Vysoké učení technické v Brně
Fakulta informačních technologií

Síťové aplikace a správa sítí

Tunelování datových přenosů přes DNS dotazy

Jakub Vlk xvlkja07

13. listopadu 2022

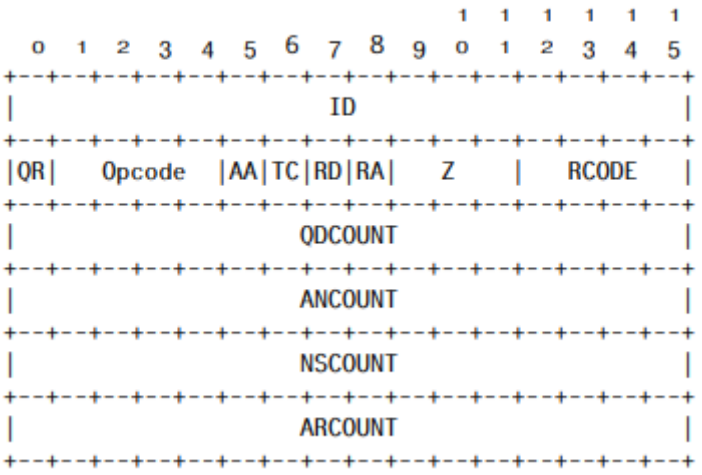
Obsah

1 Popis mechanismu pro tunelování datových přenosů prostřednictvím DNS dotazů

Tunelování probíhá prostřednictví vkládání dat do DNS dotazů. Tyto dotazy jsou posílány na server, který umí tyto dotazy zpracovat.

1.1 DNS hlavička

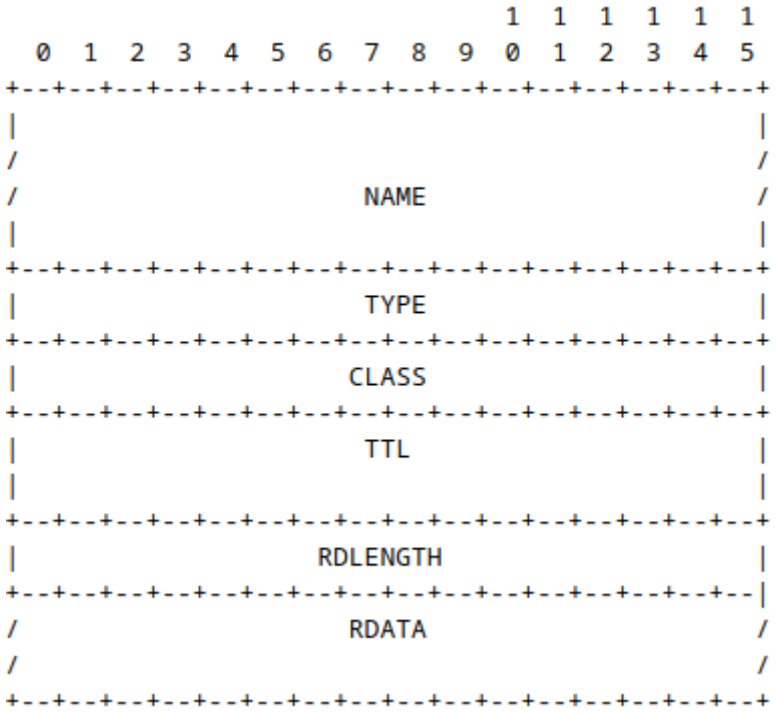
Každý DNS paket, jakýkoliv dotaz, jakákoliv komunikace protokolu DNS obsahuje DNS hlavičku ve tvaru viz obrázek 1.



Obrázek 1: Hlavička DNS protokolu

V tomto projektu jsou využívány políčka `RCODE` pro potvrzování přijetí dat a `ID` pro identifikaci přenosů od sebe. Používá se PID procesu. Ostatní políčka neobsahují speciální hodnoty.

1.2 DNS dotazy



Obrázek 2: DNS dotaz a jeho části

Do `NAME` jsou ukládána přenášená data. Zde se ve standardní DNS komunikaci umisťuje doména, na kterou se klient táže. Jinak je dotaz vytvořen standardně.

1.3 Formát DNS dotazů

Aby byl DNS dotaz validní, je potřeba dodržet následující kritéria:

- počet znaků celé dotazované domény nesmí být větší než 253 znaků (bajtů)
- jedna subdoména nesmí být delší než 63 znaků
- celý dotaz nesmí obsahovat jiné než alfanumerické znaky (velké i malé) a pomlčku

Kvůli těmto kriteriím jsou data dělena na části tak, aby ve výsledku části reprezentovaly subdomény maximální délky 63 znaků. Mimo to je taky třeba zajistit, aby znaky, reprezentující přenášená data, byly složeny pouze z dovolených znaků. Viz v sekci 4.

2 Popis návrhu a implementace klientské a serverové aplikace

2.1 Server

Server čeká dokud klient nepošle jakýkoliv dotaz. Po přijetí je dotaz přečten a je rozhodnuto a o jeho dalším osudu. Pokud se jedná o inicializační dotaz, je zaregistrován nový přenos a na dotaz je odpovězeno tak, jak popisuji v sekci 3. Pokud se nejedná o inicializační dotaz, je zjištěno, jestli je znám identifikátor v DNS hlavičce tohoto dotaz. Pokud ano, jsou data dekódována a zapsána do souboru. Více o tomto procesu v sekci 5.

2.2 Klient

Klient pošle inicializační dotaz, poté čeká na potvrzení přijetí. Soubor je čten po částech a na každou část zvlášť je aplikováno překódování base16, více o částech a jiných detailech v sekci 4. Potom jsou tyto překódované soubory vloženy do DNS dotazů a odeslány na server. Následně se čeká na odpověď. Po přečtení celého souboru je poslán ukončovací dotaz, který je popsán v sekci 3.

3 Komunikační protokol mezi klientem a serverem

Každá komunikace je zahájena inicializačním dotazem. Tento dotaz je standardní DNS dotaz. Inicializační dotaz obsahuje jako nejvyšší subdoménu řetězec `init`. Příjemce odpoví na takový DNS dotaz prázdnou DNS odpovědí, ve které je však návratová hodnota (RC - sekce 1.1) nastavena na 0 (bez chyby). Klient takovou odpověď přijme a pokračuje v komunikaci tak, že zašle první DNS dotaz obsahující data přenášeného souboru. Poté vyčká, než mu server (příjemce) odpoví stejným způsobem, jako na inicializační dotaz. Pokud odpověď nedorazí, zašle se dotaz znovu. Stane se tak 5 krát. Pokud odpověď ani tak nedorazí, je přenos ukončen. Pokud přijde správná odpověď, je zaslán další dotaz.

Například pokud používáme bázovou doménu pro tunelování `example.com`, tak inicializační dotaz bude obsahovat DNS dotaz na doménu `init.example.com`. Tento inicializační dotaz obsahuje v hlavičce protokolu DNS v políčku ID (viz v sekci 1.1) identifikátor, který se bude používat po celou dobu tohoto přenosu jako identifikátor přenosu. Po dokončení přenosu je zaslán ukončující dotaz s doménou `end.example.com`

4 Způsob kódování dat a informací

Kódovaní započne pokusem o načtením 31 bajtů, případně méně. Tato načtená data jsou překódována do base16 4.1. Načítá se pouze 31 bajtů, protože po použití base16 se množství bajtů zdvojnásobí. Potom jsou vložena do DNS dotazu ve správném formátu. To znamená, že začínají ASCII hodnotou vyjadřující počet znaků, který bude následovat. Tento proces se opakuje dokud je místo v právě tvořeném dotazu. Výsledek může vypadat takto: `<delka dat>data<delka dat2>data2<delka data3>data3<doména>`. Není nutné, aby subdomény reprezentující data byly dlouhé právě 62 znaků. Jedná se pouze o implementační zjednodušení. Příjemce dokáže zpracovat jakkoliv dlouhou subdoménu, avšak maximální délky 63 znaků (Limit DNS).

4.1 Base16

Toto překódování probíhá tak, že se prochází načtenými daty po 1 bajtu. Každý bajt je rozdělen na "polovinu"- 4 bity. Každá tato polovina je převedena na znak ze známého pole znaků, například `a-p`. Tento způsob překódování se nazývá base16. V projektu je použita moje vlastni implementace.

5 Způsob ukládání souborů na serveru

Při přijmutí inicializačního DNS dotazu je vytvořen v seznamu souborových popisovačů nový položka. Krom tohoto popisovače obsahuje taky ID (více v 1.1) a bázová doména. Při přijmutí datového dotazu je podle ID nalezen správný popisovač, do kterého se vypíšou právě příchozí data. Po přijmutí ukončujícího dotazu se z toho seznamu odstraní záznam nastavením popisovače na hodnotu NULL, tím indikuje že může být použit jiným přenosem. Tento to způsob implementace dovoluje aby probíhalo víc souběžných přenosů. Problematické u něj, že je v popisovači vyhledáváno lineárně - postupně. Seznam není nikterak řazen. V případě většího počtu přenosu by mohlo toto značně zpomalit přenosy. Seznam je dynamicky zvětšován v případě potřeby na dvojnásobek původní hodnoty.

Seznam ukládá hodnotu bázové třídy z důvodu, toho aby bylo možné program jednoduše modifikovat pro více bázových domén zároveň, případně nevyžadovat jakoukoliv bázovou doménu přímo.

6 Rozšíření

6.1 Více souběžných přenosů

Je možné, aby probíhal souběžný přenos z více klientů. Přenos těchto souborů se může překrývat. Přenos může začít nebo skočit v průběhu druhého přenosu prakticky bez omezení.

7 Omezení

Nejedinečné ID: V případě, že by dva probíhající přenosy měly stejné ID, boudou přenesená data uložena do souboru toho přenosu, jehož inicializační dotaz přišel jako první.

Moc dlouhá doména: Předpokládá se, že doména, která je vstupním parametrem, ponechá v DNS dotazu místo alespoň pro 63 znaků. Pokud toto není dodrženo, chová se program nestandardně a nedefinovaně. Je na místě aby doména byla co možná nejkratší, tak aby se maximalizoval prostor pro data.

Nevyužitý prostor: Tím, že jsou data zapisována po 31 znacích, dochází k mírnému nevyužití šířky pásma, které poskytuje DNS dotaz. Více v sekci 4.

Validní doména: Doména zadaná uživatelem musí být validní.

Velikost parametru: Parametr udávající cestu souboru ze strany klienta nesmí být delší, než 31 znaků. Toto není ověřováno.

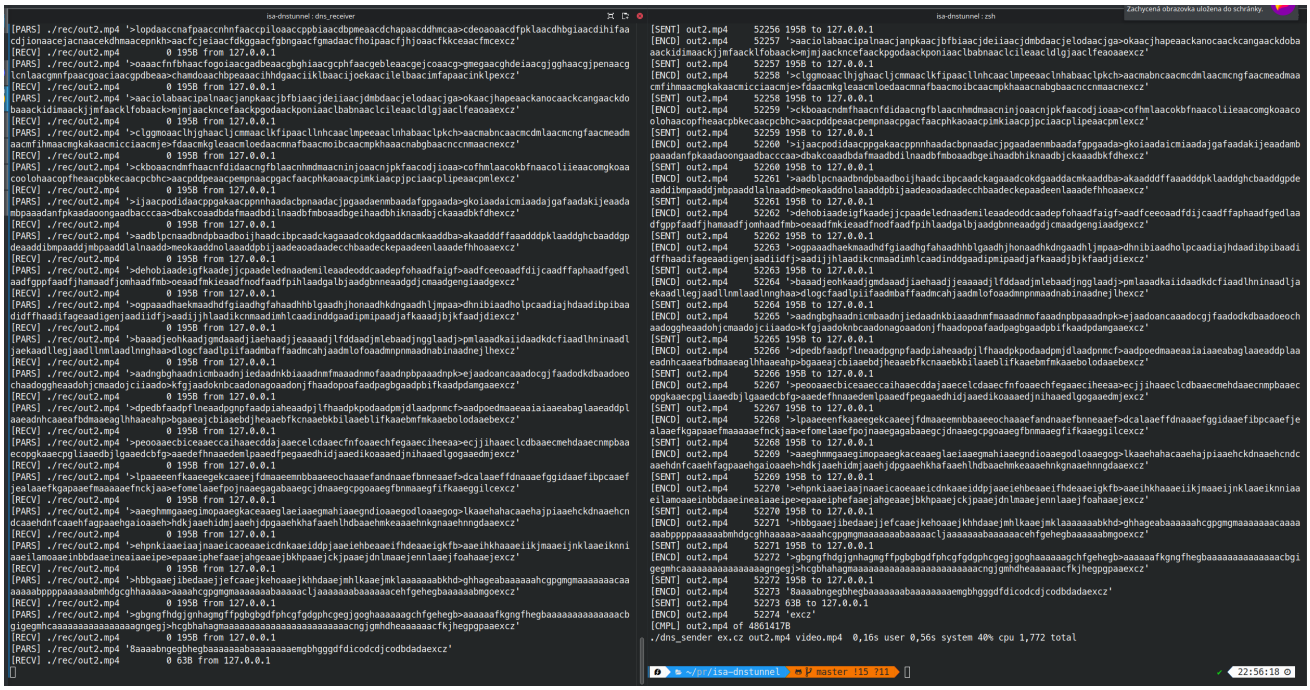
8 Popis testování a měření vytvořeného softwaru

Software jsem testoval pomocí malého skriptu, který nejdříve stáhne dva soubory z internetu – za prvé webovou stránku `fit.vutbr.cz`, která zastupuje jednodušší přenášení textu. Jako druhý soubor skript stáhne logo společnosti Google. Oba tyto soubory pošle testovací skript přes dns tunnel a nakonec je pomocí unixové utility `diff` porovná.

Výkon jsem testoval pomocí unixové utility `time`. Z času, který jsem získal, jsem spočítal přibližnou přenosovou rychlost softwaru.

$$486141/0.16 = 3038381.25B = 3.1MB$$

Přenosová rychlost je 3,1 MB za sekundu.



Obrázek 3: Testování rychlosti