracující na platformě Windows (MMPC 2014). Naštěstí díky opatřením (Dingledine 2014) jak ze strany Tor Projectu tak ze strany Microsoftu došlo k omezení dopadu tohoto botnetu, který na několik týdnů síť skoro paralyzoval a stal se nechtěným zátěžovým testem. V současnosti jsou čísla stále nad dvěma miliony připojení. Je ale těžké odhadnout, na kolik jsou tato čísla stále olivněna botnetem.

Pestré je i geografické složení uživatelské základny. Více než polovina všech uživatelů pochází z Evropy, která je zároveň regionem s nejvyšší mírou penetrace s 80 uživateli Toru na 100 000 uživatelů internetu. Samotná Itálie s 76 000 uživateli denně tvoří skoro pětinu celé evropské uživatelské základny. Pouze Spojené státy americké jsou do počtu uživatelů před zmíněnou Itálií s 126 000 unikátními uživateli připojenými k Toru denně. Uživatelé ze středního východu jsou také početní s 60 připojeními na 100 000 běžných uživatelů internetu (Graham 2014). Velice populární je Tor také v Izraeli a zejména v Íránu, který je do počtu uživatelů třetím největším.

4.3.3.2.2 Tor

Mimo základního kamene celého projektu - programu T*or* (někdy je označován také jako *Tor daemon*; po instalaci funguje jako proxy pro jednotlivé programy, které je nutné nakonfigurovat tak, aby skrze něj komunikovaly) se postupně objevilo několik oficiálních i neoficiálních projektů usnadňujících jeho použití širší populaci. Tak je tomu v případě Tor Browseru nebo pozdějšího konceptu takzvaných *Bridge relays*, díky kterým je možné vzdorovat snahám o cenzuru internetu. Vývoj je stále poměrně bouřlivý, pokračuje v několika větvích a neomezuje se pouze na opravy chyb. Stále dochází k přidávání nových funkcionalit a možností (Tor Project 2014d).

Negativní světlo na celý projekt vrhá jeho využívání k ilegálním aktivitám některých jedinců. Toto znepříjemňuje život hlavně operátorům výstupních uzlů, kteří musí čelit různým hlášením o útocích a zneužívání od poskytovatelů internetového připojení. S tím je spojena i aktivní restrikce uživatelů Toru některými weby. Mezi těmito weby najdeme Wikipedii, 4chan nebo některé sociální sítě (Pagan 2014).

Samostatnou kapitolou jsou *Hidden Services* (Tor Project 2014e), technologie hostování webové stránky dostupné pouze z vnitřku sítě pod generickou pseudo-doménou nejvyššího řádu .onion. Za využití všech bezpečnostních prvků, které Tor ve své komplexnosti nabízí (spolu s čím dál tím více oblíbenými kryptoměnami), došlo v rámci tohoto takzvaného *Darkwebu* ke vzniku e-shopů, ve kterých je možné zakoupit vše od škálovatelného DDoS útoku přes psychotropní látky až po zbraně.

Po zákroku proti na té doby největší černý obchod v rámci Tor sítě, *The Silk Road*, se rozpoutala bouřlivá debata o možné kompromitaci celé sítě. Pravdou ale zůstává, že se údajný provozovatel Ross Ulbricht prozradil sám na základě svojí neopatrnosti (Olson 2013). S tím je spojený i fakt, že při připojení do Tor sítě je poskytovatel internetového připojení nebo jiná třetí strana s přístupem do sítě schopna rozpoznat, že uživatel Tor používá, což může v určité kombinaci času a prostoru vést ke ztrátě anonymity.

4.3.3.2.3 Tor Browser

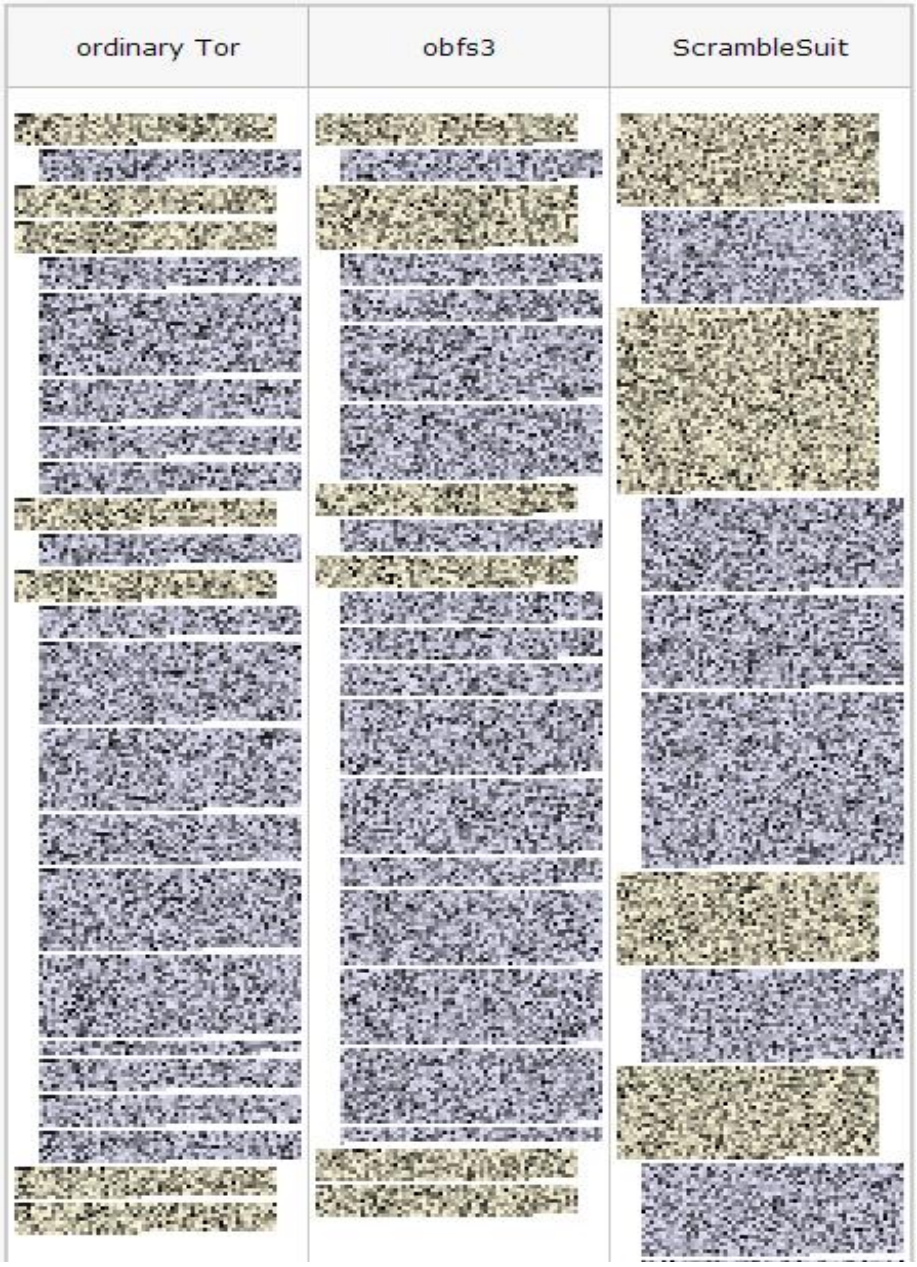
Tor Browser, dříve *Tor Browser Bundle*, je dalším stěžejním nástrojem z dílny Tor Project, o jehož vývoj se starají lidé v čele s Mikem Perrym. Jedná se o upravený prohlížeč založený vždy na poslední ESR (Mozilla 2014) verzi Firefoxu. Důvody, proč je využíván Firefox namísto Chromu, jsou popsány v blogpostu z roku 2010 (Perry 2010). Do dnešních dnů bohužel nebyla většina problémů vyřešena a prohlížeč Chrome stále zůstává nevhodný.

Kromě využití Tor sítě pro přenos dat je prohlížeč nakonfigurován a vybaven několika doplňky tak, že se jedná o jedno z nejkomplexnějších řešení pro zachování anonymity na internetu vůbec (pomineme-li kompletní linuxové distribuce, které v sobě *Tor Browser* často integrují). Ze své podstaty ho je navíc možné využít k obejití cenzury, což je umocněno i několika funkcemi vytvořených přímo k tomuto účelu. Tyto funkce jsou popsány níže. Konkrétně *Tor Browser* aktivně zamezuje fingerprintingu zařízení skrze spoofování (falšování) jazyka systému, verze prohlížeče, časové zóny a dalších. Blokuje některá vnitřní procesy Firefoxu za pomocí pluginu *TorButton* a skrze doplněk *NoScript* je možné vypnout JavaScript, který je ovšem kvůli masivnímu rozšíření napříč webem v základu povolen. Posledním obsaženým doplňkem je *HTTPS Everywhere* (HTTPS Everywhere 2014) vznikající ve spolupráci *Eletronic Frontier Foundation* a *Tor Projectu*. Tento plugin vynucuje zabezpečenou komunikaci s webovými servery skrze protokol HTTPS všude, kde je to jen možné, a brání tak odposlouchávání komunikace.

Ve verzi 3.0 se nyní *Tor Browser* uživatele při prvním spuštění dotazuje, zda jeho připojení není jakkoliv blokováno a zda nepotřebuje využít připojení skrze takzvanou *Bridge relay*, tedy pomyslný most do Tor sítě. Tyto uzly nejsou zveřejněny, a proto je nepravděpodobné jejich kompletní zablokování. O tyto mosty si musí uživatel zažádat na speciální stránce (Lovecruft 2014), nebo na speciální emailové adrese, která akceptuje dotazy pouze z emailových adres @gmail.com a @yahoo.com, které jsou navíc omezeny v čase a chytře tak kombinují ochranu proti robotům s tou ze strany Gmailu a Yahoo.

V případě, že by i standardní připojení skrze Bridge relay bylo například z důvodu detekce a následné blokace dat přenášených skrze Tor nefunkční, je možné využít vlastností *Pluggable Transportu*, které některé bridge obsahují. Pluggable Transport, který je od verze 3.6-beta-1 obsažen i v základní verzi Tor Browseru, umožňuje modifikovat tok dat takovým způsobem, že jej není možno rozeznat od běžného toku. Toho je dosaženo za pomocí protokolů obsf2 (Kadianakis 2014) obfs3 (Kadianakis 2014) a nově i ScrambleSuit (Winter 2013), jehož funkce budou spolu s dalšími zahrnuty v nově připravovaném obsf4.

Obrázek 4 Vizualizace modifikací datového toku (Tor Project 2014e)



Jak je vidět z vizualizace datového toku, obsf3 používá stejně velké pakety jako při standardní komunikaci. Tyto pakety se ale mění tak, aby vypadaly jako souvislý stejnorodý tok dat bez jakéhokoliv pravidelného schématu. ScrambleSuit navíc mění i velikost jednotlivých paket., což vede k většímu datovému toku a větší zátěži sítě.

Z důvodu bezpečnosti bylo rovněž ve verzi 3.0 (Perry 2013) zavedeno deterministické sestavení tohoto softwaru. V praxi to znamená, že bez ohledu ne to, kdo a na jakém stroji si ze zdrojových kódů sestaví samotný Tor Browser,

bude vždy naprosto identický do posledního bytu. Potenciální maligní upravená verze bude tudíž snadno detekovatelná. Dosažení a nasazení tohoto deterministického sestavení trvalo několik měsíců a dle svědectví samotného autora (Perry 2013) se nejedná o jednoduchou cestu, ale i díky jeho úsilí se do budoucna zvažuje nasazení reprodukovatelného sestavení balíčku napříč linuxovou distribucí Debian (Bobbio 2014) z důvodu větší bezpečnosti.

4.3.3.2.4 Orbot

Tor je k dispozici i pro mobilní telefony, a to konkrétně pro operační systém Android pod jménem *Orbot*. Tato aplikace není zcela oficiální, ale k jejímu vývoji dochází za podpory Tor Projectu pod hlavičkou Guardian Project. Jedná se samozřejmě o otevřený zdrojový kód. Nedávno se dočkal svojí 14. verze, která podporuje i pokročilé funkce mostů a modifikace datového toku. (Freitas 2014) Podobně jako u klasické verze Orbot vytvoří proxy, skrze kterou je možné směřovat datový tok Tor sítí. Většinu aplikací je třeba ručně nakonfigurovat (kromě několika již předkonfigurovaných). Mezi těmito aplikacemi je i obdoba Tor Browseru - Orweb z dílny stejných autorů.

4.3.3.2.4 Onion Browser

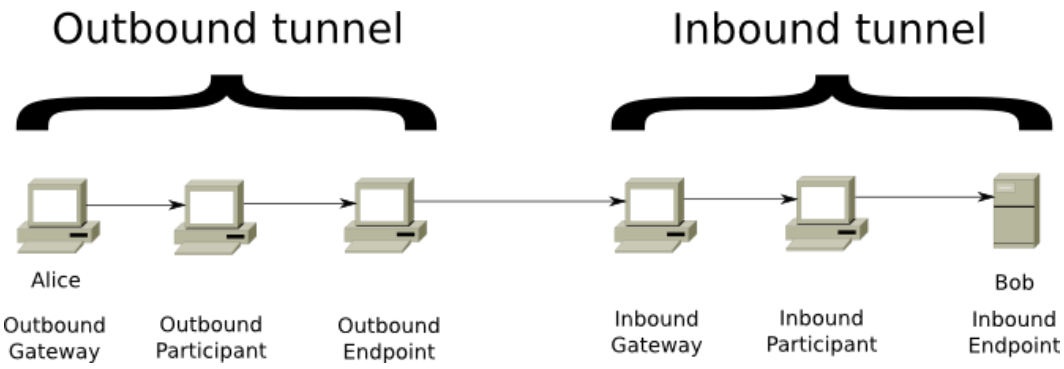
Na platformě iOS od společnosti Apple je k dispozici aplikace s názvem Onion Browser. Jak samotný autor uvádí, má se jednat o minimalistický prohlížeč, který směřuje a šifruje veškerá data skrze Tor. Spolu s dalšími vlastnostmi má sloužit jako nástroj k zachování soukromí na internetu. Z obav před bezpečností této aplikace (vzhledem k tomu, že se již několikrát v AppStoru objevila podobná, maligní aplikace) byl vykonán bezpečnostní audit v květnu 2014 (Heiderich 2014). Tento audit shledal aplikaci bezpečnou a upozornil na některé nedostatky (Tigas 2014), které byly promptně odstraněny. Mezi nimi byl například nedostatek v podobě blokování cookies třetích stran, chyba potenciálně umožňující odhalit IP adresu, nebo problém s SSL certifikáty napříč .onion doménami. Od verze 1.5 jsou již tyto nedostatky opraveny, starší verze jsou považovány za nebezpečné.

4.3.3.2 Invisible Internet Project (I2P)

Vývoj *Invisible Internet Projekt* začal v únoru roku 2003 (Kubiezie 2007) za účasti mnoha nadšenců, přičemž někteří v projektu setrvali dodnes, kdy se celý projekt blíží k milníku vydání verze 1.0. V současnosti je aktuální verze 0.9.13 (I2P 2014a).

Koncept jeho fungování je založen na lehce modifikovaném systému onion routingu zvaném *garlic routing*. Hlavní nadstavbou oproti klasickému onion routingu, kdy jsou data zabalena v několika šifrovaných vrstvách a po cestě skrze jednotlivé uzly jsou vrstvy odebírány, nabízí garlic routing možnost v jednom „česneku“ (garlic) zabalit zprávu více adresátům. To vše je umožněno systémem příchozích a odchozích tunelů.

Obrázek 5 Schéma fungování I2P (I2P 2014b)



Každý uživatel disponuje pomyslnými dvěma tunely. Každý se skládá z několika uzlů, skrze jeden jsou data odesílána a skrze druhý přijímána. V praxi garlic routing znamená, že poté, co data opustí odchozí tunel, je možné je rozdělit různým příjemcům. Následně jsou data směrována do příchozích tunelů, které jsou opět složeny z několika uzlů. Tunely jsou znovu vytvářeny každých 10 minut a počet uzlů, z kterých se bude skládat, je na volbě uživatele, což je další výhodou garlic routingu. Každý uživatel si může najít vlastní poměr mezi latencí a mírou anonymity.

Při srovnání obou projektů lze snadno dojít k závěru, že jsou si velice podobné. Hlavním rozdílem ale může být jejich zacílení (I2P 2014c). Zatímco Tor primárně

směřuje k přenosu dat vně své sítě, I2P je zaměřeno na provozování aplikací, webových serverů (.i2p) a komunikaci obecně v rámci interní sítě (přestože komunikace s vnějším internetem je možná).

4.3.3.3 Freenet Project

Autorem celého konceptu Freenetu je Ian Clarke, který jej vytvořil v roce 1999 jako závěrečnou práci při studiu na Univerzitě v Edinburgu. Práce se jmenuje *„A Distributed Decentralised Information Storage and Retrieval Systém"* (Clarke 1999). Po ukončení studií se rozhodl svoji myšlenku realizovat za pomoci několika dobrovolníků v duchu citátu Mika Godwina z Electronic Frontier Foundation (EFF 2001), ve kterém vyjadřuje svoje obavy o budoucnost internetu:

„I worry about my child and the Internet all the time, even though she's too young to have logged on yet. Here's what I worry about. I worry that 10 or 15 years from now, she will come to me and say 'Daddy, where were you when they took freedom of the press away from the Internet?"

Vývoj probíhá od roku 2000 a pokračuje dodnes. Postupně byly představeny nové funkce, jako je *darknet mód*, díky kterému je v současné době Freenet vnímám jako velice bezpečná, anonymní a decentralizovaná platforma pro sdílení dat zaměřená proti cenzuře v jakékoliv podobě.

Každý z uživatelů může vyhradit určitý prostor na svém lokálním disku, který je následně k dispozici celé síti k ukládání zašifrovaných souborů od ostatních uživatelů. Tyto soubory navíc mohou být, pokud se jedná o velký objem dat, rozděleny na několik částí. Výhodou Freenetu oproti například Hidden services v síti Tor může být to, že není nutné provozovat svůj vlastní server, a že i po vypnutí počítače jsou data online rozprostřena mezi uživatele Freenetu. Ke snazšímu využití všech možností jsou vyvíjeny speciální aplikace (podobně jako je tomu u I2P) (Freenet 2014).

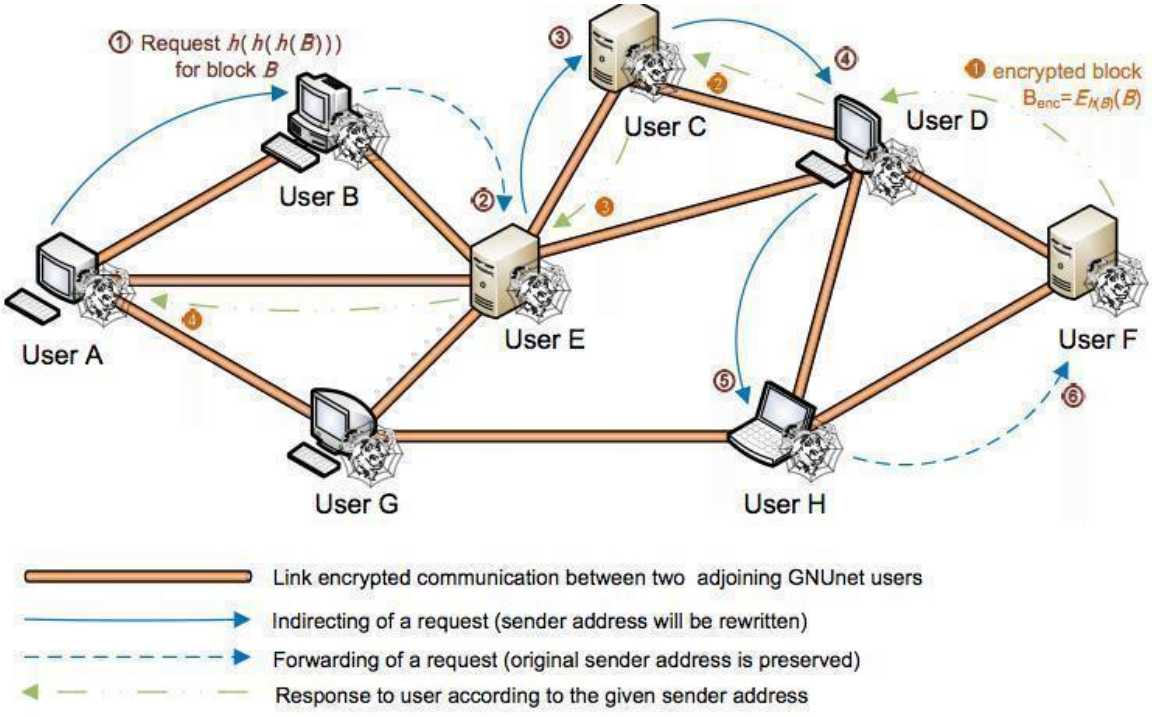
Připojení k síti Freenetu je možné ve dvou módech, v režimu *opennetu* a již zmiňovaném *darknetu*, který byl představen v roce 2008 s verzí 0.7 (Clarke

2010). V základním režimu opennetu je uživatel připojen skrze náhodně vybrané dostupné uzly v síti (další uživatele). Z pohledu anonymity je zajímavější připojení v takzvaném darknet režimu, který umožňuje manuální připojení pouze skrze uzly, kterým uživatel důvěřuje. Na základě toho je možné vytvořit si vlastní síť pro bezpečnou komunikaci, která je ještě více rezistentní k vnějším útokům.

4.3.3.4 GNUNet

GNUNet, jehož vývoj probíhá pod záštitou GNU („GNU's Not Unix!“) projektu a jeho filozofie svobodného a otevřeného softwaru je dalším pokusem o decentralizovanou síť s ohledem na bezpečnost a soukromí uživatele (GNU 2014). Ambice toho projektu reprezentuje citát současného vedoucího vývojáře Christiana Grothoffa: „*You broke the Internet. We're making ourselves a GNU one.*“ (Grothoff 2013).

Obrázek 6 Schéma fungování GNUNet (WP13 2007)



Prakticky funguje na velmi podobném principu jako Freenet a přestože je možné skrze GNUnet provozovat mnoho aplikací, v současné době převládá sdílení

dokumentů. Tomu nahrává i fakt, že vyhledávání podporuje booleovské operátory.

Celá síť se ale bohužel potýká s velkou odezvou vzhledem k ne příliš velké uživatelské základně.

Co se anonymity uživatelů týče, GNUnet seskupuje více požadavků do jedné větší pakety, pracuje s náhodným zpožděním, modifikuje pakety tak, aby byly všechny stejně velké a šifruje veškerý datový tok. V případě, že je uživatel nečinný, vytváří falešný provoz.

4.3.4 Virtuální měny

Dle definice Centrální evropské banky z roku 2012 je virtuální měnou rozuměn typ virtuálních peněz, zpravidla vydávaný a kontrolovaný svými vývojáři, který je používán a akceptován členy virtuálních komunit (Europen Central Bank 2012).

Do této široké definice spadá velké množství digitálních platidel. Od virtuálního zlata ve World of Warcraft přes kredity v rámci některých služeb až po kryptoměny, které v několika posledních letech zažívají velký nárůst popularity. Z hlediska anonymity na internetu jsou samozřejmě zajímavé právě kryptoměny v čele s Bitcoinem (Bitcoin 2014). Při úvahách o anonymním využití internetu v celé jeho šíři, tedy včetně provádění finančních transakcí, je nutné vzít tyto kryptoměny v potaz, neboť platba skrze platební kartu může v důsledku znamenat okamžitou ztrátu anonymity. Kryptoměny tak mohou znamenat vítanou alternativu k tradičním způsobům plateb na internetu.

4.3.4.1 Bitcoin

Bitcoin je internetová open-source peněžní měna, kterou lze platit prostřednictvím zcela decentralizované P2P sítě (Bitcoin 2014). Hlavní unikátnost Bitcoinu spočívá právě v jeho plné decentralizaci; je navržen tak, aby nikdo - autor ani jiní jednotlivci, skupiny či vlády – nemohl měnu jakkoliv ovlivňovat, ničit, padělat, zabavovat účty, kontrolovat peněžní toky nebo způsobovat inflaci. V síti neexistuje žádný centrální bod ani nikdo, kdo by mohl o síti rozhodovat. Na rozdíl

od ostatních dnešních měnových systémů nemá žádnou centrální autoritu, centrální banku, která by bitcoiny vydávala, spravovala a starala se o ně. Veškeré finanční operace probíhají v P2P síti a jsou chráněny silným šifrováním (Nakamoto 2008).

Bitcoin je deflační měna. Celkové množství peněz je konečné a předem známé, a jeho uvolňování do oběhu je definováno pouze matematickými zákony. V síti probíhají platby za minimální nebo žádné poplatky. Počátek této elektronické měny je datován do roku 2008, kdy byl představen v teoretické práci zveřejněné pod jménem Satoshi Nakamoto. Rok na to byl již představen funkční protokol a zveřejněn jeho kód. Tato měna je někdy označovaná jako elektronická obdoba hotovosti, z čehož se dají vyvodit její klady i zápory.

Na tvorbě této měny se podílí tzv. *mineři*, kteří tuto měnu v digitálním světě těží za pomoci výpočetního výkonu svého počítače, primárně pomocí své grafické karty, která je nejvíce vhodná pro dané výpočty. Zároveň je tato výpočetní síla využita k potvrzování uskutečněných transakcí ostatních uživatelů z důvodu předejití vícenásobným převodům již odeslaných peněz.

Navzdory celému konceptu decentralizace se tato měna nemůže vyhnout vlivům vnějšího světa a dle mnohých odborníků je snazší na ni nahlížet jako na komoditu raději než jako na měnu (Grinberg 2011). I další problémy pramení z neregulace a neregulovatelnosti tohoto prostředí. Mezi ně se řadí podvody a krádeže, a to mezi jednotlivými uživateli i ve vztahu k jednotlivým směnárnám.

I přes výše zmíněné problémy je Bitcoin z pohledu anonymity na internetu vítanou alternativou k tradičním měnám a svoji roli i díky vzrůstající popularitě plní velice dobře. V současné době je možné jej využít od nákupu služeb na internetu až po nákup nemovitostí (Kallgren 2014). Jak ukázaly některé experimenty, je možné pouze s platbami pomocí bitcoinu fungovat i v reálném světě – konkrétně v San Franciscu (Hill 2013) nebo New Yorku (Fowler 2014).

4.3.4.2 Zerocoin

Na základě Bitcoinu vzniklo mnoho dalších virtuálních měn, které se snaží jeho koncept vylepšit a nabídnout nové možnosti. Jedním z takových je i projekt Zerocoin, jehož cílem je ještě větší důraz na anonymitu uživatele při jeho používání.

Hlavní slabinu Bitcoinu vidí autoři Zerocoinu (Zerocoin 2014) ve veřejnosti všech plateb a jejich dohledatelnosti napříč historií a tím pádem i možné spojitelnosti s určitými osobami. Tomu lze zabránit i bez využití dalších nástaveb v samotném Bitcoinu za použití stejného principu jako v případě anonymních remailerů - přeposíláním platby skrze sérii mezičlánků. Tato metoda přináší mnoho rizik a tak Zerocoin, který funguje v rámci Bitcoin sítě, za pomoci další kryptografické vrstvy skrývá informace o původci, adresátovi i velikosti transakce (Miers 2014) a není možné tak najít spojitost mezi jednotlivými platbami.

4.4 Operační systémy

Vzhledem k tomu, že použití výše uvedených technologií je pro většinu běžných uživatelů technicky náročné a ošetření různých skulin v systému pro zachování opravdové anonymity skoro nemožné, je v současné době vyvíjeno několik operačních systémů, jejichž hlavním cílem je právě poskytnutí anonymity. Díky celkové robustnosti těchto systémů, u kterých je od počátku myšleno v první řadě na bezpečnost, jsou tyto systémy užívány i pokročilými uživateli jednoduše i proto, že (vyjma výše uvedených technologií, které v sobě často kombinují) nabízejí ještě něco navíc. Jejich přidaná hodnota se liší dle systému, respektive linuxové distribuce. To je dáno faktem, že skupina těchto operačních systémů je založena výhradně na Linuxu.

4.4.1 Tails (The Amnesic Incognito Live System)

Distribuce Tails, v současné době založená na systému Debian verze 6 (Squeeze), před několika týdny dosáhla milníku vydáním své verze 1.0 (Tails 2014a) a s verzí 1.1 počítá s přechodem celého systému na aktuálnější balíčky z Debianu verze 7 (Wheezy).

Tato distribuce se neinstaluje, ale přímo se spouští z externích paměťových médií (DVD nebo USB) v takzvaném *live* režimu. Sami autoři doporučují (Tails 2014b) systém zapsat na DVD, které díky své nezapisovatelné povaze zaručí, že nedojde ke změnám uvnitř systému, a tedy je bezpečnější. Oproti tomu je zapsání na USB disk pohodlnější a navíc dovolí vytvořit zašifrované persistentní (Tails 2013a) úložiště, na které je možné uložit dokumenty, konfigurační soubory a privátní klíče napříč relacemi.

Hned po prvním zavedení a dále při každém dalším systém vyzve k nastavení administrátorského hesla. Dále nabídne možnost využít takzvané *„Windows camouflage“* (Tails 2014c), tedy přizpůsobení vzhledu systému do podoby Windows XP pro menší nápadnost při použití například v internetových kavárnách. S již zmiňovanou verzí 1.0 přibyla možnost jedním kliknutím spoofovat (Tails 2014d) MAC adresu síťového adaptéru pro zabránění identifikace zařízení. Závěrečnou možností je pak síťové nastavení.

Veškerý tok dat mezi zařízením používající Tails a zbytkem internetu je realizován skrze Tor a veškeré pokusy o přímé spojení jsou striktně blokovány, jedinou výjimkou je možnost připojení do I2P sítě. Internetový prohlížeč IceWeasel, GNU odnož Firefoxu, je navíc nastaven tak, aby se jeho otisk shodoval (Tails 2014e) s klasickým Tor Browserem a nebylo tak snadné rozeznat tyto dva typy uživatelů, kteří sdílí stejnou množinu anonymity.

Tails není doporučeno provozovat ve virtuálním prostředí, přestože je to možné (Tails 2013b). Hlavním důvodem je, že mimo rizika spojená se samotným systémem vstupují v úvahu další rizika spojená s konkrétním virtualizačním softwarem a nakonec i hostitelským operačním systémem, na kterém zůstanou stopy po použití.

4.4.2 Whonix

Přestože je operační systém *Whonix* rovněž založen na Debianu v těsné provázanosti s Torem, je jeho koncept trochu odlišný a představuje zajímavou

alternativu k Tails (Whonix 2014). Hlavním prvkem tohoto systému je bezpečnost skrze izolaci celého systému, který se skládá ze dvou částí *Whonix Workstation* a *Whonix Gateway*, které je nutné provozovat na dvou oddělených virtuálních (nebo v ideálním případě nevirtuálních) strojích.

Díky tomuto zásadnímu prvku je systém odolný vůči prosáknutí IP adresy skrze pluginy, jakými jsou Adobe Flash nebo Java, které je možné bezpečně používat. Stejně tak dovoluje provozovat veškeré programy v kombinaci s Tor sítí, a to i v případě, že samotné programy nepodporují nastavení proxy.

Nevýhodou z pohledu anonymity může být to, že se tento systém standardně instaluje a i po vypnutí uchovává všechna data a metadata jako jsou cookies, pokud je uživatel sám nesmaže. Na druhou stranu je možné instalovat libovolné aplikace, které nemohou narušit síťovou bezpečnost systému.

V testovacím vydání nové verze systému byla implementována funkce přidávající další vrstvu ochrany, a to skrze možnost směrovat tok dat od uživatele přes VPN a až následně skrze Tor. V současné době je plně funkční možnost přidání proxy jako mezičlánku a v testovací fázi také skrze protokol SSH (Whonix 2014). Z praktického hlediska může tato funkce sloužit hlavně ke skrytí faktu, že uživatel používá Tor (respektive Whonix) před vlastním poskytovatelem připojení.

4.4.3 JonDo Live-DVD

Velice oblíbenou živou distribucí je také JonDo Live od tvůrců Java Anonymous Proxy (respektive JonDo). Tato distribuce je opět založena na Debianu spolu s uživatelským prostředím XFCE (JonDo 2014). Spolu s předkonfigurovanými nástroji pro fungování skrze JonDo (např. JonDo Browser) podporuje také Tor a Mixmaster remailer. Navíc obsahuje software Pond (Pond 2013) pro asynchronní komunikaci namísto klasického mailu. Tento program se snaží eliminovat nedostatky emailu, které má i při použití šifrování (např. přenosové informace). Všechny zprávy se navíc po týdnu samy smažou. JonDo Live je i po několika letech stále v aktivním vývoji a pomalu se blíží verze 1.0 (JonDo 2014).

5 Závěr

Tato bakalářská práce má několik dílčích cílů, a to poskytnout historický vhled do problematiky anonymity na internetu, porovnat mezi sebou výhody a nevýhody vystupování na internetu pod reálnou identitou v kontrastu s anonymitou a v praktické částí zmapovat v současnosti nejvíce využívané identifikační technologie a zanalyzovat soukromí podporující technologie, které v ideálním případě vedou k anonymitě na internetu.

Na začátku práce je definována anonymita obecně i ve vztahu k informačním technologiím. Následuje historický vývoj internetu ve vztahu k identifikačním technologiím a zhodnocení výhod a nevýhod užití reálné identity v kontrastu s anonymitou.

Další část práce se zabývá popisem a analýzou nejčastěji využívaných technologií sloužících k identifikaci uživatelů na internetu. Z této kapitoly je možné vyčíst trendy, ke kterým identifikační technologie směřují a na které se snaží technologie podporující soukromí včas reagovat. V globálním měřítku je hojně využíváno cookies k identifikaci uživatelů spolu s jejich IP adresami. Lze ale také pozorovat technologie fungující na principech website device fingerprintingu, které představují větší hrozbu pro soukromí uživatelů než cookies.

Nejobsáhlejší část práce je zaměřena na soukromí podporující technologie a jejich praktické využití. Struktura této kapitoly je zvolena s ohledem na komplexnost jednotlivých řešení od doplňků prohlížeče po celé operační systémy. Velký prostor je v této části věnován programu Tor, který je jedním ze stěžejních v tomto odvětví. Na jeho příkladu bylo možné jednak sledovat trendy v jeho vývoji, jednak pozorovat popularitu těchto nástrojů, která stále stoupá.

Otázka anonymity na internetu je velice komplexní záležitostí. Nelze jednoznačně vybrat jeden nástroj, který by uživateli poskytl anonymitu napříč spektrem všech služeb na internetu. Je nutné obezřetně volit konkrétní nástroje za konkrétním účelem.

Jistou míru anonymity například vůči komerčním reklamním systémům, které mohou využívat různé formy sledování uživatele, je možné dosáhnout relativně komfortní cestou instalací vhodných doplňků do webového prohlížeče. V případě, že si uživatel přeje skrýt svoji IP adresu (respektive svoji lokaci), může být vhodným řešením využití proxy či VPN od komerčních poskytovatelů.

Pro anonymitu v pravém slova smyslu je ovšem nutné zvolit technicky složitější a uživatelsky méně přívětivá řešení, která jsou za tímto účelem vyvíjena. Panuje obecná shoda, že Tor (nazývaný také jako král vysoce zabezpečené nízko latentní anonymity (The Guardian 2013)) stojí v čele těchto technologií. Za toto prvenství kromě samotných vývojářů vděčí i několika tisícům dobrovolníků provozujícím jednotlivé uzly, ze kterých je síť tvořena.

Další z výhod Toru je jeho dostupnost pro mobilní zařízení. Mimoto je základním kamenem pro několik samostatných linuxových distribucí. Právě celistvé operační systémy tohoto typu jsou v současnosti nejkomplexnějším řešením pro uživatele hledající anonymitu na internetu. Díky úzké spolupráci s vývojáři Toru a větší uživatelské přívětivosti, než jakou disponuje konkurenční systém Whonix, je v pomyslném čele operační systém TAILS.

Z této bakalářské práce vyplývá, že anonymita v prostředí internetu je velmi aktuálním tématem. V reakci na nasazení identifikačních technologií ze strany provozovatelů mnoha služeb se jejich uživatelé často uchylují k použití nástrojů pro zachování vlastní anonymity ve virtuálním prostoru. Osobně se domnívám, že prvek anonymity v prostředí internetu má nezastupitelnou roli a bylo by dobré jej do budoucna v určité formě zachovat.

Seznam použitých zdrojů

4Chan: Advertise. [online]. [cit. 2014-07-17]. Dostupné z: https://www.4chan.org/advertise

Adblock Plus [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://adblockplus.org/

ASSANGE, Julian, Jacob APPELBAUM, Andy MÜLLER-MAGUHN a Jérémie ZIMMERMANN. *Cypherpunks: freedom and the future of the internet*. London: OR Books, c2012, 186 p. ISBN 9781939293015-.

BERNERS-LEE, Tim. Information Management: A Proposal. *W3C* [online]. 1989 [cit. 2014-07-17]. Dostupné z: http://www.w3.org/History/1989/proposal.html

BOBBIO, Jeremy. Reproducible Builds. *Debian Wiki* [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://wiki.debian.org/ReproducibleBuilds

CISCO SYSTEMS, INC. How Virtual Private Networks Work. [online]. 2008 [cit. 2014-07-24]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

CLARKE, Ian. A Distributed Decentralised Information Storage and Retrieval System. [online]. 1999 [cit. 2014-07-24].

CLARKE, Ian, Oskar SANDBERG, Matthew TOSELAND a Vilhelm VERENDEL. Private Communication Through a Network of Trusted Connections: The Dark Freenet. [online]. 2010 [cit. 2014-07-24]. Dostupné z: https://freenetproject.org/papers/freenet-0.7.5-paper.pdf

DANEZIS, George, Roger DINGLEDINE a Nick MATHEWSON. Mixminion: Design of a Type III Anonymous Remailer Protocol. [online]. 2003 [cit. 2014-07-30]. Dostupné z: http://mixminion.net/minion-design.pdf

DAVIES, Caroline. Broadband firms urged to block sex websites to protect children. *The Guardian* [online]. 2010 [cit. 2014-07-17]. Dostupné z: http://www.theguardian.com/society/2010/dec/19/broadband-sex-safeguard-children-vaizey

DINGLEDINE, Roger. The lifecycle of a new relay. [online]. 2013 [cit. 2014-07-24]. Dostupné z: https://blog.torproject.org/blog/lifecycle-of-a-new-relay
DINGLEDINE, Roger. Recommended reject lines for relays affected by Heartbleed. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://lists.torproject.org/pipermail/tor-relays/2014-April/004362.html

DINGLEDINE, Roger. How to handle millions of new Tor clients. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients

DINGLEDINE, Roger, Nick MATHEWSON a Paul SYVERSON. Tor: The Second-Generation Onion Router. [online]. 2004 [cit. 2014-07-24]. Dostupné z: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

ECKERSLEY, Peter. How Unique Is Your Web Browser?. *Proceeding PETS'10 Proceedings of the 10th international conference on Privacy enhancing technologies* [online]. 2010, s. 1-18 [cit. 2014-07-24]. Dostupné z: https://panopticlick.eff.org/browser-uniqueness.pdf

ERNESTO. Which VPN Services Take Your Anonymity Seriously? 2014 Edition. [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/

FEDERRATH, Hannes. JAP. UNIVERSITY OF REGENSBURG. [online]. 2011 [cit. 2014-07-24]. Dostupné z: http://anon.inf.tu-dresden.de/index_en.html

FIFIELD, David, Nate HARDISON, Jonathan ELLITHORPE, Emily STARK, Dan BONEH, Roger DINGLEDINE a Phil PORRAS. Evading Censorship with Browser-Based Proxies. [online]. 2012, s. 239 [cit. 2014-07-24]. DOI: 10.1007/978-3-642-31680-7_13. Dostupné z: http://link.springer.com/10.1007/978-3-642-31680-7_13

FOWLER, Geoffrey. Bitcoin Experiment in Real Life: What to know about the virtual currency. [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://online.wsj.com/news/articles/SB10001424052702303491404579390971115008010

FREITAS, Nathan. GUARDIAN PROJECT. *Orbot* [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://guardianproject.info/apps/orbot/

GALPERIN. 2011 in Review: Nymwars. [online]. 2011 [cit. 2014-07-17]. Dostupné z: https://www.eff.org/deeplinks/2011/12/2011-review-nymwars

GOLDSCHLAG, David M., Michael G. REED a Paul F. SYVERSON. Hiding Routing information. [online]. 1996, s. 137 [cit. 2014-07-24]. DOI: 10.1007/3-540-61996-8_37. Dostupné z: http://link.springer.com/10.1007/3-540-61996-8_37

GRAHAM, Mark. Information Geographies: The anonymous Internet. OXFORD INTERNET INSTITUTE. [online]. [cit. 2014-07-24]. Dostupné z: http://geography.oii.ox.ac.uk/?page=tor

GRINBERG, Reuben. Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal*, [online]. 2011, Vol. 4 [cit. 2014-07-24]. Dostupné z: http://hstlj.org/wp-content/uploads/2011/12/8-Grinberg-159-208.pdf

GROTHOFF, Christian. You broke the Internet. We're making ourselves a GNU one. [online]. 2013 [cit. 2014-07-24]. Dostupné z: https://gnunet.org/internetistschuld

GUEYE, Bamba, Artur ZIVIANI, Mark CROVELLA a Serge FDIDA. Constraint-Based Geolocation of Internet Hosts. *IEEE/ACM Transactions on Networking* [online]. 2006, vol. 14, issue 6, s. 1219-1232 [cit. 2014-07-17]. DOI: 10.1109/TNET.2006.886332. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4032725

HAYNE, Stephen C. a Ronald E. RICE. Attribution accuracy when using anonymity in group support systems. *International Journal of Human-Computer Studies* [online]. 1997, vol. 47, issue 3, s. 429-452 [cit. 2014-07-17]. DOI: 10.1006/ijhc.1997.0134. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1071581997901348

HEIDERICH, Mario, Abraham ARANGUREN a Alex INFÜHR. Pentest-Report Onion Browser 04.2014. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://mike.tig.as/onionbrowser/onion-browser-cure53-security-audit-201404.pdf

HERRMANN, Dominik, Rolf WENDOLSKY a Hannes FEDERRATH. Website fingerprinting. *Proceedings of the 2009 ACM workshop on Cloud computing security - CCSW '09* [online]. New York, New York, USA: ACM Press, 2009, s. 31- [cit. 2014-07-24]. DOI: 10.1145/1655008.1655013. Dostupné z: http://portal.acm.org/citation.cfm?doid=1655008.1655013

HILL, Kashmir. 21 Things I Learned About Bitcoin From Living On It For A Week. [online]. 2013 [cit. 2014-07-24]. Dostupné z: http://www.forbes.com/sites/kashmirhill/2013/05/09/25-things-i-learned-about-bitcoin-from-living-on-it-for-a-week/

HOLIDAY, Josh. SXSW 2011: 4Chan founder Christopher Poole on anonymity and creativity. [online]. 2011 [cit. 2014-07-17]. Dostupné z: http://www.theguardian.com/technology/2011/mar/13/christopher-poole-4chan-sxsw-keynote-speech

HOWARD, Philip N a Muzammil M HUSSAIN. *Democracy's fourth wave?: digital media and the Arab Spring*. New York: Oxford University Press, c2013, xiv, 145 p. ISBN 978-019-9936-953.

CHAUM, David L. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM* [online]. 1981, vol. 24, issue 2, s. 84-90 [cit. 2014-07-24]. DOI: 10.1145/358549.358563. Dostupné z: http://portal.acm.org/citation.cfm?doid=358549.358563

CHENG, Zhiyuan, James CAVERLEE a Kyumin LEE. You are where you tweet. *Proceedings of the 19th ACM international conference on Information and knowledge management - CIKM '10* [online]. New York, New York, USA: ACM Press, 2010, s. 759- [cit. 2014-07-17]. DOI: 10.1145/1871437.1871535. Dostupné z: http://portal.acm.org/citation.cfm?doid=1871437.1871535

KADIANAKIS, George. Obsf3: Protocol Specification. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://gitweb.torproject.org/pluggable-transports/obfsproxy.git/blob/HEAD:/doc/obfs3/obfs3-protocol-spec.txt

KADIANAKIS, George. Obfs2: Protocol Specification. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://gitweb.torproject.org/pluggable-transports/obfsproxy.git/blob/HEAD:/doc/obfs2/obfs2-protocol-spec.txt

KALLGREN, Jona. New York Real-Estate Brokerage To Start Accepting Bitcoin. [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://www.coindesk.com/new-york-real-estate-accepting-bitcoin/

KANG, Ruogu, Stephanie BROWN a Sara KIESLER. Why do people seek anonymity on the internet?. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13* [online]. New York, New York, USA: ACM Press, 2013, s. 2657- [cit. 2014-07-17]. DOI: 10.1145/2470654.2481368. Dostupné z: http://dl.acm.org/citation.cfm?doid=2470654.2481368

KATZ-BASSETT, Ethan, John P. JOHN, Arvind KRISHNAMURTHY, David WETHERALL, Thomas ANDERSON a Yatin CHAWATHE. Towards IP geolocation using delay and topology measurements. *Proceedings of the 6th ACM SIGCOMM on Internet measurement - IMC '06* [online]. New York, New York, USA: ACM Press, 2006, s. 71- [cit. 2014-07-17]. DOI: 10.1145/1177080.1177090. Dostupné z: http://portal.acm.org/citation.cfm?doid=1177080.1177090

KOHUT, Andrew. Technology in the American household. *Times Mirror Center for The People & The Press* [online]. 1994 [cit. 2014-07-17]. Dostupné z: http://www.people-press.org/files/legacy-pdf/582.pdf

KOPSELL, Stefan, Rolf WENDOLSKY a Hannes FEDERRATH. Revocable Anonymity. [online]. 2006 [cit. 2014-07-24]. Dostupné z: http://anon.inf.tu-dresden.de/publications/KWF2006ETRICSRevocableAnonymity.pdf

KRISTOL, D. a MONTULLI. HTTP State Management Mechanism. [online]. 2000 [cit. 2014-07-17]. Dostupné z: http://tools.ietf.org/html/rfc2965
KRISTOL, David M. HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology* [online]. vol. 1, issue 2, s. 151-198 [cit. 2014-07-17]. DOI: 10.1145/502152.502153. Dostupné z: http://portal.acm.org/citation.cfm?doid=502152.502153

KRISTOL, David M. HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology* [online]. 2001, vol. 1, issue 2, s. 151-198 [cit. 2014-07-17]. DOI: 10.1145/502152.502153. Dostupné z: http://portal.acm.org/citation.cfm?doid=502152.502153

KUBIEZIE, Jens. To be or I2P: An introduction into anonymous communication with I2P. In: [online]. 2007 [cit. 2014-07-24]. Dostupné z: http://events.ccc.de/congress/2007/Fahrplan/attachments/1017_24c3-i2p.pdf

LEINER, Barry M., Vinton G. CERF, David D. CLARK, Robert E. KAHN, Leonard KLEINROCK, Daniel C. LYNCH, Jon POSTEL, Larry G. ROBERTS a Stephen

WOLFF. A brief history of the internet. *ACM SIGCOMM Computer Communication Review* [online]. 2009-10-07, vol. 39, issue 5, s. 22- [cit. 2014-07-17]. DOI: 10.1145/1629607.1629613. Dostupné z: http://portal.acm.org/citation.cfm?doid=1629607.1629613

LESSIG, Lawrence. *Code: version 2.0*. [2nd ed.]. New York: Basic Books, c2006, xvii, 410 p. ISBN 04-650-3914-6.

LICKLIDER, J. C. R. a Welden E. CLARK. On-line man-computer communication. *Proceedings of the May 1-3, 1962, spring joint computer conference on - AIEE-IRE '62 (Spring)* [online]. New York, New York, USA: ACM Press, 1962, s. 113- [cit. 2014-07-17]. DOI: 10.1145/1460833.1460847. Dostupné z: http://portal.acm.org/citation.cfm?doid=1460833.1460847

LOVECRUFT, Isis. BridgeDB. THE TOR PROJECT, Inc. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://bridges.torproject.org/

MADDEN, Mary a Aaron SMITH. Reputation Management and Social Media: How people monitor their identity and search for others online. [online]. 2010 [cit. 2014-07-17]. Dostupné z: http://www.pewinternet.org/2010/05/26/reputation-management-and-social-media/

MAHMUD, Jalal, Jeffrey NICHOLS a Clemens DREWS. Home Location Identification of Twitter Users. *ACM Transactions* [online]. 2014 [cit. 2014-07-17]. Dostupné z: http://arxiv.org/abs/1403.2345

MARX, Gary T. What's in a Name? Some Reflections on the Sociology of Anonymity. *The Information Society* [online]. 1999, vol. 15, issue 2, s. 99-112 [cit. 2014-07-17]. DOI: 10.1080/019722499128565. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/019722499128565

MAYER, Jonathan. Tracking the Trackers: Self-Help Tools. [online]. 2011 [cit. 2014-07-24]. Dostupné z: https://cyberlaw.stanford.edu/node/6730

MIERS, Ian, Christina GARMAN, Matthew GREEN a Aviel D. RUBIN. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

MILLER, Brad, Ling HUANG, A. D. JOSEPH a J. D. TYGAR. I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis. [online]. s. 143 [cit. 2014-07-24]. DOI: 10.1007/978-3-319-08506-7_8. Dostupné z: http://link.springer.com/10.1007/978-3-319-08506-7_8

MMPC. Sefnit's Tor botnet C&C details. *Malware Protection Center* [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://blogs.technet.com/b/mmpc/archive/2014/03/05/sefnit-s-tor-botnet-c-amp-c-details.aspx

MOELLER, U., L. COTTRELL, P. PALFRADER a L. SASSAMAN. Mixmaster Protocol Version 2. [online]. 2004 [cit. 2014-07-24]. Dostupné z: http://www.ietf.org/archive/id/draft-sassaman-mixmaster-03.txt

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [online]. 2008 [cit. 2014-07-24]. Dostupné z: https://bitcoin.org/bitcoin.pdf

NIKIFORAKIS, Nick, Alexandros KAPRAVELOS, Wouter JOOSEN, Christopher KRUEGEL, Frank PIESSENS a Giovanni VIGNA. Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting. *2013 IEEE Symposium on Security and Privacy* [online]. IEEE, 2013, s. 541-555 [cit. 2014-07-24]. DOI: 10.1109/SP.2013.43. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6547132

OLSON, Parmy. The man behind Silk Road – the internet's biggest market for illegal drugs. [online]. 2013 [cit. 2014-07-24]. Dostupné z: http://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht

PAGAN, Matt. List Of Services Blocking Tor. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://trac.torproject.org/projects/tor/wiki/org/doc/ListOfServicesBlockingTor

PERRY, Mike. Reduced Exit Policy. [online]. 2011 [cit. 2014-07-24]. Dostupné z: https://trac.torproject.org/projects/tor/wiki/doc/ReducedExitPolicy

PERRY, Mike. Deterministic Builds Part One: Cyberwar and Global Compromise. [online]. 2013 [cit. 2014-07-24]. Dostupné z: https://blog.torproject.org/blog/deterministic-builds-part-one-cyberwar-and-global-compromise

PERRY, Mike. Announcing Tor Browser Bundle 3.0alpha1. [online]. 2013 [cit. 2014-07-24]. Dostupné z: https://blog.torproject.org/blog/announcing-tor-browser-bundle-30alpha1

PERRY, Mike. Google Chrome Incognito Mode, Tor, and Fingerprinting. [online]. 2010 [cit. 2014-07-24]. Dostupné z: https://blog.torproject.org/blog/google-chrome-incognito-mode-tor-and-fingerprinting

PFITZMANN, Andreas a Marit KÖHNTOPP. Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology. *Designing Privacy Enhancing Technologies* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001-3-16, s. 1 [cit. 2014-07-17]. DOI: 10.1007/3-540-44702-4_1. Dostupné z: http://link.springer.com/10.1007/3-540-44702-4_1

PRIVACY BADGER. How is Privacy Badger different to Disconnect, Adblock Plus, Ghostery, and other blocking extensions?. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://www.eff.org/privacybadger#how_is_it_different

RAWLINSON, Kevin. Turkey blocks use of Twitter after prime minister attacks social media site. [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://www.theguardian.com/world/2014/mar/21/turkey-blocks-twitter-prime-minister

REED, M.G., P.F. SYVERSON a D.M. GOLDSCHLAG. Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications* [online]. 2006, vol. 16, issue 4, s. 482-494 [cit. 2014-07-17]. DOI: 10.1109/49.668972. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=668972

SALTZER, J. H., D. P. REED a D. D. CLARK. End-to-end arguments in system design. *ACM Transactions on Computer Systems* [online]. 1984, vol. 2, issue 4, s. 277-288 [cit. 2014-07-17]. DOI: 10.1145/357401.357402. Dostupné z: http://portal.acm.org/citation.cfm?doid=357401.357402

SOLTANI, Ashkan, Shannon CANTY, Quentin MAYO, Lauren THOMAS a Chris Jay HOOFNAGLE. Flash Cookies and Privacy. *SSRN Electronic Journal* [online]. s. - [cit. 2014-07-17]. DOI: 10.2139/ssrn.1446862. Dostupné z: http://www.ssrn.com/abstract=1446862

STEINER, Peter. On the Internet, nobody knows you're a dog. *The New Yorker magazine* [online]. 1993

SYVERSON, Paul. Onion Routing: Brief Selected History. [online]. 2005 [cit. 2014-07-24]. Dostupné z: http://www.onion-router.net/History.html

TIGAS, Mike. Onion Browser. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://mike.tig.as/onionbrowser/

TOR, Project. Tor: Sponsors. *Tor Project* [online]. 2014 [cit. 2014-07-17]. Dostupné z: https://www.torproject.org/about/sponsors.html.en

TURKLE, Sherry. *Life on the screen: identity in the age of the Internet*. New York: Simon, c1995, 347 s. ISBN 978-068-4833-484.

WARD, Mark. UK government tackles wrongly-blocked websites. *BBC News* [online]. 2014 [cit. 2014-07-17]. Dostupné z: http://www.bbc.com/news/technology-25962555

WINTER, Philipp, Tobias PULLS a Juergen FUSS. ScrambleSuit: A Polymorphic Network Protocol to Circumvent Censorship. *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society - WPES '13* [online]. New York, New York, USA: ACM Press, 2013, s. 213-224 [cit. 2014-07-24]. DOI: 10.1145/2517840.2517856. Dostupné z: http://dl.acm.org/citation.cfm?doid=2517840.2517856

WP13. D13.1: Identity and impact of privacy enhancing technologies. *Future of Identity in the Information Society* [online]. 2007 [cit. 2014-07-29]. Dostupné z: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp13-del13.1.identity_and_impact_PET.pdf

TLS heartbeat read overrun (CVE-2014-0160). *OpenSSL Security Advisory* [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://www.openssl.org/news/secadv_20140407.txt

Adblock Edge [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://addons.mozilla.org/cs/firefox/addon/adblock-edge/

Eletronic Frontier Foundation: Privacy Badger [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://www.eff.org/privacybadger

Self-Destructing Cookies [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://addons.mozilla.org/cs/firefox/addon/self-destructing-cookies/

Tor: ChangeLog. [online]. 2014d [cit. 2014-07-24]. Dostupné z: https://gitweb.torproject.org/tor.git?a=blob_plain;hb=HEAD;f=ChangeLog

Mozilla Firefox: ESR Overview. MOZILLA. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://www.mozilla.org/en-US/firefox/organizations/faq/

EFF: Quotes Collection. [online]. 2001 [cit. 2014-07-24]. Dostupné z: https://w2.eff.org/Misc/EFF/quotes.eff.txt

Tails: Choosing between burning a DVD and installing onto a USB stick or SD card. *Tails* [online]. 2014b [cit. 2014-07-24]. Dostupné z: https://tails.boum.org/doc/first_steps/media/index.en.html

Tails: Fingerprint. *Tails* [online]. 2014e [cit. 2014-07-24]. Dostupné z: https://tails.boum.org/contribute/design/#index4h1

POND. *Pond* [online]. 2013 [cit. 2014-07-24]. Dostupné z: https://pond.imperialviolet.org/

Wikipedia: Onion Routing. [online]. 2014 [cit. 2014-07-30]. Dostupné z: https://en.wikipedia.org/wiki/Onion_routing

Internet World Stats: Usage and Population Statistics [online]. 2014 [cit. 2014-07-17]. Dostupné z: http://www.internetworldstats.com/stats.htm

Wireshark [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://www.wireshark.org/

Disconnect [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://disconnect.me/

NoScript [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://noscript.net/

JonDo [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://anonymous-proxy-servers.net/en/jondo.html

GNUNet [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://gnunet.org/

Tails: Tails 1.0 is out. *Tails* [online]. 2014a [cit. 2014-07-24]. Dostupné z: https://tails.boum.org/news/version_1.0/index.en.html

Tails: MAC address spoofing. *Tails* [online]. 2014d [cit. 2014-07-24]. Dostupné z: https://tails.boum.org/doc/first_steps/startup_options/mac_spoofing/index.en.html

JonDo: Live-DVD [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://anonymous-proxy-servers.net/en/jondo-live-cd.html

I2P: Tunnel overview. [online]. 2014a [cit. 2014-07-29]. Dostupné z: https://geti2p.net/uk/docs/tunnels/implementation

Tor: A Childs Garden Of Pluggable Transports. [online]. 2014e [cit. 2014-07-30]. Dostupné z: https://trac.torproject.org/projects/tor/wiki/doc/AChildsGardenOfPluggableTransports

Enemies of the Internet. *Reporters Without Borders: For Freedom of Information* [online]. 2014 [cit. 2014-07-17]. Dostupné z: http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf

Cookies. EVROPSKÁ KOMISE. [online]. 2014 [cit. 2014-07-17]. Dostupné z: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

Twitter [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://twitter.com

Skype [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://www.skype.com/

Ghostery [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://www.ghostery.com/

HTTPS Everywhere [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://www.eff.org/Https-everywhere

Tor: Hidden Service Protocol. [online]. 2014e [cit. 2014-07-24]. Dostupné z: https://www.torproject.org/docs/hidden-services.html.en

I2P: Comparison of Tor and I2P. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://geti2p.net/en/comparison/tor

Bitcoin [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://bitcoin.org/

Tails: Windows camouflage. *Tails* [online]. 2014c [cit. 2014-07-24]. Dostupné z: https://tails.boum.org/doc/first_steps/startup_options/windows_camouflage/index.en.html

Tor: Metrics. [online]. 2014c [cit. 2014-07-30]. Dostupné z: https://metrics.torproject.org/

ELECTRONIC FRONTIER FOUNDATION. *Panopticlick* [online]. 2010 [cit. 2014-07-17]. Dostupné z: https://panopticlick.eff.org/

ALEXA INTERNET, Inc. *Alexa top 10 000 sites on the web* [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://www.alexa.com/topsites

Tor Project [online]. 2014a [cit. 2014-07-24]. Dostupné z: https://www.torproject.org/

I2P [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://geti2p.net/en/

Freenet: Freenet 0.7 applications. [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://freenetproject.org/tools.html

Virtual currency schemes. Frankfurt-on-Main: European Central Bank, 2012. ISBN 978-928-9908-627.

Tails: Persistence. *Tails* [online]. 2013a [cit. 2014-07-24]. Dostupné z: https://tails.boum.org/contribute/design/persistence/

Tails: Virtualization. *Tails* [online]. 2013b [cit. 2014-07-24]. Dostupné z: https://tails.boum.org/doc/advanced_topics/virtualization/index.en.html

JonDo: Changelog Live Cd [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://anonymous-proxy-servers.net/wiki/index.php/Changelog_livecd_en

Tor: Overview. [online]. 2014b [cit. 2014-07-30]. Dostupné z: https://www.torproject.org/about/overview

Whonix [online]. 2014 [cit. 2014-07-24]. Dostupné z: https://www.whonix.org

Zerocoin [online]. 2014 [cit. 2014-07-24]. Dostupné z: http://zerocoin.org/

Seznam tabulek

Seznam grafů

Seznam obrázků

Seznam zkratek

NCP	Network Control Program
TCP	Transmission Control Protocol
IP	Internet Protocol
FTP	File Transfer Protocol
DNS	Domain Name System
ARPA	Advanced Research Projects Agency
DARPA	Defense Advanced Research Projects Agency
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
NAT	Network Address Translation
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IETF	Internet Engineering Task Force
EFF	Eletronic Frontier Foundation
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
SMTP	Simple Mail Transfer Protocol
JAP	Java Anon Proxy
TOR	The Onion Router
P2P	Peer-to-peer
DDoS	Distributed Denial of Service
ESR	Extended Support Release
I2P	The Invisible Internet Project
GNU	GNU's Not Unix!
TAILS	The Amnesic Incognito Live System
SSH	Secure Shell