VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta informačních technologií

SÍŤOVÉ APLIKACE A SPRÁVA SÍTÍ

2021

Projekt – Klient POP3 s podporou TLS

Dokumentácia

Peter Rúček (xrucek00) 5. november 2021

Obsah

1. Úvod

Táto dokumentácia popisuje problematiku, funkcionalitu, návrh a implementáciu aplikácie *popcl*. *Popcl* je POP3 command-line klient s podporou TLS/SSL. Tento program umožňuje sťahovať a mazať e-maily na mailových serveroch, pomocou protokolu POP3 a POP3s.

2. Uvedenie do problematiky

2.1. POP3

POP (Post Office Protocol) je internetový protokol, ktorý sa používa pre sťahovanie e-mailových správ zo vzdialeného serveru na klienta. Jedná sa o aplikační protokol pracujúci cez TCP/IP spojenie. V súčasnosti je používaná najmä tretia verzia (POP3), ktorá bola štandardizovaná v roku 1996 v RFC 1939.

Protokol POP3 má pre svoje účely vyhradený TCP port 110. Komunikácia prebieha na princípe výmeny správ medzi klientom a serverom. Príkaz vždy začína na začiatku riadku, v základnej implementácií POP3 majú príkazy 3 alebo 4 znaky. Príkazy nerozlišujú veľké a malé písmena. Za príkazom môžu nasledovať ďalšie argumenty oddelené medzerami. Riadky sú oddeľované pomocou CRLF. Každá odpoveď od serveru musí začínať indikáciou stavu operácie – buď +OK, alebo -ERR.[1]

2.2. POP3 s TLS/SSL

SSL je skratka pre Secured Socket Layer, TLS je skratkou pre Transport Layer Security a je len novšou verziu SSL – v podstate ide o bezpečný spôsob poskytovania autentifikácie a šifrovania počas online komunikácie medzi počítačom a poštovým serverom. [2]

Takmer všetky dnes používané metódy šifrovania využívajú verejné a súkromné kľúče. Tieto kľúče sa považujú za oveľa bezpečnejšie ako staršie symetrické kľúče. Pri verejných a súkromných kľúčoch sa používajú dva kľúče, ktoré sú matematicky prepojené (pár kľúčov), ale sú odlišné. To znamená, že správu

[1] *Wikipedia*. (23. 7 2021). Dostupné na Internete: https://cs.wikipedia.org/wiki/Post_Office_Protocol

[2] *Purple dog*. [citované dňa 4.11.2021] Dostupné na Internete: https://www.purpledogdesign.com/clients/knowledgebase/58/What-is-SSL-or-TLS-and-do-I need-a-secure-email-connection.html

zašifrovanú verejným kľúčom nemožno dešifrovať rovnakým verejným kľúčom. Na dešifrovanie správy je potrebný súkromný kľúč.

SSL/TLS používa systém verejných a súkromných kľúčov na šifrovanie údajov a integritu údajov. Verejné kľúče môžu byť sprístupnené komukoľvek, preto termín „verejné“.

Z tohto dôvodu sa naskytá otázka dôvery, konkrétne: Ako poznať, že konkrétny verejný kľúč patrí osobe/entite, za ktorú sa vydáva. Odpoveďou je používať digitálny certifikát. Digitálny certifikát poskytuje prepojenie medzi verejným kľúčom a entitou, ktorá bola overená (podpísaná) dôveryhodnou treťou stranou (certifikačná autorita). Digitálny certifikát poskytuje výhodný spôsob distribúcie dôveryhodných verejných šifrovacích kľúčov. [3]

3. Základné informácie o programe

Program je napísaný v jazyku C++ 11. Okrem štandardných knižníc využíva knižnicu OpenSSL a BIO API pre komunikáciu so serverom. Aplikácia podporuje 3 typy spojenia so serverom:

- Nešifrované spojenie na porte 110 (väčšina POP3 serverov už dnes nepodporuje)
- STLS šifrované spojenie – najskôr sa nadviaže nešifrované spojenie a na šifrovanie sa prepne po zaslaní príkazu STLS
- Šifrované spojenie POP3s na porte 995 – komunikácia je od začiatku po koniec šifrovaná.

V aplikácií *popcl* sa každá táto možnosť dá zvoliť konkrétnym prepínačom. Ďalej sa pomocou prepínačov dá nastaviť či chceme sťahovať iba nové správy zo servera, alebo či chceme vymazať všetky správy na serveri.

[3] Cope, S. (2. 1 2021). *Steves internet guide*. Dostupné na Internete: http://www.steves-internet-guide.com/ssl-certificates-explained/

4. Návrh aplikácie

V programe je využitý objektový návrh a je rozdelený do 3 modulov:

4.1. popcl

Vstupný bod programu, v tele modulu je len funkcia *main()*, ktorá inštanciuje triedy PopOptions a POP3. Tento modul zapisuje na *stdout* počet stiahnutých/ vymazaných správ a vracia návratový kód programu (OK pre 0).

4.2. Trieda PopOptions

Slúži na spracovanie argumentov príkazového riadku. Vykonáva naplnenie privátnych premenných dátami potrebnými v triede POP3. Takisto kontroluje či súbory a priečinky, ktoré sú parametrami niektorých prepínačov, existujú. Trieda obsahuje verejnú metódu *Create(),* ktorá po zavolaní vykoná všetky kontroly a spracovania argumentov. Pri chybe vypíše danú chybu na *stderr* a vráti návratový kód ARG_ERR 1.

4.3. Trieda POP3

Táto trieda vykonáva kompletnú komunikáciu zo serverom, od nadviazania spojenia až po jeho ukončenie. Trieda obsahuje jedinú verejnú metódu – *Execute(),* ktorá vykoná funkcionalitu predpísanú zadanými prepínačmi. Pri chybe vypíše danú chybu na *stderr* a vráti návratový kód POP_ERR 2.

5. Popis implementácie

V tejto časti sú popísané základné časti programu a zaujímavejšie časti zdrojového kódu.

5.1. Parsovanie argumentov

Ako bolo spomenuté vyššie, celá táto časť prebieha v triede PopOptions. V tele funkcie *ArgumentParse()* sa v cykle postupne prechádzajú všetky prepínače a parametre a validujú sa. Zaujímavejšou pasážou parsovania argumentov bolo hľadanie servera medzi parametrami, keďže jeho pozícia sa môže nachádzať kdekoľvek. Slúži na to funkcia *FindServer(),* ktorá musí prejsť všetky *argv* a podľa ostatných argumentov sa do pomocného poľa značí kde server byť nemôže. Pre úspešné nájdenie servera sa v poli, po prejdení všetkých argumentov, musí nachádzať iba jeden index na ktorom sa môže nachádzať.

5.2. Pripojenie k serveru

Podľa toho aký druh pripojenia zo serverom sa má vykonať, sa vykonávajú rôzne akcie. Pri nešifrovanej variante a pri variante šifrovanej od začiatku (pop3s) sa využíva funkcia *BIO_do_connect()*, s tým rozdielom, že pri šifrovanej variante sa naviac nastavia rôzne ssl parametre a skontrolujú sa certifikáty oboch strán. Pri STLS variante sa najskôr vytvorí nešifrované spojenie, ďalej bezprostredne po pripojení posielame serveru príkaz STLS, čím sa dožadujeme o prepnutie na šifrovanie, pri ktorom sa opäť musia nastaviť viaceré ssl parametre, následne sa už nepracuje pomocou BIO funkcií, ale pomocou SSl funckií a takisto ako v predošlom prípade sa skontrolujú certifikáty.

5.3. Komunikácia zo serverom

Pre komunikáciu sa využívajú funkcie *WriteMessage()* a *ReadMessage()*. Pre poslanie požiadavku serveru sa teda využíva funkcia *WriteMessage()*, ktorá ako parameter berie presné znenie správy - príkaz ktorý chceme poslať. Napr. *WriteMessage("RETR 1 \r\n")*. Hneď po odoslaní je treba prečítať odpoveď, pomocou *ReadMessage()*. Ona ako parameter berie string ktorý by sa mal nachádzať na konci správy, tým určuje či sa odpoveď odoslala celá. Takisto sa v tejto funkcií kontroluje či server odoslal pozitívnu (+OK) alebo negatívnu (-ERR) odpoveď. Napr. *ReadMessage("\r\n.\r\n")*.

Hneď po pripojení je potrebné prečítať uvítaciu správu servera bez toho aby sa niečo pred tým poslalo. Ďalej sa musí zaslať užívateľské meno a heslo. Po úspešnom prevedení týchto krokov ja klient vo fáze kedy si môže od servera pýtať informácie o mailoch nachádzajúcich sa v e-mailovej schránke. Po dokončení práce s e-mailmi ukončíme spojenie so serverom zaslaním príkazu QUIT.

5.4. Sťahovanie a ukladanie e-mailov

Aby bol zaslaný e-mail je potrebné serveru poslať príkaz RETR *num*, kde *num* predstavuje číslo e-mailu v mailovej schránke. Túto správu je však potrebné pred uložením spracovať. Treba vymazať prvý riadok odpovede kde server poslal status odpovede a počet oktetov daného e-mailu. A keďže každý e-mail končí tzv. ukončovací oktetom ("\r\n\.\r\n"), pridáva ďalšiu bodku navyše ak sa v tele správy nachádza tento ukončovací oktet. Preto pred uložením správy je potrebné ešte tieto prebytočné bodky vymazať. Následne sa môže e-mail uložiť. Uloží sa do adresára zadaného povinným parametrom prepínača -o, pod názvom :

“uživateľské meno na serveri“ + “_mail_“ + “číslo e-mailu na serveri“ + “.eml“ (napr. xrucek00_mail_1.eml) .

5.5. Mazanie e-mailov

Pri zadaní prepínača -d sa nesťahujú žiadne e-maily zo serveru, ale vymažú sa všetky e-maily nachádzajúce sa na serveri. Zasiela sa príkaz DELE *num*, kde *num* predstavuje číslo e-mailu v mailovej schránke a vymažú sa takto postupne všetky.

5.6. Vlastné riešenia

5.6.1. Sťahovanie iba nových e-mailov

Pri zadaní prepínača -n sa majú zo serveru stiahnuť iba nové správy. To ako to realizovať, či je správa nová u protokolu POP3 je problematické. V tomto programe sa využíva fakt, že každá správa má na serveri unikátne ID, a dá sa naň dotázať príkazom UIDL *num*, kde *num* predstavuje číslo e-mailu v mailovej schránke. V aktuálnom adresári sa vytvorí súbor “.UIDL_db“ kde sú uložené UID všetkých stiahnutých e-mailov. Takže vždy keď sa ide sťahovať e-mail (nemusí byť zapnutý prepínač -n), sa zistí UID daného e-mailu a pokiaľ sa nenachádza v súbore tak sa doňho zapíše. Rozdiel v tom, či je zapnutý prepínač -n alebo nie, je v tom, že keď nie je zapnutý tak skontroluje či sa v súbore dané UID nachádza a keď je tak síce do súboru nezapíše UID ale e-mail sa stiahne aj tak. Keď je prepínač zapnutý tak sa takto stiahnu iba správy ktoré nie sú lokálne stiahnuté.

5.6.2. Prepínače -d a -n naraz

Táto možnosť je v aplikácií implementovaná tak, že sa prepínač -d ignoruje. Je to z toho dôvodu, že mazanie je dosť zákerná vec a užívateľ sa mohol iba pomýliť a sémantika zmazať iba nové správy pravdepodobne nemá nijaké uplatnenie. Takže sa stiahnu iba nové správy.

5.6.3. Neexistujúci súbor alebo adresár

Pokiaľ dané súbory alebo adresáre neexistujú, program vypíše chybu, ktorou na to upozorní, aplikácia teda nevytvára nové adresáre.

6. Návod na použitie

Program *popcl*, umožňuje čítať elektronickú poštu skrz protokol POP3 (RFC 1939 s rozšírením pop3s a POP3 STARTTLS - RFC 2595). Program podporuje iba autentizáciu príkazmi USER/PASS. Program po spustení stiahne správy uložené na servery a uloží ich do zadaného adresára (každú správu zvlášť). Na štandardní výstup vypíše počet stiahnutých správ. Pomocou dodatočných parametrov je možné funkcionalitu meniť.

Použitie:
popcl <server> [-p <port>] [-T|-S [-c <certfile>] [-C <certaddr>]] [-d] [-n] -a <auth_file> -o <out_dir>

Poradie parametrov je ľubovoľné. Popis parametrov:

- Povinne je uvedený názov <server> (IP adresa, alebo doménové meno) požadovaného zdroja.
- Voliteľný parameter -p špecifikuje číslo portu <port> na serveri.
- Parameter -T zapína šifrovanie celej komunikácie (pop3s), pokiaľ nie je parameter uvedený použije sa nešifrovaný variant protokolu.
- Parameter -S naviaže nešifrované spojenie so serverom a pomocou príkazu STLS (RFC 2595) prejde na šifrovanú variantu protokolu.
- Voliteľný parameter -c definuje súbor <certfile> s certifikátmi, ktorý sa použije pre overenie platnosti certifikátu SSL/TLS predloženého serverom (použitie len s parametrom -T, alebo -S).
- Voliteľný parameter -C určuje adresár <certaddr>, v ktorom sa majú vyhľadávať certifikáty, ktoré sa použijú pre overenie platnosti certifikátu SSL/TLS predloženého serverom. (Použitie len s parametrom -T, nebo -S.)
- Pokiaľ nie je uvedený parameter -c ani -C, tak sa použije úložisko certifikátov získané funkciou SSL_CTX_set_default_verify_paths().
- Pri použití parametru -d sa zašle serveru príkaz pre zmazanie správ.
- Pri použití parametru -n sa budú čítať a sťahovať iba nové správy.
- Povinný parameter -a <auth_file> vynucuje autentizáciu (príkaz USER), obsah konfiguračného súboru <auth_file> je zobrazený nižšie.
- Povinný parameter -o <out_dir> špecifikuje výstupní adresár <out_dir>, do ktorého má program stiahnuté správy uložiť.

Konfiguračí súbor s autentizačnými údaji obsahuje užívateľské meno, heslo v jednoduchom formátu (konvencia pro textové súbory v prostredí UNIX/Linux):

username = meno
password = heslo

6.1. Praktická ukážka

./popcl -o DIR -a school_aut eva.fit.vutbr.cz -T

Downloaded 1060 emails.

./popcl -o DIR -a school_aut eva.fit.vutbr.cz -T -n

Downloaded 0 new emails.

./popcl mail.websupport.sk -o ~/TEST -a right_aut_file -d

Deleted 7 emails.

./popcl mail.websupport.sk -o ~/TEST -a wrong_aut_file -d

ERROR: Password wrong.

./popcl mail.websupport.sk -f

Usage: popcl <server> [-p <port>] [-T|-S [-c <certfile>] [-C <certaddr>]] [-d] [-n] -a <auth_file> -o <out_dir>

./popcl 147.223.22.17 -o DIR -a aut_file -S

Downloaded 205 emails.

./popcl -o ~ -a school_ aut -T -d 2001:67c:1220:8b0::93e5:b00e

Deleted 1060 emails.

7. Bibliografia

Cope, S. (2. 1 2021). *Steves internet guide*. Dostupné na Internete: http://www.steves-internet-guide.com/ssl-certificates-explained/

Purple dog. (dátum neznámy). Dostupné na Internete: https://www.purpledogdesign.com/clients/knowledgebase/58/What-is-SSL-or-TLS-and-do-I-need-a-secure-email-connection.html

Wikipedia. (23. 7 2021). Dostupné na Internete: https://cs.wikipedia.org/wiki/Post_Office_Protocol