Dokumentácia k projektu ISA
Filtrujúci DNS resolver

18.11.2020

Lukáš Javorský (xjavor20)

Obsah

Úvod

Na internete existuje nespočetne veľa domén, ktoré by mohli byť škodlivé pre užívateľa. Tieto domény obsahujú skripty, ktoré sa zameriavajú na špecifické diery systémových aplikácii, ktoré má každý počítač. Taktiež existujú domény, ktorých obsah je nežiadúci napríklad pre deti, alebo pre iné reštriktívne pravidlá.

Takéto domény je bohužiaľ niekedy ťažké odhaliť. Preto existujú portály, kde to už niekto spravil pre nami. Určite tam nie sú všetky, ale pre začiatok ich je tam dostatočne aby sme sa vyhli práve takýmto doménam, ktoré nám môžu uškodiť.

Súbory obsahujúce tieto domény sú zapísané v textovej forme (viď príklad[1]). Tento súbor ale sám o sebe nič neznamená a preto je potrebné vytvoriť aplikácie, ktoré vedia takéto súbory prečítať a filtrovať to všetko za nás.

Čo je to DNS?

DNS alebo inak Domain Name System je systém pre preklad doménových mien na IP adresy[2]. Tento systém komunikuje s klientom nad UDP vrstvou, ktorú si vysvetlíme v kapitole „Čo je UDP?“. To je jeho základná a najpoužívanejšia funkcionalita, ale vie toho omnoho viac. Pre tento projekt je potrebné pochopiť len už spomínanú funkciu a to preklad doménového mena (napr. www.google.com) na IP adresu (napr. 216.58.201.110).

Prečo je DNS preklad potrebný v internete?

Možno ste už počuli, že počítače nefungujú ako ľudia, ale fungujú, riadia sa a komunikujú v binárnej sústave (t.j. 0 a 1). Tým pádom by počítač nerozumel ako na koho server sa má dotazovať ak mu zadáte „google.com“. Počítač ale rozumie IP adresám, tým pádom keď mu nejakú zadáte, vie kam má komunikáciu preposielať. Na počiatkoch internetu sa komunikovalo len pomocou IP adries, tie sú ale ako asi uznáte dosť ťažké na zapamätanie, preto bol vytvorený DNS.

Dotaz (Query) A

To že preklad doménového mena na IP adresu robí DNS už vieme. Tento preklad ale musí byť niečím podmienený. Vtedy na rad prichádzajú dotazy.

Typov dotazov na DNS server je naozaj veľa[3], v našom prípade ale stačí pochopiť jeden a to typ **A**. Tento typ označuje, že sa klient požaduje preklad doménového mena na IP adresu. Preto ako vstup dotazu je doménové meno a odpoveď od DNS servera obsahuje (pokiaľ ju našiel) IP adresu, ktorá korešponduje s doménovým menom.

DNS paket

Práve v tejto aplikácii sa veľmi často pracovalo s DNS hlavičkou. Táto hlavička popisuje veľa vecí, tie tu si ale môžete podrobne prečítať v príslušnom RFC [2] na kapitole 4.

[1] https://pgl.yoyo.org/adservers/serverlist.php?hostformat=nohtml&showintro=1
[2] https://cs.wikipedia.org/wiki/IP_adresa
[3] https://en.wikipedia.org/wiki/List_of_DNS_record_types

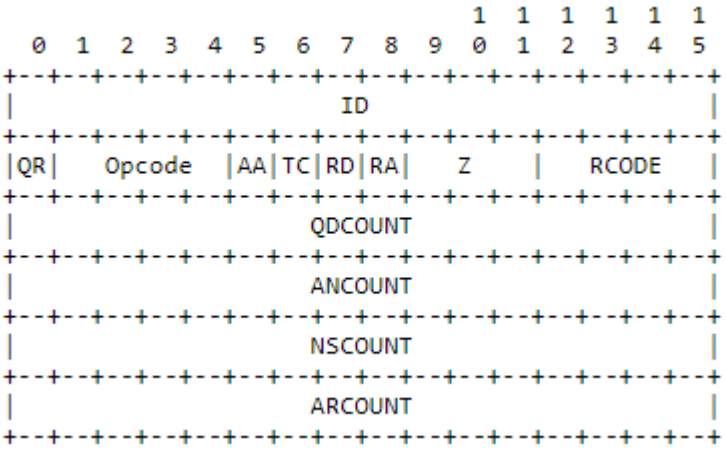


Figure 1 DNS hlavička, zdroj:[2]

Taktiež sa pracovalo s DNS otázkou, ktorá obsahuje doménu, ktorú chce klien preložiť. Preto bolo potrebné túto doménu z otázky vykrojiť a prispôsobiť jej ďalšie kroky.

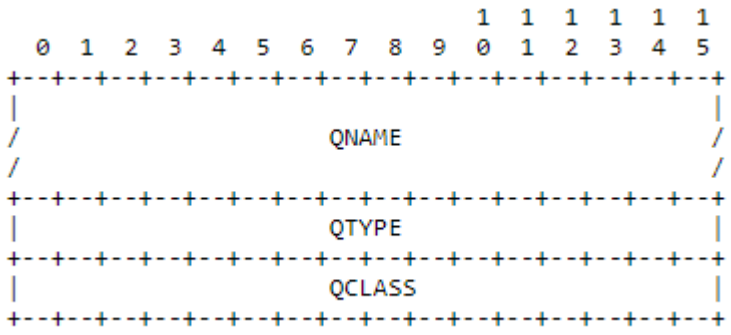


Figure 2 DNS otázka, zdroj:[2]

Čo je UDP?

User Datagram Protocol je protokol na transportnej vrstve, ktorý využíva práve DNS. Tento protokol je implementovaný tak, že server počúva na konkrétnom porte a v prípade dotazu ho spracuje, a pošle odpoveď naspäť na tento port. Keďže je UDP vytvorený aby bol hlavne rýchly, stráca tým na bezpečnosti. Preto je nutné si najprv premyslieť, či nám nevadí, že našu komunikáciu môže ten kto ju odchytí aj prečítať. Taktiež musíme počítať s tým, že sa datagramy stratia v sieti. UDP totižto nekontroluje, či pakety v poriadku dorazili a preto je to úlohou klienta, aby to zaistil.

DNS a UDP

To že DNS je postavený nad UDP protokol už spomenuté bolo. Otázka je ale prečo. Zoberte si príklad, keby musíte čakať už aj niekoľko sekúnd viac pri načítavaní videa o základoch sieťovej komunikácie. Určite by vás to po niekoľkých takýchto skúsenostiach prestalo baviť. Preto sa rozhodlo, že je dôležitejšie aby preklad bol rýchly a nemusí byť až taký bezpečný.

Filtrujúci DNS resolver

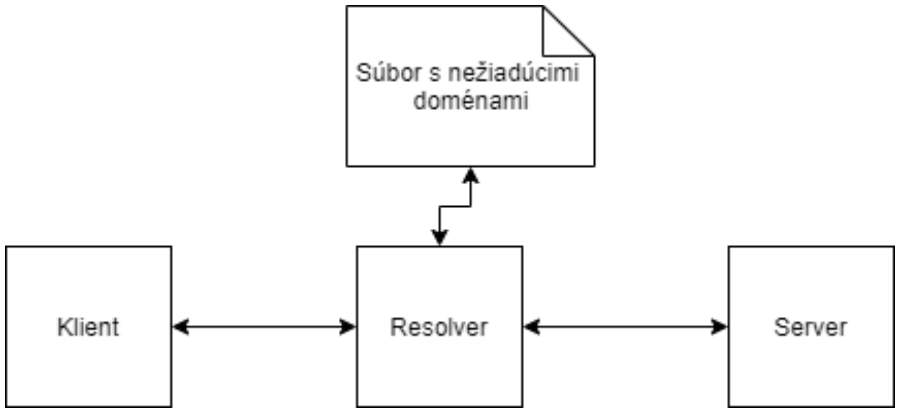
Prvé slovo „filtrujúci“ už naznačuje, že bude niečo filtrovať. Sú to práve nežiadúce domény, ktoré sa spomínajú v predošlom odseku. Resolver zistí akú doménu mu klient poslal pre preklad a ešte pred tým ako túto doménu preloží skontroluje, či nie je v zozname škodlivých/zakázaných domén.

Návrh aplikácie

Aplikácia zastupuje funkciu lokálneho DNS serveru, ktorý kontroluje požadované doménové mená. V prípade, že doména, ktorú chce klient preložiť je zakázaná, resolver vráti dotaz s korešpondenčným návratovým kódom (**RCODE** v DNS hlavičke). Návratové kódy sú viac popísané v kapitole Implementácia.

Pokiaľ ale tento dotaz je správny, resolver sa mení na klienta a dotazuje sa na server zadaný užívateľom s tým istým dotazom (tzn. rekurzivný dotaz).

Návrh aplikácie si preto vieme zjednodušene predstaviť ako nasledujúci obrázok.



Implementácia

Implementáciu môjho DNS resolveru som navrhol podľa zadania školského projektu. Toto zadanie špecifikovalo, že resolver má riešiť len dotazy s typom A. Ostatné dotazy sú vracané s návratovým kódom rovným **4**, ktorý symbolizuje, že táto funkcionalita nie je implementovaná.

Ďalej pokiaľ je dotaz správny, sa kontroluje doména. Pokiaľ je táto doména v zozname zakázaných resolver vráti dotaz rovnako ako v predošlom prípade, ale s návratovým kódom rovným **5** (Odmietnutý).

Ak ale doména v zozname nie je, sa tento dotaz posúva ďalej. Resolver sa preto správa ako dočasný klient a posiela dotaz na server zadaný užívateľom. Pokiaľ tento server nie je validný, resolver vracia dotaz klientovi s návratovým kódom **2** (Problém serveru).

V prípade správneho serveru, sa tento dotaz vyhodnotí a resolver ho príjme a ďalej prepošle klientovi.

Pri každom odoslaní odpovede klientovi sa nastavuje QR príznak v DNS hlavičke na hodnotu **1**. Táto hodnota symbolizuje že ide o odpoveď a nie o dotaz.

Použitie

Aplikácia je písaná v programovacom jazyku C a preto ju treba najprv preložiť. O preklad sa nám postará **Makefile**, preto stačí spustiť: `make` v adresári aplikácie. Týmto by sa mal vytvoriť binárny súbor s názvom **dns**.

Použitie aplikácie **dns** je možné nájsť v README.md súbore alebo spustením súboru s možnosťou `--help`. To znamená `./dns –help`.

Argumenty

Aplikácia potrebuje pre jej spustenie 2 (voliteľne 3) argumenty, ktoré môžu byť zadané v ľubovoľnom poradí.

Dva povinné argumenty sú:

- -s <SERVER> - definuje server, na ktorý sa má náš lokálny resolver dotazovať v prípade validného dotazu.
- -f <FILTER_FILENAME> - definuje cestu k súboru s nežiadúcimi doménami.

Voliteľný:

- -p <PORT> - definuje port na ktorom má lokálny resolver počúvať. Pokiaľ tento argument nie je prítomný, uvažuje sa port 53.

Príklad použitia

`dns -s 8.8.8.8 -f domains.txt -p 42420`

Obmedzenia programu

Program nedokáže prekladať ani akokoľvek pracovať s IPv6 paketmi. Taktiež podporuje zadanie serveru (-s argumet) len vo forme IP adresy.

Literatúra

[1] Študijná literatúra a príklady predmetu ISA

[2] RFC1035

[3] UDP Server-Client implementation in C

[4] Socket Programming in C/C++