Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Možnosti eliminácie cenzúry na internete

Bakalárska práca

2014
Marek Čačko

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Možnosti eliminácie cenzúry na internete

Bakalárska práca

Študijný program: Informatika
Študijný odbor: 2508 Informatika
Školiace pracovisko: Katedra Informatiky FMFI
Vedúci práce: RNDr. Michal Rjaško PhD.

Bratislava, 2014
Marek Čačko

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Marek Čačko
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: 9.2.1. informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský

Názov: Možnosti eliminácie cenzúry na internete
Possibilities of evading internet censorship

Cieľ: Preskúmať možnosť a navrhnúť, prípadne implementovať, riešenia na elemináciu cenzúry na internete.

Vedúci: RNDr. Michal Rjaško, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: doc. RNDr. Daniel Olejár, PhD.

Dátum zadania: 30.10.2013

Dátum schválenia: 30.10.2013 doc. RNDr. Daniel Olejár, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Abstrakt

V tejto práci vysvetlíme ako funguje cenzúra na internete a popíšeme kľúčové vlastnosti najznámejších nástrojov na jej obchádzanie. Tieto nástroje sú Proxy server, VPN, Dust, Telex, Freenet a Tor. V práci taktiež navrhneme naše vlastné riešenie na obchádzanie cenzúry a popíšeme, ako by sme ho implementovali.

Kľúčové slová: internetová cenzúra, obchádzanie cenzúry, internet

Abstract

In this thesis we explain how internet censorship works and describe key features of the best-known tools to circumvent internet censorship. These tools are Proxy server, VPN, Dust, Telex, Freenet and Tor. In this thesis we also design our own solution designed to internet censorship circumvention and describe how we would implement it.

Keywords: internet censorship, censorship circumvention, internet

Obsah

Zoznam obrázkov

Úvod

Kontrola a obmedzovanie názorov existovali vždy, no postupne, ako sa menil spôsob šírenia informácií medzi ľuďmi, tak sa upravovala aj forma ich kontroly. Po vynájdení kníhtlače sa začali zakazovať prvé knihy. Následne, ako sa začali rozširovať noviny, tak začal byť kontrolovaný aj ich obsah. Rovnako aj rozhlasové či televízne vysielanie začali byť krátko po svojom vzniku pod kontrolou. A rovnaký osud postretol aj internet.

Keď bol internet ešte nová technológia, tak fungoval bez regulácií obsahu a bol na ňom slobodný prístup ku ľubovoľným informáciám. Mnohí ľudia v tom čase vyhlasovali, že internet, vďaka spôsobu, ako funguje, zostane jediným médiom, ktoré nikdy nebude môcť byť pod kontrolou cenzúry. Spočiatku to aj platilo, pretože pre cenzora, ktorý dovtedy kontroloval všetko ostatné, bol internet niečo úplne nové, s čím nedokázal účinne pracovať. V priebehu rokov, ho však aj vďaka rôznym legislatívnym zásahom dostal pod kontrolu. Počet krajín, kde je prístup k internetovému obsahu nejakým spôsobom blokovaný a filtrovaný, neustále narastá. Internet postupne prestáva byť slobodné médium, a preto je dôležité sa snažiť tento fakt zmeniť, alebo aspoň internet pomocou rôznych technológií k slobodnému médiu čo najviac priblížiť.

Táto práca pozostáva zo štyroch kapitol. V prvej kapitole uvedieme základné informácie o internetovej cenzúre, spôsobe jej fungovania a použitia a taktiež informácie o jej súčasnom rozšírení vo svete. V nasledujúcej kapitole, postupne predstavíme niektoré nástroje určené na jej obchádzanie, a to postupne: Proxy server, VPN, Telex, Tor, Freenet a Dust. Pri týchto riešeniach uvedieme ich kľúčové vlastnosti, spôsoby použitia a aj ich rôzne nedostatky či slabiny. V tretej kapitole navrhneme naše vlastné riešenie, ktoré by dokázalo obchádzať cenzúru na internete. V poslednej, štvrtej, kapitole popíšeme, ako by sme v tomto našom návrhu riešili rôzny problémy a ako by sme ho implementovali.

KAPITOLA 1

Cenzúra na internete

Cenzúra na internete je ovládanie, prípadne potláčanie toho, čo smie alebo nesmie byť na internete prístupné a publikované. Môže byť praktizovaná buď samotnou vládou alebo aj rôznymi súkromnými subjektami, ako sú napríklad poskytovatelia internetového pripojenia, webhostingové spoločnosti, prípadne správcovia rôznych internetových služieb. Toto sa deje či už na príkaz vlády, alebo z ich vlastného podnetu. Napríklad keď zistia, že spôsob akým sa využívajú ich služby porušuje ich vlastné podmienky používania alebo je dokonca protizákonný. Cenzúra sa však zvykne uplatňovať aj vo firmách, keď chce zamestnávateľ napríklad zamedziť zamestnancom prístup na stránky, ktoré nesúvisia s ich pracovnou náplňou a hrozilo by, že by ich rozptyľovali pri práci, prípadne aby im zabránil vo vynášaní citlivých údajov mimo firemnú sieť. Internetová cenzúra sa ďalej vyskytuje aj v školách, knižniciach či internetových kaviarniach.

Keďže cenzor väčšinou nemá nad celou sieťou absolútnu kontrolu, na rozdiel od štátov, kde je potláčaná osobná sloboda ako napríklad v Severnej Kórei, dosiahnutie úplnej cenzúry je veľmi náročné ak nie dokonca nemožné. To z dôvodu, že aj keď napríklad cenzor na smerovačoch na národnej úrovni vo svojej krajine zakáže prístup na určité IP adresy, vďaka čomu je k týmto adresám priame pripojenie z tejto krajiny nemožné, tak ak existuje prístup aspoň na jednu IP adresu, ktorá sa nachádza mimo tejto cenzurovanej siete, tak je možné cez túto IP adresu cenzúru účinne obísť a dostať sa tak ku blokovanému obsahu. Takýto prístup využívania prostredníka, ku ktorému nie je obmedzené pripojenie a z ktorého sa následne dá dostať na blokovaný server sa používa v takmer každom riešení, ktoré je určené na obchádzanie cenzúry. Tieto riešenia sa opierajú o fakt, že internetová cenzúra funguje na princípe čiernych zoznamov a teda všetko čo nie je zakázané, je povolené. Ak by to totiž fungovalo naopak, a celý systém by sa zmenil tak, že by cenzúra fungovala na báze bielych zoznamov a teda by existoval len zoznam IP adries, ku ktorým by bol povolený prístup a všetky ostatné IP adresy by neboli povolené, tak by situácia bola oveľa náročnejšia. To z toho dôvodu, že povolené adresy by boli s najväčšou pravdepodobnosťou pod kontrolou

cenzora a teda by sa na obchádzaní cenzúry nepodieľali. Naštastie však firewally filtrujúce internetovú prevádzku vo väčšine prípadov fungujú na báze čiernych zoznamov a teda cenzúra na internete sa dá aj naďalej účinne eliminovať. Tu nastáva otázka, prečo keď je cenzúra na internete pri súčastnom modeli fungovania prekonateľná, tak prečo sa na biele zoznamy neprešlo. Dôvodom sú peniaze a konkurencieschopnosť. Internet sa totiž stal nenahraditeľným ekonomickým nástrojom, využívaným v každej sfére natoľko, že ak chce krajina fungovať a prosperovať, tak internet potrebuje a takáto zmena by internet ako taký zničila. A však internetová cenzúra funguje stále spoľahlivo, pretože aj keď mnohé funkčné riešenia na jej obchádzanie existujú, tak tieto riešenia sú často krát použiteľné len pre technicky zdatných používateľov, ktorí im rozumejú a vedia ako ich správne použiť.

Tieto riešenia sa však neustále vyvíjajú a informácie o ich existencii sa postupne dostávajú do povedomia bežných ľudí. Avšak súčasne ako sa zlepšujú riešenia na obchádzanie cenzúry, tak rovnako napreduje aj druhá strana v riešeniach, ako čo najefektívnejšie a najúčinnejšie internet cenzurovať. Ide o boj medzi dvoma stranami, kde však má cenzor väčšinou "navrch". Predovšetkým z toho dôvodu, že kým riešenia na filtrovanie a blokovanie internetovej prevádzky vyvíjajú veľké softvérové a hardverové spoločnosti častokrát priamo financované rôznymi vládami tak na druhej strane frontu sú väčšinou len nadšenci a rôzne organizácie, ktoré to nerobia za účelom zisku a teda finančné prostriedky a kapacity oboch strán sú diametrálne odlišné. Veľká výhoda na strane cenzora je aj fakt, že legislatíva je väčšinou na jeho strane a ak potrebuje dosiahnuť väčšiu kontrolu, tak to vie častokrát dosiahnuť.

1.1 Metódy cenzúry

Jeden z hlavných rozdieľov medzi cenzúrou na internete a cenzúrou v tradičných médiach ako sú noviny, rádio, či televízia je v tom, že hranice krajiny sú na internete jednoduchšie prekonateľné a teda, ak aj cenzor v celej krajina zakáže publikovanie určitej informácie, tak stále je k nej vďaka povahe internetu možné pristupovať zo zdrojov, ak samozrejme existujú, ktoré sa nachádzajú mimo tejto krajiny a nepodliehajú cenzúre. Ak chcel teda cenzor účinne filtrovať aj informácie na internete tak sa musel naučiť pracovať tak, aby zabránil prístupu k informáciám, ku ktorým nemal fyzický prístup a ani nad nimi nemal legálnu kontrolu.

Prvé firewally, ktoré blokovali a filtrovali internetovú prevádzku fungovali na báze SPI (Shalow Packet Inspection), čo znamená, že sa kontrolovali len hlavičky paketov. V nich sa sledovalo či sa ich počiatočá IP adresa, cieľová IP adresa alebo port nenachádzal na čiernom zozname, ktorý bol väčšinou statický. Ak sa žiadna zhoda nenašla, tak bol tento paket odoslaný požadovaným smerom, no ak sa však našla, tak bol zahodený a prípadne mohli byť vyvodené ďalšie dôsledky. Takéto riešenie nebolo náročné na výkon, pretože tieto údaje bolo potrebné pri smerovaní paketu aj tak pozrieť, aby sa určilo, kam bolo treba paket ďalej poslať. Pri takomto jednoduchom systéme sa firewall vždy zaoberal len jednotlivými

paketmi a nemal žiadnu komplexnú informáciu o tom, k akej komunikácii tieto pakety patria. Takéto riešenia sa väčšinou dali obchádzať pomerne jednoducho.

Postupne, ako však začal narastať výpočtový výkon, tak sa pre firewally začali otvárať mnohé nové možnosti, ktoré si pred tým nemohli dovoliť. Statické čierne zoznamy sa začali stávať čoraz viac dynamickými, firewally si mohli udržiavať prehľad o konkrétnych komunikáciach, ktoré cez ne prechádzali a pri filtrovaný paketov sa prešlo z SPI na DPI (Deep Packet Inspection), čo znamená, že sa začal kontrolovať okrem hlavičiek paketov aj ich obsah. Pri takomto kontrolovaní paketov sa kontrolujú všetky údaje, ktoré nie sú šifrované, sleduje sa dĺžka paketov a všetky ostatné údaje, ktoré sa dajú z paketov zistiť. Vďaka tomuto dokáže firewall blokovať komunikáciu aj podľa protokolov, dokonca aj keď sa jedná o šifrovanú komunikáciu, ako je napríklad SSL/TLS. To z toho dôvodu, že tieto protokoly sú väčšinou identifikovateľné podľa nejakého odtlačku. Napríklad, keď spomínané SSL/TLS pri dohadovaní šifry a výmene kľúčov používa nešifrovanú komunikáciu a teda sa dá odpozorovať, že medzi týmito dvomi IP adresami, ktoré sa dohadujú, vznikne čoskoro šifrované SSL/TLS spojenie.

Avšak rovnako, ako sa zvýšil výkon, tak sa zväčšil aj obsah dát prenášaných po sieti a tak stále nie je možné súčastne pri smerovaní paketov aj detailne kontrolovať celú komunikáciu. Takáto kontrola sa teda zvyčajne vykonáva len na vzorkách paketov, alebo sa paket cez systém pustí, no jeho kópia sa odosiela aj na neskoršiu analýzu do výpočtového strediska určeného na analýzu paketov. Pri tejto analýze, keď sa príde na to, že tento paket obsahuje niečo "zlé"tak sa toto zistenie zohľadní pri kontrole ďalšej komunikácie, kedy už takýto paket bude zablokovaný.

Na dosahovanie cenzúry internetového obsahu existujú viaceré metódy, ktoré môžu byť technického charakteru, ale môžu byť aj netechnické. Medzi metódy technického charakteru patria napríklad:

Blokovanie IP adries

Pomocou zoznamu alebo rozsahu IP adries sa blokuje priamy prístup k týmto adresám a týmto sa stávajú v rámci celej cenzúrovanej siete nedostupné.

Filtrovanie DNS

Blokovované domény sa neprekladajú na IP adresy, a preto sa k nim nedá pristupovať cez ich názov. V horšom prípade, môže byť požiadavka na skutočný DNS server presmerovaná na upravený DNS server, ktorý je súčasťou systému na filtrovanie dátovej komunikácie a ktorý vracia inú IP adresu ako je skutočná IP adresa požadovanej stránky, a teda presmerúvava pripojenie na inú adresu.

Filtrovanie paketov podľa obsahu

Pri kontrolovaní obsahu paketov, za predpokladu, že sa nejedná o šifrovanú komunikáciu, a v paketoch sa nachádza čistý text, sa sleduje, či paket neobsahuje rôzne zakázané

slová. Ak ide o šifrovanú komunikáciu, tak sa firewall snaží podľa nešifrovaných častí paketu, veľkosti a priebehu komunikácie určiť, v akom protokole by sa mohla komunikácia odohrávať. Na základe týchto informácii sa firewall rozhoduje, či danú komunikáciu nepreruší. Pri TCP pripojení sa toto môže diať tak, že firewall odošle na IP adresu používateľa paket so žiadosťou na prerušenie spojenia, ktorý vyzerá ako by pochádzal od servera, s ktorým klient komunikuje a ten, keď mu takýto paket príde, nevie zistiť, že sa nejedná o skutočnú požiadavku od servera a komunikáciu ukončí.

Útoky na počítačové siete

Systémy, ktoré slúžia na obchádzanie cenzúry a ktoré sú používané vo väčšom rozsahu sa stávajú terčom rôznych útokov na ich infraštruktúru napríklad pomocou DoS útokov.

Odstraňovanie výsledkov pri vyhľadávaní

Rôzne vyhľadávače môžu z výsledkov vyraďovať záznamy, ktoré nechcú používateľom vrátiť. Jedná sa napríklad o situácie, keď sa používateľ snaží pristupovať k údajom, ktoré sú v jeho krajine zakázané, tak aby firma prevádzkujúca tento vyhľadávač neporušila zákon, takéto výsledky odstraňuje.

K cenzúre na internete patria aj rôzne netechnické metódy, ktorých obchádzanie je oveľa náročnejšie. Ide napríklad o zabavovanie IP adries, domén alebo celého hardvéru, vďaka rôznym žalobám zo strany právnikov alebo pri zásahoch polície. Medzi známe prípady spadajúce do tejto kategórie patrí napríklad Megaupload, ktorý bol po obvinení z hostovania a šírenia nelegálneho obsahu zablokovaný, vypnutý a následne mu bol zabavený všetok hardvér. Ďalším z prípadov, je webová stránka The Pirate Bay, ktorá často presúva svoj hardvér a doménu, zo strachu, aby oň neprišla. Napríklad v roku 2013 sa serveri The Pirate Bay presunuli postupne z Grónska, na Island a potom na ostrov Svätý Martin v Karibskom mori. V decembri v roku 2013 doména prešla postupne z .ac (ostrov Ascension v strede Atlantiku), .sx (Svatý Martin), .pe (Peru), .gy (Guyana) a momentálne je na .se (Švédsko) [9].

1.2 Cenzúra vo svete

Rozsah cenzúry je v každej krajine iný. Vo väčšine rozvinutých krajín je prítomná iba mierna alebo dokonca skoro žiadna forma cenzúry, v menej rozvinutých krajinách prevažne s diktátorským režimom je však uplatňovaná v oveľa väčšom rozsahu. Kým v rozvinutých krajinách sa cenzúra väčšinou týka len rôznych morálnych noriem a nelegálnych aktivít, tak v menej rozvinutých krajinách sa zachádza ďalej a je blokovaný slobodný prístup k informáciam predovšetkým zo zahraničia, ktoré majú na niektoré veci iný názor, ako je ten všeobecné uznávaný a šírený v krajine, a je potláčaná komunikácia medzi občanmi, predovšetkým počas rôznych udalostí ako sú voľby, protesty či vzbury.

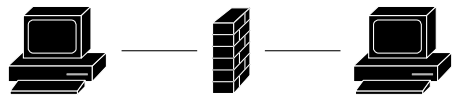
Medzi krajiny s celoštátnym firewallom a s najväčšou formou blokovania a filtrovania patria napríklad krajiny strednej a východnej Ázie, krajiny na strednom východe a v severnej Afrike. Od roku 2006 začala mimovládna orgranizácia Reportéri bez hraníc zostavovať zoznam "nepriateľov internetu". Podľa poslednej správy z roku 2014 [8] z dôvodu cenzurovania internetu patria do tohto zoznamu krajiny: Bahrajn, Bielorusko, Čína, Etiópia, Irán, Kuba, Pakistan, Ruská Federácia, Saudská Arábia, Severná Kórea, Spojené Arabské Emiráty, Sudán, Sýria, Turkménsko, Uzbekistan a Vietnam. Ale taktiež zaviedla zoznam krajín, ktoré sú pre rožširovanie cenzúry pod dohľadom a sem patria aj štáty ako napríklad Francúzsko či Austrália. V ostatných oblastiach sveta sa však tiež v nejakej miere vyskytuje cenzúra. Dokonca aj v demokratických krajinách so silnou podporou slobody prejavu a tlače. Napríklad v Nemecku a vo Francúzsku sú blokované stránky s nacistickou tématikou.

Motívy zavedenia cenzúry sú rôzne. Môže ísť napríklad o politické dôvody keď sa vláda snaží udržať svoju moc a potláčať názory opozície. Tiež môže ísť o rôzne morálne normy a protizákonné aktivity ako sú materiály podporujúce nenávisť, násilie, rasizmus, homofóbiu alebo detskú pornografiu. Blokovanie môže nastávať aj z bezpečnostných dôvodov, keď ide o blokovanie obsahu obsahujúceho rôzny malvér. Blokovanie z bezpečnostných dôvodov nastáva aj v záujme obrany krajiny, ako napríklad v Južnej Kórei sú blokované stránky podporujúce Severnú Kóreu. Ďalším z dôvodov blokovania je ochrana ekonomických záujmov, keď sa blokujú rôzne služby, ktoré slúžia napríklad na prístup k nelegálnemu obsahu ako sú filmy a hudba.

KAPITOLA 2

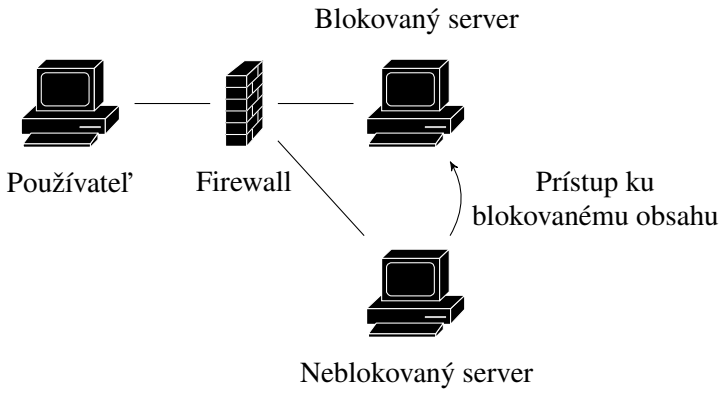
Obchádzanie cenzúry

V súčastnosti existujú mnohé riešenia, ktoré sa používajú na obchádzanie internetovej cenzúry a na prístup ku filtrovanému obsahu. Toto obchádzanie je možné predovšetkým vďaka faktu, že ako je znázornené na obrázku 2.1, tak blokovanie a filtrovanie pre cenzora neželaný obsah nedokáže z internetu odstrániť, a teda k nemu len zamedzuje priamy prístup.



Obr. 2.1: Blokovanie prístupu na server

Spôsob, ako je možné pristupovať ku cenzurovanému obsahu spočíva v tom, že keď je priama cesta ku požadovaným materiálom blokovaná, tak je potrebné k tomuto obsahu nájsť odlišnú cestu. Ako je znázornené na obrázku 2.2 tak častokrát, je obchádzanie internetovej cenzúry riešené v podstate jednoduchým spôsobom. Používateľ totiž zo svojho lokálneho počítača šifrovane komunikuje cez iný počítač, ktorý sa nachádza v inej sieti, ktorá však už nie je filtrovaná a z ktorej je teda cenzurovaný materiál voľne prístupný.



Obr. 2.2: Obchádzanie blokovania prístupu na server

Táto komunikácia musí byť šifrovaná z toho dôvodu, že ak by nebola, tak by firewall videl o akú komunikáciu sa používateľ snaží a vedel by z nej jednoducho prečítať, že chce pristupovať k cenzurovaným informáciám, a tak by túto komunikáciu zablokoval. Komunikácia cez iný počítač však obsahuje jeden slabý bod, ktorý je prítomný v skoro každom riešení a to ten, že používateľ nevie overiť, či stránka, ktorú požadoval je naozaj tá, ktorú mu počítač, s ktorým komunikuje aj vrátil a či nie je upravená alebo dokonca úplne iná. Pretože tento počítač, ktorý sa snaží používateľ využiť na obchádzanie cenzúry v skutočnosti nemusí slúžiť na jej obchádzanie, ale môže byť priamo súčasťou systému na filtrovanie komunikácie. Prípadne, môže tento počítač slúžiť na to aby škodil menením obsahu alebo vrátený obsah upravoval vo svôj vlastný prospech. Všetky riešenia na obchádzanie cenzúry sú teda založené na dôvere používateľov v to, že slúžia len a len na obchádzanie cenzúry a okrem tohto účelu nezasahujú do komunikácie žiadnym nevhodným spôsobom. Takýto pohľad však nie je ničím prekvapivým, keďže v podstate celý internet funguje spôsobom, že používatelia predpokladajú, že to, čo sa im na nejakú ich požiadavku vráti je naozaj to, čo aj požadovali. A nad tým, že to tak byť nemusí, sa väčšina ľudí ani nepozastaví. Vieme však, že vrátená odpoveď byť upravená môže, keďže môže byť napríklad cenzurovaná.

Skoro všetky riešenia slúžiace na obchádzanie cenzúry na internete by sa dali rozdeliť na dve skupiny. Do prvej skupiny by sa dali zaradiť riešenia, ktoré fungujú na báze prostredníka, ktorý presmeruváva komunikáciu, zo servera alebo siete, ku ktorej má používateľ prístup na cenzurovaný server. Príklad takéhoto riešenia je proxy server. Druhá veľká skupina obsahuje rôzne distribuované P2P siete, alebo siete fungujúce na spôsobe postupného preposielania požiadaviek cez viacero uzlov. Do tejto kategórie patria napríklad riešenia ako sú Tor a Freenet. Zvyšné riešenia sa do týchto dvoch skupín zaradiť nedajú, pretože fungujú na inom princípe, alebo sú to len rôzne špecifické protokoly napríklad na utajenie komunikácie.

Nástrojov na obchádzanie cenzúry je mnoho, pričom niektoré majú len špecifické použitie na určitú formu cenzúry v určitej krajine, no niektoré nástroje sú komplexné a dajú sa využiť vo väčšine prípadov. Rôznia sa v spôsobe, jednoduchosti použitia, rýchlosti, bezpečnosti a rizika odhalenia. Spraviť nástroj, ktorý by bol súčastne aj veľmi rýchly aj bezpečný, alebo aby bol jednoduchý na použitie a súčastne, aby odhalenie jeho použitia bolo náročné je pomerne ťažké, pretože tieto vlastnosti idú častokrát proti sebe. Totiž, aby bol nástroj bezpečný, tak jeho komunikácia musí byť napríklad nejakým spôsobom šifrovaná, prípadne prechádza cez viacero počítačov, ktoré majú čo sa rýchlosti a kvality týka veľmi rôznorodé pripojenie na internet, a takýmto spôsobom sa prenášané dáta nafukujú a rýchlosť linky klesá, čoho dôsledkom je, že oproti komunikácii bez tohto nástroja je možné za rovnakú jednotku času preniesť výrazne viac dát. Použitie mnohých nástrojov, ktoré patria medzi tie rozšírenejšie a používanejšie predovšetkým pre svoju jednoduchosť sa dá ľahšie odhaliť, pretože firewall sa s nimi častejšie stretáva. Takéto nástroje sa buď firewall postupne naučí identifikovať, prípadne sa stávajú častým terčom rôznych útokov.

Obchádzanie cenzúry na internete má však aj svoje riziká. Veľkosť takéhoto rizika závisí od toho, kde sa používateľ snaží cenzúru obchádzať, pretože napríklad v práci to môže znamenať okamžitú výpoveď, v škole vyhodenie zo školy. No situácia môže byť horšia, keďže v mnohých krajinách, kde je obsah na internete cenzurovaný je aj jej obchádzanie postihované zákonom. Forma trestu závisí od konkrétnej krajiny, no v niektorých krajinách sa obchádzanie cenzúry trestá až väzením.

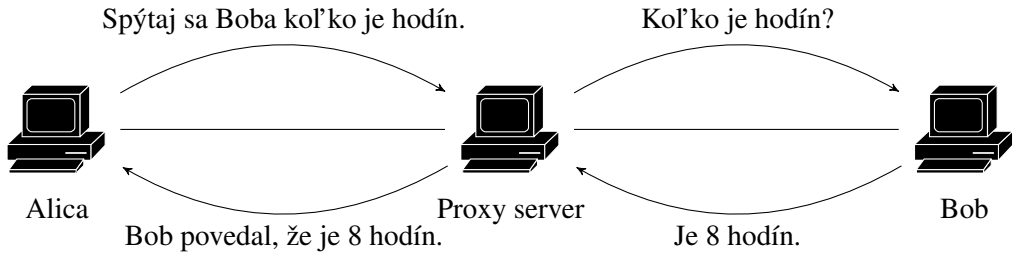
V nasledujúcej časti práce sa nachádza popis fungovania šiestich riešení na obchádzanie cenzúry: proxy server, VPN, Telex, Tor, Freenet a Dust. Tieto riešenia sme si vybrali preto, lebo patria medzi najpoužívanejšie alebo sú nejakým spôsobom inovatívne a odkazujeme sa na ne v našom návrhu.

2.1 Riešenia na báze prostredníka

Riešenia popisované v tejto časti, sú založené na úlohe prostredníka, ktorého úlohou je presmerovať požiadavku. Pri ich použití totiž používateľ, ktorý ma zamedzený prístup k určitému serveru, využije takéhoto prostredníka a pomocou neho komunikuje so serverom, ku ktorému nemá priamy prístup. Táto forma komunikácia môže byť buď preposielaním požiadaviek alebo napríklad pomocou vytvoreného tunela.

2.1.1 Proxy server

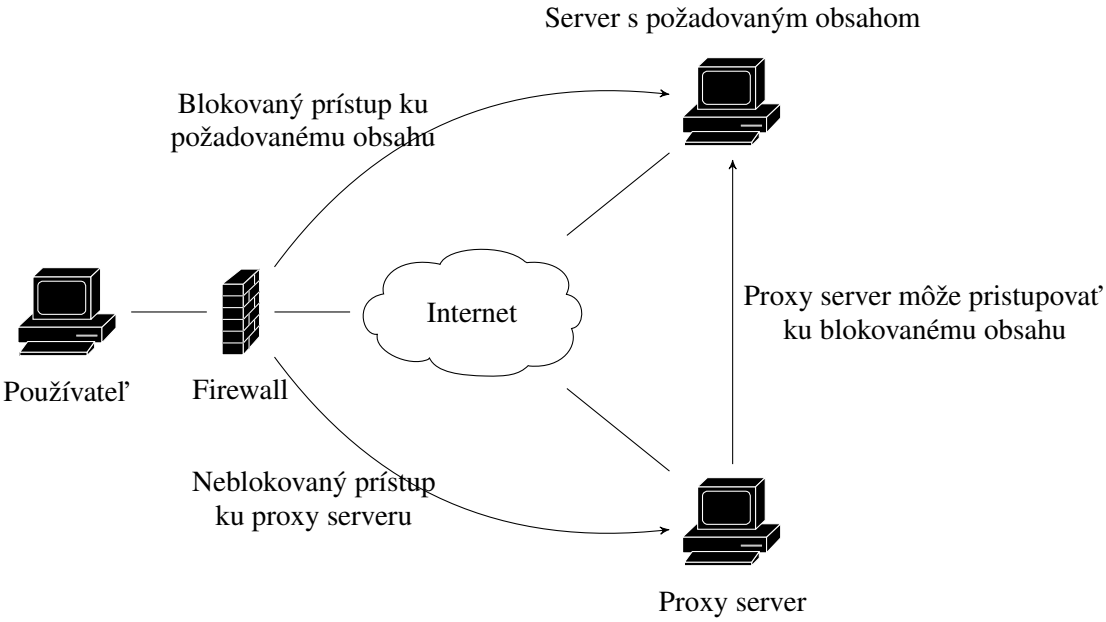
Toto riešenie patrí medzi najjednoduchšie nástroje používané na prístup k obsahu, ku ktorému je priamy prístup blokovaný a je základom mnohých ďalších riešení. Proxy server má však aj mnohé iné využitie okrem toho, že sa používa na prístup ku filtrovaným materiálom. Používa sa napríklad na rôzne kešovanie dát, preklady webových stránok, ale aj na odpočúvanie komunikácie či filtrovanie obsahu. Jeho fungovanie je znázornené na obrázku 2.3.



Obr. 2.3: Fungovanie proxy servera

Keď sa chce Alica niečo spýtať Boba, tak sa ho to nespýta priamo, ale využije na to proxy server. Teda, keď napríklad chce Alica vedieť, aký je aktuálny čas, tak namiesto toho, aby sama oslovila Boba a spýtala sa ho, aký je aktuálny čas, tak povie proxy serveru, aby sa on spýtal Boba, aký je aktuálny čas a nech jej potom povie, čo zistil. Proxy server sa teda Boba

spýta, aký je aktuálny čas, Bob mu odpovie, že je 8 hodín a následne proxy server povie Alici, že mu Bob povedal, že je 8 hodín. Bob z tejto komunikácie nevie zistiť, že v skutočnosti aktuálny čas chcela vedieť Alica a nie proxy server. Rovnako Alica nevie zistiť, či jej proxy server povedal to, čo mu povedal Bob a nejako túto informáciu neupravil.



Obr. 2.4: Použitie proxy servera na obchádzanie cenzúry

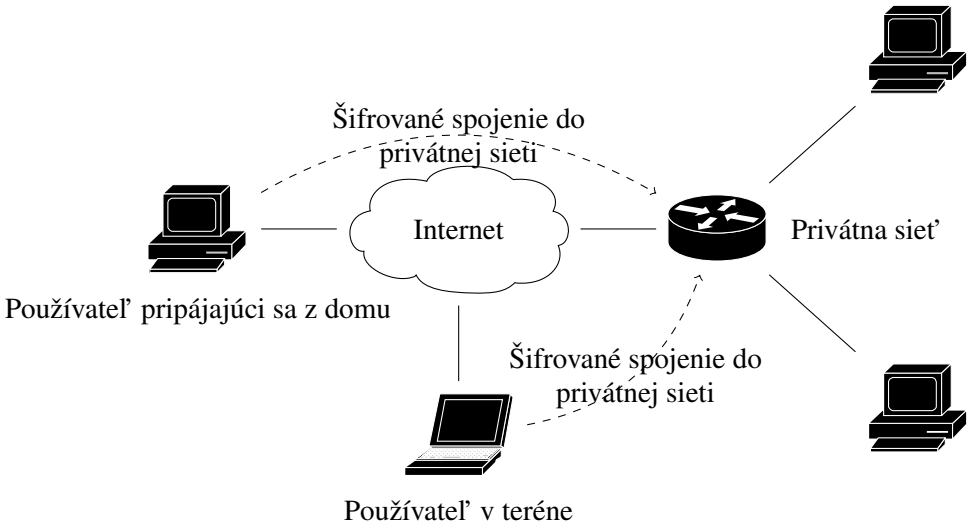
Použitie proxy servera na prístup ku blokovanému obsahu je nasledovné a je znázornené na obrázku 2.4. Používateľ nejakým spôsobom získa informácie na pripojenie sa ku proxy serveru, ako sú jeho IP adresa, port na ktorom počúva, prípadne, ak je to potrebné, tak aj meno a heslo na prístup k serveru. Tento proxy server však musí byť umiestnený mimo cenzúrovanej siete, pretože inak by jeho použitie nemalo pre používateľa žiaden význam, pretože by bol v rovnakej situácii ako na začiatku a ku cenzurovanému obsahu by stále nemal prístup. Pomocou týchto údajov si používateľ nastaví aplikáciu, pomocou ktorej chce komunikovať s proxy serverom. Väčšinou ide o webový prehliadač, keďže najčastejšie sa pristupuje ku blokovaným webovým stránkam, no toto riešenie sa dá použiť pre ľubovolný program, ak spolu s používaným proxy serverom podporujú protokol SOCKS [4]. Existujú aj mnohé webové stránky, ktoré samé o sebe slúžia ako jednoduchý proxy server a zobrazujú v sebe obsah z iných webových stránok. Používateľ komunikuje s proxy serverom cez šifrované spojenie, ktoré v sebe obsahuje informáciu o tom, o aký obsah má používateľ záujem. Keď používateľ pošle proxy serveru zašifrovaný paket s požiadavkou, že chce dáta z konkrétnej adresy, tak proxy server tento paket rozšifruje, pozrie sa, akú adresu a požiadavku paket vo vnútri obsahuje. Následne pošle paket s touto požiadavkou na adresu, ktorú obdržal, no ako zdrojovú adresu uvedie svoju. Keď proxy server príjme odpoveď, tak ju zašifruje a pošle používateľovi ako odpoveď. Vďaka tomuto riešeniu, systém, ktorý filtruje komunikáciu nevie, že používateľ v skutočnosti nekomunikuje so skutočným serverom, pretože vidí iba

šifrovanú komunikáciu medzi používateľom a týmto serverom a server obsahujúci obsah ku ktorému používateľ pristupuje nevie, kto k nemu v skutočnosti pristupoval, pretože z jeho pohľadu to vyzerá tak, že požadovaný obsah odoslal niekomu kto oň požiadal a nevie, že išlo len o proxy server, ktorý tento obsah poslal ďalej.

Proxy server ako nástroj na prístup ku blokovanému obsahu má však jeden veľký nedostatok. Jeho slabina spočíva v tom, že funguje len dovtedy, kým systém, ktorý filtruje prístup ku cenzurovanému obsahu tento proxy server neidentifikuje a následne nerozšíri zoznam blokovaných IP adries o IP adresu na ktorej sa tento proxy server nachádza. Toto spôsobí, že proxy server sa stane v tejto cenzurovanej sieti nedostupným. Používatelia následne potrebujú nejakým spôsobom získať prístupové údaje na iný proxy server. Tento proxy potom búdu používať dovtedy, pokým sa aj jeho IP adresa nedostane na zoznam blokovaných IP adries a následne sa tento proces nebude znova opakovať. Z tohtt dôvodu, je aj šírenie informácii o spôsobe pripojenia na proxy server náročné. Je treba totiž dávať pozor na to, aby cenzor tieto informáciu nezachytil. Ak by sa mu to podarilo, tak by hrozilo, že tento proxy server bude krátko po svojom vzniku zablokovaný.

2.1.2 VPN

VPN (Virtual Private Network - virtuálna privátna sieť) [5] slúži na prepojenie viacerých počítačov, pripojených prostredníctvom verejnej siete ako je napríklad internet, do jednej veľkej spoločnej privátnej siete. Ako je znázornené na obrázku 2.5, tak tieto počítače následne môžu komunikovať ako by boli pripojené pomocou priameho kábla do uzavretej privátnej siete.

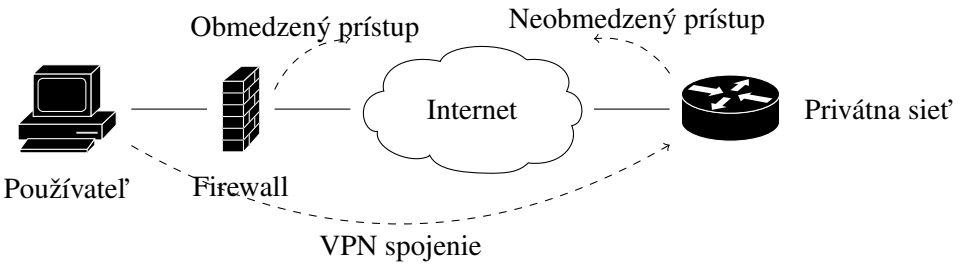


Obr. 2.5: Schéma VPN

Keďže celá komunikácia medzi počítačom a sieťou, ku ktorej sa pomocou VPN pripája vzniká až po obojstranom overení certifikátov a následne prebieha ako šifrované tunelové

spojenie, tak je toto riešenie bezpečné a aj vďaka tomu sa z VPN stal rozšírený a používaný nástroj. K tomuto prispel aj fakt, že VPN je priamo podporované vo väčšine operačných systémov a je integrované do mnohých sieťových prvkov.

Pri použití tohto riešenia v situácii, keď je požadovaný prístup ku filtrovanému obsahu sa využíva fakt, že používateľ má po použití VPN prístup do inej siete, ako je tá filtrovaná, v ktorej sa fyzicky nachádza. V tejto sieti má používateľ prístup ku všetkému, čo je v tejto sieti dostupné. Na rozdiel od zvyčajného použitia VPN, ktoré sa používa na prístup k údajom, vo vnútri lokálnej siete, tak VPN pri obchádzaní cenzúry slúži na prístup von z lokálnej siete, do internetu. Kedže sa totiž táto sieť už nenachádza pod kontrolou cenzora, tak používateľ má z tejto siete neobmedzený prístup na internet. Takéto použitie VPN je znázornené na obrázku 2.6.



Obr. 2.6: Použitie VPN na obchádzanie cenzúry

VPN je podobné svojou funkčnosťou proxy serveru, ale sú medzi nimi určité rozdiely. Pripojenie na proxy server sa jednoduchšie nastavuje, no nie je podporované každou aplikáciou na rozdiel od VPN, ktoré je zvyčajne podporované priamo operačným systémom. Cez VPN sa dá komunikovať pomocou ľubovoľného protokolu, pričom proxy sever je určený predovšetkým len na prístup ku webovým stránkam a s ostatnými protokolmi funguje podľa toho, aký protokol beží na strane servera. Toto má za následok, že pripojenie ku proxy serveru funguje len pre aplikácie, kde je pripojenie nastavené a podporované, no VPN na druhej strane vytvára virtuálny sieťový port, cez ktorý môže prechádzať všetka sieťová komunikácia. Keďže je však komunikácia cez VPN zložitejšia a teda jej spravovanie si vyžaduje viac systémových prostriedkov, tak proxy server s rovnakým výkonom a pripojením dokáže obslúžiť viac používateľov ako VPN. Ďalší z rozdielov medzi proxy serverom a VPN je aj v tom, čo robia s paketmi, ktoré cez ne prechádzajú. Proxy server totiž všetky pakety, ktoré odosiela vytvára na základe požiadavky a odpovede, ktoré dostane, pričom VPN pakety pred tým, ako ich odošle, iba zašifruje a zabalí ako VPN komunikáciu.

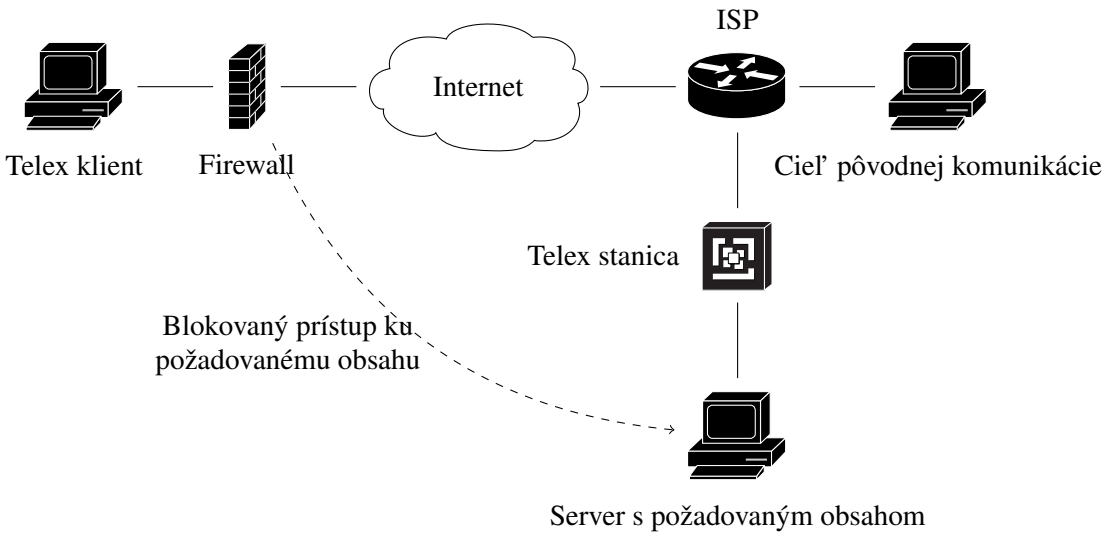
2.1.3 Telex

Telex [12] je nástroj na obchádzanie cenzúri vznikajúci vďaka spolupráci kanadskej univerzity v meste Waterloo a americkej univerzite v Michigene. Snažia sa ním riešiť nedostatky

iných nástrojov, ktoré sa vyskytujú napríklad, pri použití proxy servera či VPN. Pri týchto riešeniach je totiž potrebné poznať nastavenia, pomocou ktorých sa k nim dá pripojiť. Ďalšia ich nevýhoda, ktorá je dôležitejšia, je v tom, že po zablokovaní ich IP adries je potrebné, aby sa premiestnili na inú adresu a následne rozšíriť prístupové údaje používateľom, nech sa k nim môžu pripojiť bez toho, aby sa k týmto údajom znova dostal cenzor. Telex totiž používa odlišný spôsob prístupu. Kým predošlé riešenia fungovali na spôsobe, že sa používateľ musel niekam pripojiť a z tohoto miesta už mal následne prístup do necenzurovanej siete, tak Telex funguje tak, že pri jeho použití používateľ získava prístup do necenzurovanej siete v strede sieťovej infraštruktúry. Telex totiž predpokladá spoluprácu poskytovateľov internetového pripojenia, čo je rozdiel voči iným riešeniam v tom, že ostatné riešenia väčšinou fungujú vďaka dobrovoľníkom, ktorí prepožičiavajú svoje internetové spojenie a výpočtový výkon ostatným používateľom. Táto zmena zaužívaného konceptu je založená na myšlienke, že proti cenzúre na celoštátnej úrovni, by mal bojovať systém na obchádzanie cenzúry, ktorý operuje tiež na celoštátnej úrovni, čo by ich sily vyrovnalo.

Vďaka tomuto spôsobu fungovania teda Telex nepotrebuje medzi používateľov šíriť žiadnu IP adresu, prípadne iné informácie potrebné na pripojenie, pretože ich používatelia ani nepotrebujú. Jedinú vec, ktorú totiž pri tomto riešení používatelia ku použitiu Telexu potrebujú, je Telex klient. Keď sa chce používateľ s týmto klientom pripojiť na blokovanú stránku, tak klient vytvorí šifrované spojenie na neblokovanú stránku mimo cenzurovanej siete. Keďže toto spojenie vyzerá ako štandardné HTTPS spojenie smerujúce na nezakázaný server nevykazuje žiadne podozrivé správanie, tak ho systém slúžiaci na filtrovanie dátovej komunikácie povolí. Spojenie, ktoré ide od klienta smerom na internet však slúži len ako zásterka, ktorá je určená na oklamanie cenzora, ktorý nedokáže zistiť, že klient v skutočnosti vôbec nemá záujem, aby sa dostal na adresu, ktorá je v hlavičke paketu uvedená a chce, aby jeho komunikácia bola odklonená iným smerom. Klient totiž, keď vytváral spojenie, tak ho označil ako Telex požiadavku vložením špeciálnej steganografickej značky do hlavičky. Táto značka je vytvorená pomocou asymetrického šifrovania a teda označiť spojenie ako Telex spojenie môže každý, no len Telex server dokáže toto spojenie rozpoznať, pretože len on je držiteľom privátnych kľúčov. Táto značka sa odosiela pri dohadovaní SSL/TLS spojenia medzi počítačom používateľa, na ktorom beží Telex klient a serverom.

Vzhľadom na to, že toto spojenie je šifrované a nie je odlíšitelné od šifrovaného spojenia nepoužívajúceho Telex, tak jediným riešením ako Telex spojenia účinne blokovať je plošné blokovanie celého SSL/TLS protokolu. Toto by však malo za následok zneprístupnenie všetkej šifrovanej komunikácie, ktorá je šifrovaná pomocou SSL/TLS, a teda by nebolo možné pristupovať ku veľkej časti internetu.



Obr. 2.7: Schéma telexu

Ako toto spojenie funguje, je znázornené na obrázku 2.7. V prvom kroku si používateľov klient zvolí vhodnú web stránku, ktorá nie je blokovaná a je dostatočne bežná, aby nevzbudila podozrenie cenzora. Následne sa používateľ k tejto stránke pokúsi pripojiť pomocou HTTPS, pričom Telex klient toto spojenie označí špeciálnou značkou do hlavičky. Potom, ako toto spojenie s označenou hlavičkou putuje internetom smerom k neblokovanej službe, tak prechádza cez viacero smerovačov patriacich rôznym poskytovateľom internetového pripojenia. Cestou k adrese nachádzajúcej sa v hlavičke paketu, by mal mať aspoň jeden z týchto poskytovateľov internetového pripojenia na smerovačoch pripojenú Telex stanicu. Na tomto smerovači by sa všetky pakety presmerovali na Telex stanicu. Toto zariadenie by pomocou privátneho kľúča dokázala rozpoznať, či sa jedná o Telex spojenie. Keď by Telex stanica toto spojenie identifikovala, tak by povedala smerovaču, aby túto komunikáciu neposielal ďalej ale odklonil na požadovanú stránku. Takto by vznikol šifrovaný tunel medzi používateľom a pôvodne blokovanou stránkou, ktorý prechádza cez smerovač s Telex stanicou, ktorá toto spojenie identifikovala. Ak by Telex stanica v spojení žiadnu značku nenašla, tak by spojenie bez zmeny pokračovalo na pôvodnú adresu.

Toto riešenie však momentálne ešte nie je prevádzky schopné, pretože jediné miesto, kde sa Telex stanica nachádza je v laboratóriu, kde je Telex vyvíjaný. No podľa informácií na stránke projektu, pri testovaní dosahoval prototyp Telexu, čo sa výkonu a stability týka, priaznivé výsledky. Momentálne by sa toto riešenie malo nachádzať vo fáze vylepšovania a testovania v spolupráci s partnerským poskytovateľom internetového pripojenia, a tak sa možno čoskoro stane plne funkčným a použiteľným.

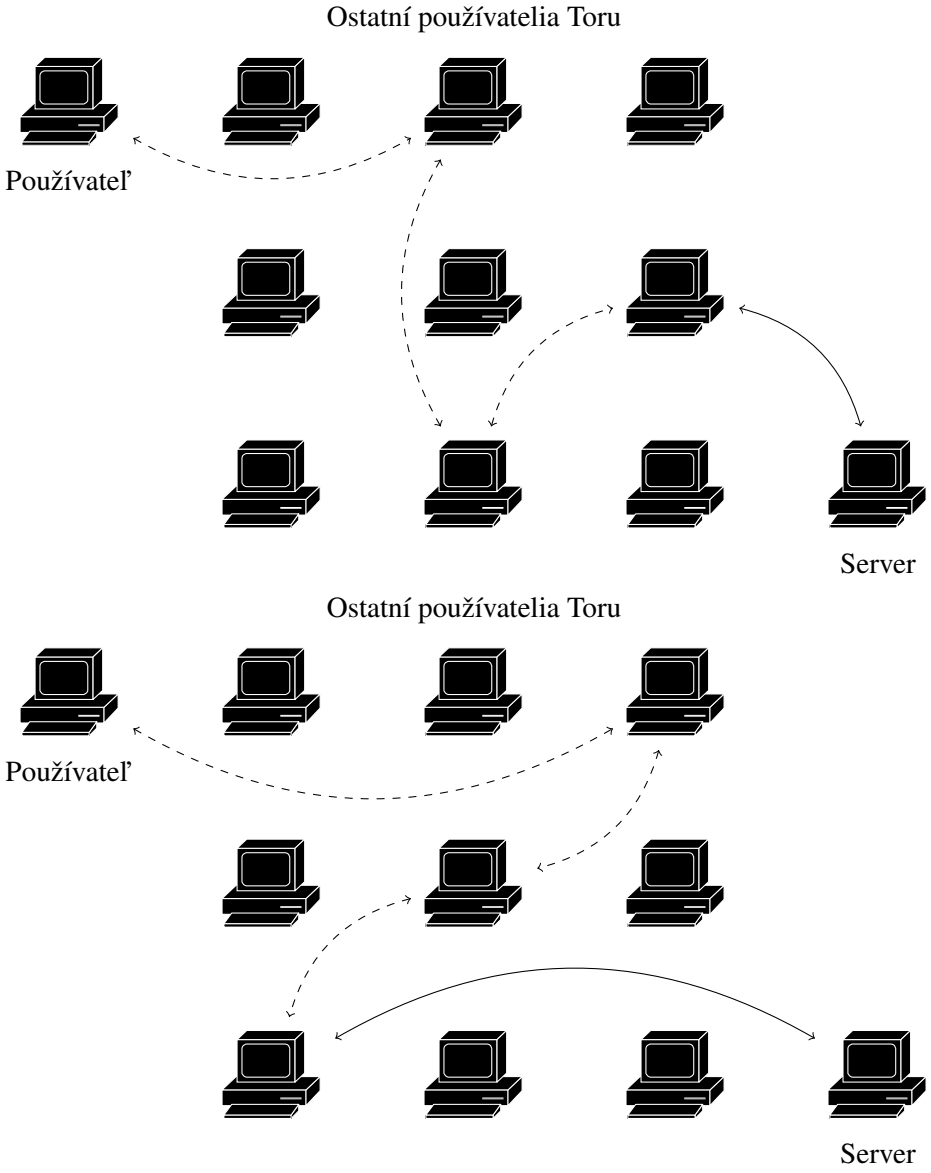
2.2 Distribuované siete

Medzi riešenia, patriace do tejto kategórie sa radia také, ktorých architektúra je postavená na sieti tvorenej z viacerých používateľov, uzlov, ktorí ich používajú. Používatelia sú si v tejto sieti navzájom nápomocní. Napríklad, cez nich navzájom prechádza komunikácia smerujúca von zo siete, alebo si poskytujú dátový priestor. Vďaka svojej architektúre častokrát slúžia aj na ochranu anonymity používateľov. Tieto siete v sebe často obsahujú aj rôzne služby, ktoré sú prístupné len v rámci nej, no niektoré riešenia ako napríklad I2P [13] majú vyriešený spôsob, ako dokážu smerovať dátovú prevádzku z internetu do tejto siete, a teda mať tieto služby prístupné aj priamo z internetu. Najvýznamnejšie riešenia patriace do tejto skupiny sú Tor a Freenet.

2.2.1 Tor

Nástroj Tor [3] je decentralizovaná sieť určená pôvodne na anonymný prístup do internetu, ale stal sa z neho aj jeden z najznámejších nástrojov na obchádzanie cenzúry na internete. Jeho popularita už vzrástla na toľko, že organizácia Internet Engineering Task Force (IETF), ktorá je centrálnym miestom tvorby internetových štandardov, zvažuje vytvorenie z protokolu Tor internetový štandard. Názov Tor pochádza z pôvodnej skratky názvu The Onion Router, čo vystihuje spôsob akým funguje. Komunikácia pri používaní Toru totiž pred tým, ako sa dostane od používateľa na požadovaný server, prechádza cez viacero ďalších uzlov, čo sú ďalší používatelia Toru. Medzi každou za sebou nasledujúcou dvojicou, cez ktorú prechádza, vytvára samostatný šifrovaný kanál a tak sa celá komunikácia skladá z viacerých šifrovaných vrstiev, v čom je analógia s cibuľou, podľa ktorej bolo toto riešenie nazvané. Vďaka architektúre, že spojenie prechádza cez ostatných používateľov, získava Tor oproti napríklad proxy serveru veľkú výhodu, pretože používateľ pri tomto riešení má viac možností ako vstúpiť do siete Tor, a teda aby mu cenzor zabránil Tor používať, tak je potrebné, aby zablokoval adresy všetkých vstupných bodov do siete. Používateľ môže na komunikáciu so serverom používať len aplikácie s podporou protokolu SOCKS, pretože Tor podporuje iba tento protokol.

Ako Tor funguje, je zobrazené na obrázku 2.8. Pred začiatkom komunikácie, používateľov klient obdrží zo špeciálneho servera zoznam ďalších používateľov používajúcich Tor. Z nich si zopár náhodne zvolí a použije ich na cestu k serveru, ku ktorému chce pristupovať. Táto cesta však zostáva v platnosti iba určitý čas a keď tento čas uplynie, tak sa znovu náhodne zvolia uzly, cez ktoré bude viesť ďalšie spojenie. Toto spôsobuje, že aj dve cesty k rovnakému serveru od toho istého používateľa vstupujú do siete Tor cez iný uzol, cez rôzne uzly prechádzajú a cez odlišný uzol z tejto siete smerom k tomuto serveru vychádzajú. Následkom tohto správania je napríklad to, že obe cesty majú z pohľadu servera rôznu IP adresu a teda obe cesty pokladá za dvoch rôznych používateľov.



Obr. 2.8: Schéma Toru pri dvoch rôznych spojeniach

Medzi každou za sebou idúcou dvojicou uzlov, cez ktoré komunikácia prechádza sa nachádza samostatná zašifrovaná vrstva. Táto vrstva je šifrovaná pomocou SSL/TLS. V obrázku je každá táto vrstva znázornená prerušovanými čiarami a posledné spojenie od uzla smerom na server je šifrované podľa toho, akým spôsobom používateľ s týmto serverom komunikuje, a teda je rovnaké, ako by k nemu pristupoval používateľ priamo. Takáto vrstvená komunikácia má za následok, že komunikácia je bezpečná a navyše používateľovi zaručuje anonymitu, pretože ani server ani používatelia, cez ktorých prechádza komunikácia, nevedia určiť, od ktorého používateľa komunikácia pôvodne pochádza. Každý uzol v komunikácii, totiž vie iba to kto mu niečo poslal a vie, komu to má poslať ďalej. Avšak to, že je celá komunikácia takto šifrovaná je jeden z dôvodov toho, že pri používaní Toru výrazne klesá rýchlosť sieťového spojenia a čas odozvy. Druhý a vážnejší dôvod je však v tom, že výsledná rýchlosť je závislá od rýchlosti internetového pripojenia každého používateľa, cez ktorého komunikácia

prechádza a navyše môže byť rýchlosť pripojenia priamo používateľmi znižovaná, ak pre Tor nechcú povoliť celú šírku pásma. Tieto dva faktory teda môžu rýchlosť internetového pripojenia ovplyvniť až na toľko, že napríklad z pôvodného pripojenia 10 MBit/s sa stane 50 KBit/s. A však aj keď je to 200-násobný pokles v rýchlosti, tak sa Tor so svojou architektúrou hlási ku "low lattecncy"riešeniam a teda stále patrí medzi tie rýchlejšie. Napríklad od Freenetu, ktorý sa uvádza v ďalšej časti, je Tor výrazne rýchlejší.

Tor podporuje koncept "skrytých služieb", čo sú služby, ktoré sa nachádzajú vo vnútri siete Tor. Ide väčšinou o webové stránky, ale aj o služby ako sú dátové uložištia, služby na P2P zdieľanie súborov, email či rôzne vyhladávače. Tieto služby sú dostupné len zo siete Tor a na prístup k nim je potrebné poznať ich špecifickú adresu (onion address), ktorá popisuje kde sa táto služba nachádza. Vďaka tomuto, že sa k tejto službe pristupuje cez túto adresu a nie napríklad cez IP adresu, tak sa z nej nedá priamo zistiť, kde sa táto služba fyzicky nachádza, a teda je jej umiestnenie anonymné. Rovnako vďaka spôsobu fungovania Toru je zachovaná aj anonymita používateľov, ktorí k nej pristupujú. Vzhľadom na to, že Tor je decentralizovaná sieť, a teda neexistuje žiaden centrálny server, tak neexistuje ani žiaden súhrný zoznam všetkých skrytých služieb a tak k službe je možné pristupovať len so znalosťou jej adresy. Z toho vyplýva, že je možné jednoducho vytvoriť súkromnú službu, ku ktorej by mali prístup len používatelia, ktorý by vedeli jej názov.

To, ako sa však Tor rozšíril a stal sa populárnym má aj svoje nevýhody. Keďže pre cenzora je častokrát náročné Tor (a podobne fungujúce siete) blokovať, tak sa namiesto toho Tor často stáva terčom rôznych útokom, za účelom, aby bolo jeho používanie čo najviac zneprístupnené. Naštastie veľa týchto útokov bolo dobre zdokumentovaných a do Toru boli postupne pridané rôzne vylepšenia, aby sa tieto útoky viackrát neopakovali.

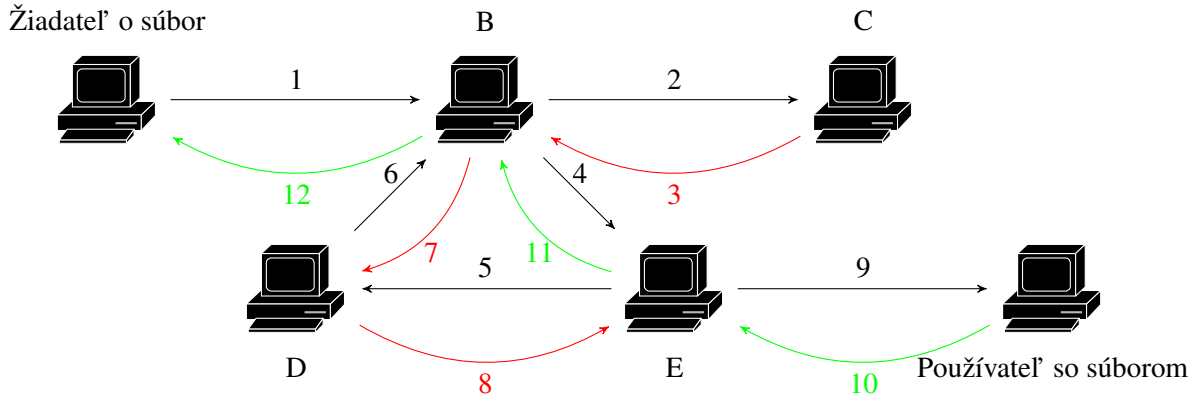
2.2.2 Freenet

Freenet [2] je softvér postavený na decentralizovanej P2P architektúre. Jeho cieľom je anonymné, bezpečné a necenzurovateľné zdieľanie informácií. Pri používaní tohto nástroja, každý používateľ dáva k dispozícii na svojom počítači dátový priestor pre potrebu celej siete. Tento priestor je spravovaný automaticky a tvorí jeden veľký virtuálny súborový systém. Systém je navrhnutý tak, že súbory v sieti putujú a replikujú sa podľa toho, ako a kde sú používané. Keďže dátový priestor v sieti má obmedzenú veľkosť, tak súbory, ktoré sa nepoužívajú sú v prípade potreby mazané. Z tohto dôvodu nie je Freenet vhodný na archiváciu rozsiahlých dát, ku ktorým by nikto nepristupoval, pretože by boli po čase odstránené, aby vzniklo miesto pre nové súbory.

Pridávanie súborov do siete prebieha tak, že používateľ pošle do siete správu, obsahujúcu zašifrovaný súbor a k nemu priradený jedinečný globálny identifikátor (GUID). Odoslaná

správa so zašifrovaným súborom a GUID spôsobý, že sa súbor uloží na nešpecifikované uzly v sieti. Teda, keď používateľ vloží do siete nejaký súbor, tak sa zvyčajne uloží na úplne iný počítač ako je ten, z ktorého bol do siete vložený. Z jeho pôvodného miesta sa následne premiestňuje a replikuje podľa toho, ako veľmi je používaný, a teda ani vlastník súboru nevie povedať, kde sa jeho súbor nachádza. Vďaka tomuto riešeniu, ak chce vlastník súboru, aby bol jeho súbor neustále dostupný, tak nemusí byť neustále online, pretože sa jeho súbor nachádza na iných uzloch. Používatelia väčšinou nevedia, aké súbory sa u nich nachádzajú, pretože sú zašifrované a nevedia ich rozšifrovať a ani k nim pristupovať bez znalosti ich GUID. Tento zoznam, GUID všetkých súborov, ktoré sa u používateľa nachádzajú síce existuje, ale je pre neho v nečitateľnej podobe. Takéto riešenie slúži aj na to, aby používatelia nemohli byť zodpovední a postihovaní za obsah, ktorý sa u nich nachádza, keďže nevedia čo je na ich počítačoch uložené.

Keďže každý uzol obsahuje určité súbory a pamätá si len aké súbory cez neho prechádzali, tak žiaden uzol nemá úplnú informáciu o tom, kde sa nachádzajú všetky súbory. Na získanie súboru zo siete, musí používateľ poslať správu obsahujúcu GUID súboru, ktorý chce získať. Táto správa potom putuje sieťou tak, že sa vždy posiela len na jeden uzol, o ktorom sa predpokladá, že by mohol vedieť, kde sa súbor nachádza. Keď takýto uzol obdrží správu, že niekto hľadá súbor, tak sa pozrie do svojej tabuľky, či sa u neho tento súbor nenachádza. Ak sa nachádza tak ho pošle na ten uzol, z ktorého prišla požiadavka. Ak sa nenachádza, tak si vyberie nejaký uzol, ku ktorému je pripojený a pošle mu správu, že tento súbor hľadá. Niektoré distibuované siete hľadanie súboru riešia tak, že posielajú správu každému pripojenému uzlu, ktoré pošlú rovnakú správu všetkým k nim pripojením uzlom, čo vedie k pomerne rýchlemu nájdeniu súbora, no na druhej strane aj k veľkému zahlteniu siete, čo je pri veľkých sieťach, v ktorých sa často niečo hľadá nepoužiteľné. Ako získavanie súboru prebieha, je znázornené na obrázku 2.9. Hľadanie súboru prebieha v podstate pomocou prehľadávania do hĺbky.



Obr. 2.9: Požiadavka na získanie súboru v sieti Freenet

Z tohto obrázku je vidieť, že kým sa v sieti požadovaný súbor nájde, tak treba v najhoršom prípade pomocou prehľadávania do hĺbky prehľadať celú sieť. Aby takéto požiadavky

zbytočne neprechádzali celou sieťou, tak pri každom hľadaní súboru sa počíta cez koľko uzlov už táto požiadavka prešla a keď sa dosiahne určitý počet, tak sa táto požiadavka zastaví a už ďalej nepokračuje. Namiesto toho, aby sa však zahodila, začne sa vracať s tým, že súbor nenašla. Každým prechodom späť sa zníži počet uzlov, cez ktoré už požiadavka prešla a keď príde na uzol, ktorý je pripojený aj iným smerom akým už požiadavka išla, tak sa pošle týmto smerom, kým zase nedosiahne kritický počet uzlov. Až keď sa prehľadajú všetky vetvy do určitej hĺbky, tak sa vráti požiadavka ako neúspešná naspäť používateľovi. Ten ju môže následne poslať s väčším maximálnym počtom prechodov. Vzhľadom na to, že Freenet sa snaží uchovávať aj anonymitu používateľov a počet uzlov, cez ktoré už požiadavka prešla môže o používateľovi prezradiť, že niečo hľadá, ale aj kde sa súbor nachádza ostatným uzlom. Preto, aby sa tieto informácie aspoň trochu ochránili, tak počet uzlov, cez ktorý už požiadavka prešla sa zvyšuje náhodne podľa určitej pravdepodobnosti a rovnako sa podľa inej pravdepodobnosti znižuje.

Keď chce používateľ svoj súbor zmeniť, tak si tento súbor zo siete vypýta a upraví ho vďaka kľúču, ktorý mu vznikol pri vytvorení tohto súbora a používateľa identifikuje ako vlastníka tohto súboru. Po jeho zmene je tento súbor odoslaný späť do siete s tým, že bol zmenený a všetky kópie sa postupne nahradia touto verziou.

Okrem toho, že Freenet podporuje zdieľanie súborov, tak obsahuje aj možnosť publikovania a prezerania rôznych "freesites", čo sú špeciálne webové stránky upravené pre potreby Freenetu a prístupné len cez túto sieť. Ďalšie podporované služby sú napríklad aj komunikácia na rôznych fórach, či email. Všetky tieto služby sú založené na rovnakom spôsobe fungovania ako Freenet narába so súbormi. Freenet tiež obsahuje možnosť pripojenia v režime "darknet". Tento režim slúži na pripojenie sa len ku používateľom, ktorým používateľ dôveruje. Pri tomto režime si totiž používateľ môže explicitne zvoliť, ku komu chce byť pripojený. Pri takomto pripojení vznikne distribuovaná sieť len medzi týmito používateľmi, vďaka čomu vznikne ešte bezpečnejšia a ťažšie detekovatelná sieť. A však títo používatelia nemusia byť pripojení všetci navzájom a ani nemusia byť pripojení k tým istým používateľom. Cieľom takejto siete je eliminovať počet ľudí, ktorí by jej chceli škodiť. Pretože pomocou Darknetu môže vzniknúť aj rozsiahla sieť, ale aby sa k nej používateľ mohol dostať, musí byť nejakým spôsobom prepojený s ostatnými používateľmi, ktorí ho k sebe pripoja len vtedy, keď ho poznajú a vedia, že nebude škodiť.

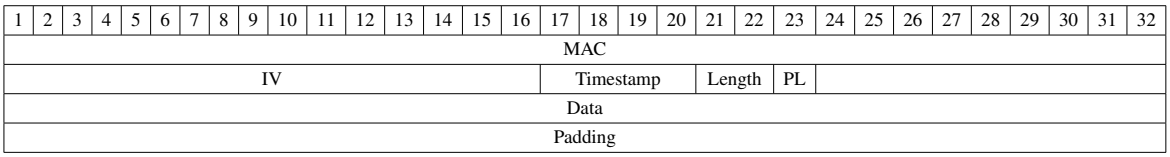
2.3 Ostatné riešenia

Okrem riešení patriacich do predchádzajúcich dvoch kategórií zostávajú ďalšie, ktoré sa k nim zaradiť nedajú. Ide napríklad o rôzne špeciálne protokoly ako je napríklad protokol Dust, ktorého popis sa nachádza v ďalšej časti práce, ale aj riešenia na archivovanie a vytváranie kópií webových stránok [1], či služby, ktoré odosielajú webové stránky ako email [10].

2.3.1 Dust

Dust [11] je internetový protokol, ktorý bol vytvorený na univerzite v Austine. Je navrhnutý tak, aby odolal súčastným spôsobom, ktoré sa používajú na cenzúrovanie internetovej komunikácie a teda aby nemohol byť filtrovaný pomocou DPI (Deep Packet Inspection). Dust používa od ostatných riešení odlišnú techniku na vytváranie bezpečného spojenia, ktoré je určené na komunikáciu cez filtrovaný dátový kanál. Následne ako je toto spojenie vytvorené, tak Dust pakety sú neodlíšiteľné od náhodných paketov, a tak nemôžu byť filtrované zaužívanými spôsobmi. Oproti ostatným šifrovacím protokolom totiž Dust pri dohadovaní spojenia neprenáša žiaden nešifrovaný text, ktorý by firewallu dovoľoval to, že by vďaka nemu mohol túto komunikáciu identifikovať a následne ju zablokovať. To preto, lebo aj tie jeho časti, ktoré nie sú šifrované, sú náhodne volené hodnoty určené len na jedno použitie. Aby toto bolo dosiahnuteľné, tak výmena kľúčov pri tomto riešení zo strany servera prebieha tak, že sa pošle "pozývací"paket, inak ako priamo na IP adresu používateľa, napríklad na jeho emailovú adresu. Tento paket obsahuje informácie, ako sú IP adresa servera, jeho port či verejný kľúč používateľa. Následne keď chce používateľ dokončiť výmenu kľúčov tak pošle na adresu z "pozývacieho"paketu úvodný paket, za ktorým môžu nasledovať dátové pakety. V implementácii protokolu Dust sa na šifrovanie používa hešovacia funkcia Skein, čo je neúspešný kandidát na štandard SHA-3.

Pri celej komunikácii sa komunikuje pomocou paketov, ktorých tvar je znázornený na obrázku 2.10. Toto je základný paket, z ktorého vychádzajú ostatné pakety, pričom dátový paket vyzerá rovnako. Čísla na hornej časti obrázku vyjadrujú veľkosť jednotlivých častí paketu.

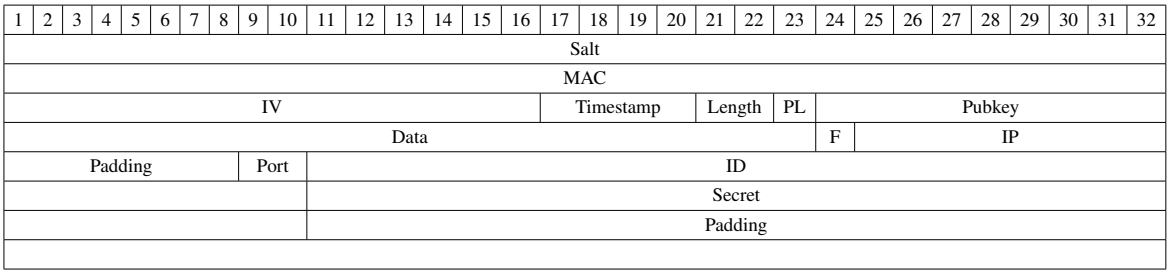


Obr. 2.10: Dátový paket protokolu Dust

Hodnota MAC je počítaná pomocou šifrovanej časti paketu, inicializačného vektoru (IV) a kľúča, ktorý závisí od jednotlivého typu paketu. Vďaka tomuto je možné overiť, či paket nebol nejako poškodený. Inicializačný vektor je náhodná hodnota na jedno použitie, použitá na zašifrovanie obsahu paketu a na výpočet MAC hodnoty. Toto zaručuje, že šifrovaný obsah aj MAC budú aj pri odosielaní rovnakých dát rôzne. Zvyšok paketu okrem posledného poľa na konci paketu je šifrovaný. Koniec paketu má náhodnú dĺžku, aby dĺžka paketu bola čo najviac náhodná.

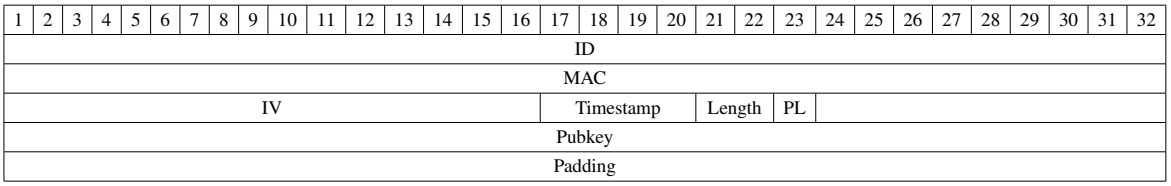
Komunikácia medzi serverom a používateľom je nasledovná. Aby server mohol akceptovať pakety z neznámej IP adresy, tak musí najprv absolvovať výmenu kľúčov s používateľom

na tejto IP adrese. Na začiatku server vygeneruje náhodné id a heslo, a následne pošle používateľovi "pozývací"paket spolu s heslom, ktorým je tento paket zašifrovaný. Ako vyzerá tento paket, je znázornené na obrázku 2.11. "Pozývací"paket má tvar ako predchádzajúci paket, s tým rozdielom, že v dátovej časti sa nachádzajú všetky informácie potrebné pre používateľa na pripojenie sa k serveru, ako sú IP adresa servera, jeho port, verejný kľúč, používatelové id a ešte jedno (iné) heslo. Na začiatku tohto paketu sa ešte nachádza "soľ", aby bolo znemožnené rozbitie paketu hrubou silou.



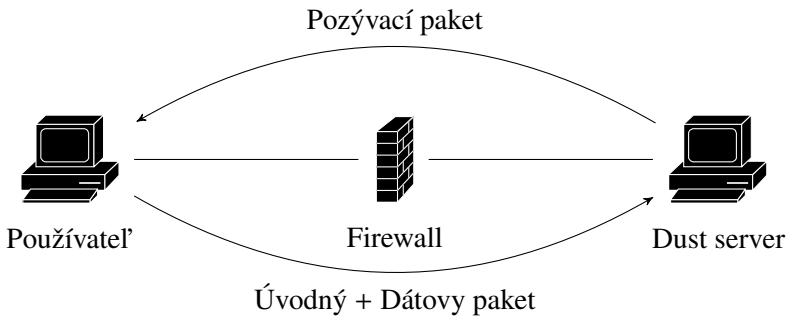
Obr. 2.11: Pozývací paket

Následne ako tento paket používateľ príjme, tak ho pomocou priloženého hesla rozšifruje, a na IP adresu a port, ktorý z neho získa pošle úvodný paket, ktorý je znázornený na obrázku 2.12. Tento paket sa začína prijatým id a je zašifrovaný pomocou hesla, ktoré sa nachádzalo vo vnútri "pozývacieho"paketu. Toto použité id bolo používateľovi pridelené len za týmto jedným účelom a už ho nepoužije.



Obr. 2.12: Úvodný paket protokolu Dust

Keď server tento paket príjme, tak by mal pochádzať pre neho z neznámej IP adresy, a teda vie, že sa jedná o úvodný paket. Podľa id, ktoré je uvedené na začiatku prijatého paketu sa pokúsi vo svojej databáze k nemu nájsť heslo, aby ho mohol rozšifrovať. Po tomto kroku server zaradí IP adresu používateľa medzi známe IP adresy, čo znamená, že medzi nimi už môže prebiehať dátová komunikácia pomocou dátových paketov. Prvý a jediný dátový paket môže byť odoslaný spolu s úvodným paketom v jednom TCP pakete, a tak teda môže celá komunikácia z pohľadu cenzora prebehnúť len za pomoci jedného TCP paketu. Priebeh komunikácie pri použití protokolu Dust je znázornený na obrázku 2.13.



Obr. 2.13: Priebeh komunikácie pri použití protokolu Dust

Aj keď je protokol Dust určený proti súčasnému spôsobu šifrovania, tak ku svojmu fungovaniu potrebuje ešte nejaké iné riešenie. To z toho dôvodu, že žiadnym spôsobom nerieši blokovanie IP adries a teda ak chce fungovať spôsobom klient a server, tak na svoje fungovanie vo väčšine prípadov potrebuje bežať napríklad za proxy serverom.

KAPITOLA 3

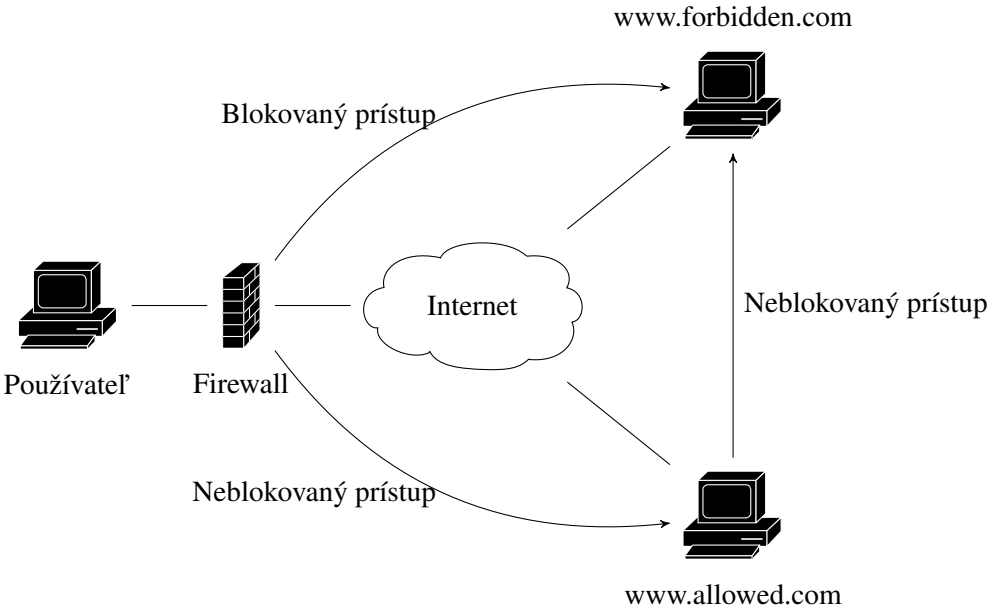
Vlastný návrh

Pri navrhovaní vlastného nástroja na obchádzanie cenzúri, sme sa snažili riešiť zraniteľnosť, ktorá je prítomná, napríklad, pri použití proxy servera a to, že takéto riešenia je možné jednoducho zneprístupniť pomocou zablokovania ich IP adries. Myšlienka, ktorú sme pri tomto probléme navrhli je mať proxy serverov výrazne viac, ako je cenzor schopný blokovať bez toho, aby toto blokovanie neovplyvnilo aj väčšinu zvyšnej internetovej prevádzky, ktorá aj keď je z pohľadu cenzora neškodná, by po zásahu zostala zablokovaná. V našom návrhu totiž predpokladáme, že by sme na proxy servery premenili veľkú časť webových serverov a používateľ by si len vybral, ku ktorému by chcel pristupovať, čo by mohol byť napríklad aj web server, na ktorom sa nachádza webová stránka, ktorú zvyčajne navštevuje, a tento web server by obsluhoval jeho požiadavky do necenzurovaného internetu. Samozrejme by musel byť umiestený mimo cenzurovanej siete, lebo inak by si s nim používateľ nepomohol.

Tieto upravené webové servery by fungovali tak ako v súčastnosti, no dokázali by tiež obslúžiť požiadavky, ktoré by požadovali súbory, nachádzajúce sa na ostatných webových serveroch. Myšlienka, mať webové servery, schopné presmerovať komunikáciu, vychádza z Telexu, ktorý ale presmerúvava komunikáciu pomocou staníc pripojených na prepínačoch internetových providerov. Naše riešenie je také rozsiahle preto, pretože rovnako ako autori Telexu si aj my myslíme, že proti cenzúre pracujúcej na celonárodnej úrovni by malo bojovať aj rovnako rozsiahle riešenie, ktoré by operovalo na rovnako veľkej úrovni. Rozdiel medzi našim návrhom a Telexom je v tom, že zatiaľ, čo Telex na svoje fungovanie požaduje aktívnu spoluprácu určitého internetového providera, tak pri našom návrhu predpokladáme aktívnu účasť správcov webových serverov. Totiž, aby náš návrh fungoval, predpokladáme, že by sa na určitých webových serveroch nachádzalo naše vlastné rozšírenie, ktoré by bolo schopné preposielať požiadavky používateľa na ostatné webové servery, ktoré by serveru vracali odpoveď a ten by ich preposielal naspäť používateľovi. Čím by bolo takýchto serverov viac, tým by toto riešenie lepšie fungovalo.

3.1 Popis návrhu

Spôsob, ako by malo naše riešenie fungovať, je znázornený na obrázku 3.1. Používateľ, ktorý by chcel komunikovať so stránkou www.forbidden.com, ktorá je v sieti, ku ktorej je používateľ pripojený blokovaná, by vytvoril spojenie so stránkou www.allowed.com, ku ktorej vie bez obmedzenia pristupovať a ktorá sa nachádza mimo cenzurovanej siete. Toto spojenie by však muselo byť šifrované, pretože inak by cenzor v komunikácii videl, že sa používateľ snaží pristupovať k iným súborom ako sú lokálne súbory umiestnené na serveri, ku ktorému je používateľ pripojený a toto pripojenie by s najväčšou pravdepodobnosťou zablokoval. Po pripojení ku stránke www.allowed.com, by následne cez túto stránku mohol komunikovať so stránkou www.forbidden.com.



Obr. 3.1: Schéma použitia návrhu

Takáto komunikácia by bola možná vďaka požiadavkám odosielaným na špeciálnu adresu. Táto adresa by sa skladala z troch častí. Prvá časť by určovala webový server, ku ktorému je používateľ priamo pripojený a s ktorým vlastne komunikuje, druhá časť by bola špeciálna značka slúžiaca pre potreby nášho rozšírenia a tretia časť by bola URL adresa súboru, ku ktorému chce používateľ pristupovať. Teda v prípade, ktorý je znázornený na obrázku 3.1, by používateľ posielal požiadavky s adresou www.allowed.com/@@www.forbidden.com/. Ako špeciálnu značku sme zatiaľ pre názornosť zvolili @@, no jej konkrétna podoba je vec implementácie. Dôležité však je, aby jej podoba bola konzistentná, aby nemohla byť pri rôznych rozšíreniach prítomných na serveri interpretovaná odlišným spôsobom, ako si želáme a aby s ňou dokázali prehliadače a aj samotný webový server pracovať. Tiež sa však od jej podoby vyžaduje, aby nemala taký tvar, že by bola používaná v skutočnej adrese. Táto značka by mala dva významy. Jej prvý význam by bol v tom, že by jej výskyt v adrese pre webový server indikoval, že používateľ chce využiť služby nášho rozšírenia a druhá, že by

oddeľovala adresu servera a začiatok adresy, ktorú používateľ požaduje. Keď by teda webový server s rozšírením prijal požiadavku, tak by sa pozrel, či sa v adrese na správnom mieste nenachádza tento oddeľovač. Na správnom mieste preto, pretože ak by bol tento oddeľovač napríklad na konci požiadavky, tak by nebolo jasné, kam chce používateľ pristupovať, a teda by táto značka nemala zmysel. Táto značka musí byť samozrejme v komunikácii skrytá, aby ju cenzor nenašiel a nezablokoval komunikáciu. Ak by webový server značku v komunikácii našiel, tak by stiahol z internetu požadovaný súbor a poslal by ho používateľovi. V takomto prípade by pre systém filtrujúci dátovú prevádzku toto správanie vyzeralo, že server vracia používateľovi na jeho požiadavku lokálny súbor. Ak by žiadnu značku nenašiel, tak by na požiadavku reagoval štandardným spôsobom.

3.2 Možné problémy

Pri tomto návrhu je potrebné vyriešiť viaceré problémy, napríklad s cookies, ale aj s priloženými súbormi k webových stránkam. Čo sa týka týchto súborov, tak pri sťahovaní webovej stránky webovým serverom je potrebné, aby z neho stiahol aj všetky súbory, ktoré využíva pôvodná stránka. Medzi tieto súbory patria napríklad obrázky, vlastné písma, CSS súbory alebo JavaScriptové súbory. Väčšinou tieto súbory nie sú nevyhnutné a webové stránky v rámci možností fungujú aj bez nich, no sú potrebné aby stránky fungovali tak, ako majú. Preto je potrebné, aby webový server spolu s požadovanou stránkou stiahol aj všetky ostatné súbory, ktoré stránka potrebuje.

Cookies ale aj mnohé doplnky, ktoré prišli spolu s HTML5 však predstavujú trochu zložitejší problém. Tieto doplnky totiž väčšinou slúžia na ukladanie rôznych dát na strane používateľa a používajú sa napríklad pri prihlasovaní sa na stránku. Problém je v tom, že sú väčšinou priradené ku konkrétnej doméne. No pri našom riešení sa tvárime, ako by sa viaceré webové stránky nachádzali na jednej doméne. Totiž www.allowed.com/@@www.forbidden.com a www.allowed.com/@@www.forbidden2.com sú dve rôzne požiadavky na dve nezávislé webové stránky. No podľa oboch požiadaviek ide o rovnakú doménu www.allowed.com, a teda by mali mať spoločné cookies, čomu je ale potrebné zabrániť.

Spôsoby, ktorými navrhujeme vyriešenie týchto, ale aj iných problémov, uvádzame v nasledujúcej kapitole, ktorá je o tom, ako by sme toto riešenie implementovali.

KAPITOLA 4

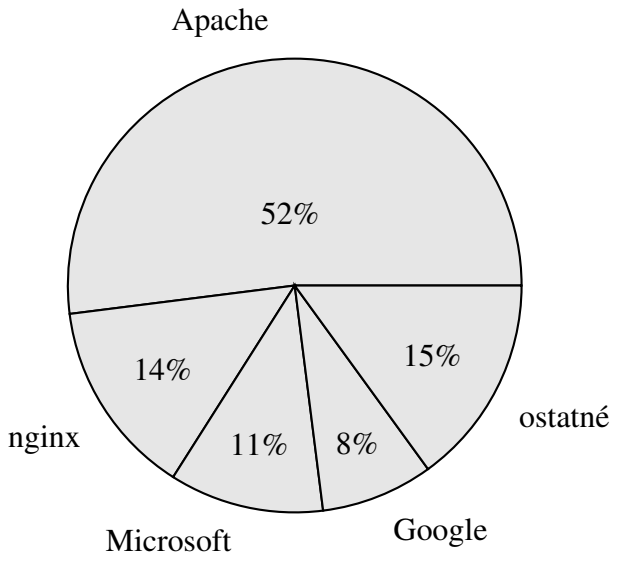
Popis implementácie

4.1 Architektúra

Na implementáciu tohto riešenia je potrebné upraviť webový server a ponúknuť používateľom nástroj, aby s ním dokázali komunikovať. Naše riešenie je teda založené na architektúre servera a klienta, kde ako server je rozšírenie do webového servera a ako klient doplnok do prehliadača.

4.1.1 Server

Pri webových serveroch sa nám zdá najlepšie, sa zamerať na webový server Apache. Tento webový server totiž veľmi dobre podporuje systém rozšírení. Okrem toho je už 18 rokov na prvom mieste v trhovom podiele webových serverov a v čase písania tejto práce na ňom fungovalo viac ako 52% aktívnych webových stránok, čo je takmer 100 miliónov. Tento podiel je znázornený na grafe 4.1.



Obr. 4.1: Trhový podiel webových serverov ku 05/2014

4.1.2 Klient

Na vytvorenie klienta navrhujeme vytvoriť doplnky už do existujúcich webových prehliadačov. Koncept doplnkov totiž podporuje väčšina moderných webových prehliadačov. Existuje aj možnosť vytvoriť vlastný webový prehliadač, ktorý by dokázal s naším rozšírením pracovať, čo by malo výhodu v tom, že by sme mali kontrolu nad všetkým, čo sa v prehliadači deje. Pred touto možnosťou však preferujeme použitie doplnkov. Tento dôvod je čisto pragmatický, pretože používatelia už používajú určité webové prehliadače a ak by chceli využívať náš doplnok na serveroch a ten by bol podporovaný len našim prehliadačom, tak by používatelia museli mať prehliadače dva. Toto by ich však čo skoro omrzelo, vrátili by sa len k jednému prehliadaču a ak by sme chceli, aby ten prehliadač bol náš, musel byť lepší ako ostatné, a to nie je naším cieľom.

Tieto doplnky by mali vedieť na strane používateľa riešiť viaceré veci. Za prvé je potrebné zautomatizovať tvorbu požiadaviek, aby používateľ nemusel pred každú požiadavku na stránku www.forbidden.com písať aj prefix, z akého servera chce k nemu pristupovať. Taktiež je potrebné aby dokázal ponúknuť zoznam serverov, ktoré sú schopné tieto požiadavky spracovať a mal by vedieť medzi nimi rozumne prepínať. Pretože, ak by používateľ celý deň komunikoval len s jedným serverom, tak by to mohlo pôsobiť podozrivo, a preto je potrebné, aby sa využívané servery striedali.

4.1.3 Komunikácia medzi serverom a klientom

Komunikácia medzi serverom a klientom by fungovala nasledujúcim spôsobom. Používateľ by chcel navštíviť stránku www.forbidden.com. Klient by si zo zoznamu serverov s naším rozšírením vybral server www.allowed.com. Klient by používateľovu požiadavku transformoval a pridal by k nej prefix www.allowed.com/@@. Takúto transformovanú požiadavku by následne poslal serveru www.allowed.com. Kedže server by v tom čase nemal mať vytvorené spojenie s týmto klientom, tak by toto bola prvá požiadavka. Prvú prijatú požiadavku od klienta by skontroloval, či obsahuje našu špeciálnu značku. Keďže by tam bola, tak by toto spojenie začalo obsluhovať naše rozšírenie. Všetky požiadavky, ktoré by v rámci tohto spojenia prijalo, tak by z nich zobralo tú časť, ktorá by sa nachádzala za značkou. Keďže táto časť by mala byť normálna webová adresa, tak by webový server na túto adresu vytvoril spojenie a odpoveď na každú požiadavku, ktorú by dostal, by poslal používateľovi, ako jeho odpoveď.

Ak by pri testovaní, či spojenie značku obsahuje, bol webový server neúspešný a nepodarilo by sa mu ju nájsť, tak by fungoval štandardným spôsobom a obsluhoval by požiadavky len na jeho súbory. Ďalšie požiadavky od tohto klienta by už nekontroloval, pretože predpokladáme, že ak by pri prvej požiadavke chcel pristupovať k lokálnemu súboru, tak k lokálnym súborom bude chcieť pristupovať pomocou všetkých nasledujúcich požiadaviek v tomto spojení.

4.2 Priložené súbory

Ako sme naznačili v predchádzajúcej kapitole, tak dnešné webové stránky sa skladajú z množstva priložených súborov ako sú obrázky, písma, CSS či JavaScript. Tieto súbory je potrebné s každou požiadavkou stiahnuť. Riešilo by sa to takým spôsobom, že po tom, ako webový server stiahne webovú stránku, tak si ju pozrie a identifikuje v nej všetky odkazy na CSS, JS, obrázky. Následne všetky tieto súbory stiahne. Dnes sa mnohé takéto súbory nenachádzajú len na lokálnom serveri, ale môžu odkazovať aj na iné serveri. Deje sa to napríklad, ak chce mať webová stránka k dispozícii aktuálnu verziu súboru. Toto ale nie je žiaden problém, pretože webový server by pri sťahovaní súborov iba navštívil viac serverov. Keď webový server tieto súbory stiahne, tak je potrebné, aby si aj ich pozrel. To z toho dôvodu, lebo napríklad aj CSS súbory môžu obsahovať odkazy na obrázky, prípadne ďalšie CSS súbory. Posielanie týchto súborov používateľovi by malo prebiehať potom, ako sa tento súbor stiahne na server a skontroluje, či neobsahuje odkazy na ďalšie súbory, ktoré je potrebné stiahnuť.

4.3 JavaScript, Ajax, WebSockety a odkazy

Aj keď JavaScript priamo nepodporuje importovanie ďalšieho JavaScriptového súboru, tak sa to dá spraviť napríklad pomocou Ajaxu. Ajax sa však používa predovšetkým na získavanie dát zo servera, keď je už stránka načítaná. Funguje to spôsobom, že JavaScriptová funkcia požiada o odpoveď server. V JavaScripte ale nevieme prepísať všetky adresy a názvy súborov, pretože môžu byť dynamicky generované podľa toho, ako používateľ pracuje so stránkou. Preto sa ako najlepšie riešenie ukazuje, sledovať či sa stránka nepokúsi pristupovať k súborom na internete. Keď takéto niečo nastane, tak takúto požiadavku odchytíme, a automaticky sa k nej pripojí prefix s adresou servera, z ktorého má tento súbor stiahnuť. Rovnako navrhujeme riešiť aj všetky odkazy vedúce zo stránky. Toto riešenie by bolo rovnaké, ako keď klient vytvára prvé spojenie, pretože k nemu sa tiež automaticky dopĺňa prefix.

Podobne je však potrebné riešiť aj WebSockety, ktoré sú však odlišné v tom, že vytvárajú samostatné spojenie. Toto spojenie je treba presmerovať na webový server s naším rozšírením rovnakým spôsobom ako všetky ostatné odkazy s tým, že tento web server by vytvoril vlastné spojenie na pôvodnú adresu a medzi týmito dvomi spojeniami by presúval dáta od používateľa na server, a naopak.

4.4 Cookies

Cookies, ale aj mnohé iné funkcie, ktoré prišli spolu s HTML5 slúžia na ukladanie dát u používateľa. Problém s nimi nastáva v tom, že sú viazané na doménu. V našom návrhu by to znamenalo, že dve rôzne stránky, ku ktorým by sa pristupovalo cez rovnaký server, www.allowed.com/@@www.forbidden.com a www.allowed.com/@@www.forbidden2.com,

by vyzerali, že sú na tej istej doméne, a preto by mali tieto dáta spoločné. Toto však nie je vhodné. Preto je potrebné, aby si klient udržiaval dáta podľa ich skutočnej adresy. Toto na štastie nie je až také zložité, pretože klient vie, k akej stránke chce pristupovať, a teda vie k nej priradiť dáta, ktoré dostane. Keď chce cookies poslať spolu s požiadavkou, tak sa môže správať štandardným spôsobom, pretože ak chce navštíviť stránku www.forbidden.com a má k nej cookies, tak ich pripojí do požiadavky a až potom je požiadavka upravená. Vďaka tomuto sú tieto dáta nezávislé od použitia konkrétneho servera.

4.5 Hľadanie a výber serverov

Otázka hľadania a výberu serverov podporujúcich naše rozšírenie je veľmi dôležitá, pretože ak by klient o nich nemal informáciu, tak by nevedel, kam má svoje požiadavky smerovať. Preto navrhujeme mať viacero centrálnych serverov, na ktoré by sa všetky servery s naším rozšírením hlásili. V podstate, vždy keď by sa na serveri zaplo naše rozšírenie, tak by oznámilo centrálnemu serveru, že je schopné fungovať a že môže adresu tohto servera rozšíriť. Tieto centrálne servery by si udržiavali zoznam všetkých serverov s naším rozšírením a navzájom by si vymieňali informácie keď zistia, že existuje ďalší server. Tento zoznam by ale nemohol byť voľne k dispozícii, pretože inak by skončil u cenzora ako čierny zoznam. Namiesto toho by klient obsahoval malú integrovanú podmnožinu adries centrálnych serverov, od ktorých by si v prípade potreby pýtal adresy serverov, ktoré môže používať. Tieto servery by v intervaloch obmieňal, aby boli čo najviac rovnomerne vyťažené. Dať k dispozícii tieto IP adresy priamo do klienta ale znamená, že by k nim mal prístup aj cenzor, a teda by vedel, čo má zablokovať. Toto by však nepostihovalo všetkých používateľov rovnako, pretože aj v súčastnosti v mnohých krajinách, kde sa uplatňuje cenzúra, nie je obmedzený prístup k riešeniam na jej obchádzanie a teda predpokladáme, že ani prístup k týmto serverom by nebol všade blokovaný. Každopádne je potrebné, aby mal používateľ možnosť do klienta samostatne tieto adresy vložiť. Či už adresy serverov, ktoré chce používať alebo adresy centrálnych serverov.

4.6 Šifrovanie

Ako pri každom riešení určenom na obchádzanie cenzúry, aj pri našom riešení je potrebné, aby komunikácia prebiehala šifrovane. Náš návrh počíta s tým, že celá komunikácia by prebiehala ako klasické HTTPS spojenie. Cenzor by túto komunikáciu nevedel odlíšiť od ostatného HTTPS spojenia a teda by napríklad nevedel určiť, či pri prístupe k stránke www.allowed.com sa používateľ snaží pristupovať k lokálnym súborom, alebo požaduje, aby mu server stiahol súbor z blokovaného servera.

4.7 Spôsoby blokovania

Keďže je komunikácia pri použití nášho riešenia neodlíšiteľná od ostatnej HTTPS komunikácie, tak nie je možné, aby bolo naše riešenie blokované podľa použitého protokolu bez toho, aby toto blokovanie neovplyvnilo aj ostatné spojenia. Jediná možnosť, ako ho podľa protokolu blokovať, je zablokovať každé HTTPS spojenie.

Druhá možnosť blokovania je, že by cenzor blokoval IP adresy serverov, ktoré sa pri tomto riešení používajú. Cenzor však k týmto IP adresám nemá mať priamy prístup a teda by nemal vedieť zablokovať všetky súčasne. Vzhľadom na to, že aj centrálnych serverov aj webových serverov by malo byť viac, tak by cenzor potreboval zablokovať všetky ich adresy. V ideálnom prípade ak by sa toto riešenie rozšírilo, tak by cenzor potreboval blokovať viac ako 50% všetkých serverov.

Záver

V tejto práci sme popísali fungovanie cenzúry na internete, vysvetlili sme ako funguje a predstavili sme niektoré z mnohých riešení určených na jej obchádzanie. Tieto predstavené riešenia patria medzi tie najznámejšie alebo najzaujímavejšie. Uviedli sme spôsob ich použitia, kľúčové vlastnosti, ale aj ich slabé stránky či nedostatky.

Navrhli sme tiež naše vlastné riešenie, ktoré by podľa nás dokázalo účinne proti cenzúre bojovať. Popísali sme spôsob, ako by malo fungovať, akým spôsobom by malo byť implementované a ako by sme sa v tomto návrhu vysporiadali s rôznymi problémami, ako sú cookies či získavanie zoznamu serverov. V ďalšom kroku je však potrebné vytvoriť podľa tohto návrhu prototyp a otestovať použiteľnosť a funkčnosť tohto návrhu. Až potom sa dá začať implementovať, čo je však veľmi dlhodobý proces. Pre porovnanie, nástroje Tor a Freenet, ktoré sú v tejto práci popisované, sú už niekoľko rokov funkčné a používané, ale stále nie sú autormi označované ako dokončené a stále sa na nich intenzívne pracuje. Pri tom prvá verzia Toru pochádza z roku 2002, a dokonca prvá verzia Freenetu už z roku 2000.

Literatúra

[1] Internet Archive. About the internet archive, 2001. URL https://archive.org/about/.

[2] Ian Clarke. A distributed decentralized information storage and retrieval system. Master's thesis, 1999.

[3] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[4] M. Leech, M. Ganis, and Y. Lee. Socks protocol version 5. Technical report, ietf, 1996.

[5] Mark Lewis. *Comparing, Designing, and Deploying VPNs*. Cisco Press, Reading, Massachusetts, 2006.

[6] Netcraft. May 2014 web server survey, 2014. URL http://news.netcraft.com/archives/2014/05/07/may-2014-web-server-survey.html.

[7] Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, and John Palfrey. 2010 circumvention tool usage report. *Proceedings of the 19th USENIX Security Symposium*, August 2010.

[8] RWB. Enemies of the internet 2014, 2014. URL http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf.

[9] TorrentFreak. Pirate bay back in sweden's calm waters after .gy suspension, 2013. URL https://torrentfreak.com/pirate-bay-back-in-swedens-calm-waters-after-gy-suspension-131219/.

[10] Web2Mail. Web2mail, 2014. URL http://www.web2mail.com/.

[11] Brandon Wiley. Dust: A blocking-resistant internet transport protocol, 2013.

[12] Eric Wustrow, Scott Wolchok, Ian Goldberg, and J. Alex Halderman. Telex: Anticensorship in the network infrastructure. *Proceedings of the 20th USENIX Security Symposium*, August 2011.

[13] Bassam Zantout and Ramzi Haraty. I2p data communication system. In *Proceedings of ICN 2011, The Tenth International Conference on Networks*, January 2011.