VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Síťové aplikace a správa sítí

Klient POP3 s podporou TLS

17. listopadu 2017

Rostislav Navrátil - xnavra57

Obsah

1 Abstrakt

Program popcl, který umožňuje čtení elektronické pošty skrze protokol POP3. Program po spuštění stáhne zprávy uložené na serveru a uloží je do zadaného adresáře a na standardní výstup vypíše počet stažených zpráv. Pomocí dodatečných parametrů se funkcionalita programu mění.

2 Struktura AllFlags

Jedná se o globální strukturu, která se skládá z příznaků označujicí použití parametrů popasaných v následující sekci. Příznaky jsou datového typu integer a nesou hodnotu 0 v případě, kdy příslušný parametr nebyl použit a hodnotu 1 v případě, kdy příslušný parametr použit byl. Struktura dále obsahuje proměnné typy string, do kterých se po zpracovaní parametrů uloží, nebo může uložit přihlašovací jméno, heslo, ip adresa serveru, typ ip adresy serveru, cesta k adresáři certifikátů, cesta k certifikačnímu souboru a cesta k výstupnímu adresáři. Struktura obsahuje i struktury `sockaddr_in` pro funkce, které se zabývají internetovými adresami, číslo socketu a ukazatel na SSL.

3 Parametry

Na zpracování parametrů je použita funkce getopt z knihovny `getopt.h` [1]. Funkce zpracuje všechny použité parametry a v globální struktuře `AllFlags` nastaví příznaky použitých parametrů na hodnotu 1. Během zpracování parametrů dochází ke kontrole, zda se uživatel nesnaží během jednoho volaní programu, použít jeden parametr vícekrát. Tento jev vede k ukončení programu s hodnotou číslo 1 a na standartní chybový výstup se vypíše oznámení o chybě. Po zpracování parametrů dochází ke kontrole špatně použité kombinace parametrů, které opět vedou k ukončení programu a výpisu oznámení na standartní chybový výstup. Dále proběhne ošetření portu zadaného uživatelem, nebo jeho nastavení, pokud nebyl použit parametr -p [2][3].

3.1 Použití parametrů

```
popcl <server> [-p <port>] [-T/-S [-c <certfile>] [-C <certaddr>]] [-d] [-n]
 -a <authfile> -o <outdir>
```

3.2 Jméno serveru

Povinný parametr (IP adresa, nebo doménové jméno) požadovaného zdroje.

3.3 Číslo portu

Volitelný parametr -p specifikuje číslo portu na serveru. Jedinné povolené hodnoty jsou 110 a 995. Výchozí hodnota portu je určena podle způsobu komunikace ze servrem. V případě nešifrované komunikace je nastaven port 110 a v případě čistě šifrované (Použití parametru -T) je nastaven port 995 [2][3].

3.4 Šifrování celé komunikace

Volitelný parametr -T zapíná šifrování celé komunikace (pop3s), pokud není parametr uveden použije se nešifrovaná varianta protokolu. Parametr nelze použít v kombinaci s parametrem -S.

3.5 TLS

Volitelný parametr -S naváže nešifrované spojení se serverem a pomocí příkazu STLS přejde na šifrovanou variantu protokolu. Parametr nelze použít v kombinaci s parametrem -T [3].

3.6 Certifikační soubor

Volitelný parametr -c definuje soubor s certifikáty, který se použije pro ověření platnosti certifikátu SSL/TLS předloženého serverem (použití pouze s parametrem -T, nebo -S).

3.7 Certifikační složka

Volitelný parametr -C určuje adresář, ve kterém se mají vyhledávat certifikáty, které se použijí pro ověření platnosti certifikátu SSL/TLS předloženého serverem. (Použití pouze s parametrem -T, nebo -S.)

3.8 Mazání zpráv

Volitelný parametr -d Smaže všechny zprávy na serveru.

3.9 Práce s novými zprávami

Volitelný parametr -n Stahuje ze serveru pouze ty zprávy, které nejsou uloženy ve složce, kterou určuje parametr -o. V kombinaci z parametrem -d smaže ze serveru zprávy, které jsou již uloženy ve složce, kterou určuje parametr -o.

3.10 Výstupní adresář

Povinný parametr -o specifikuje výstupní adresář, do kterého má program stažené zprávy uložit. Adresář musí existovat.

3.11 Autentizace

Povinný parametr -a vynucuje autentizaci z obsahu konfiguračního souboru.

4 Autentizační soubor

Má přesně definovaný formát:

```
username = jmeno
password = heslo
```

5 Běh programu

5.1 Zpracování adresy serveru

Po zpracování parametrů je volána funkce `kindOfServerAddr`. Jako parametr funkce je zde adresa serveru. Funkce zjistí jesli se jedná o IPv4, nebo IPv6 adresu a podle toho nastaví v globální struktuře příznak `ipKind` na příslušnou hodnotu. U IPv4 je tahle hodnota 2 a u IPV6 je to 10. V Případě kdy uživatel zadal doménové jméno, dojde k přeložení doménového jména na IPv4 adresu pomocí funkce `dns`, která používá funkci `gethostbyname` z knihovny `netdb.h` [4]. Funkce `dns` vrací hodnotu 0 při úspěchu a při neúspěchu hodnotu 1 čímž se vyvolá ukončení programu s hodnotou 1 a na standartní chybový výstup se vypíše příčina chyby.

5.2 Připojení k serveru

Zavolání funkce `connectToServer` způsobí vytvoření socketu a připojení k serveru. Podle přepínače `ipKind` z globální struktury, se pozná jestli se má vytvořit IPv4 nebo IPv6 socket. Po inicializaci socketu nastane připojení k serveru pomocí funkce `connect` z knihovny `sys/socket.h`.
V případě, kdy je zvolena šifrovaná komunikace (parametr -T) se provede zavolání funkce `secure`, ve které dojde k inicializaci SSL funkcí z knihovny `openssl/ssl.h`. Dále se podle přepínačů z globální struktury zjistí jestli byl zadán parametr -C, -c, jejich kombinace, nebo žádný z nich. Nejvyšší prioritu má parametr -c, který způsobí zavolání funkce `SSL_CTX_load_verify_locations(ctx,f.certFile.c_str(), nullptr)`. Proměnná `certFile` pochází z globální struktury a obsahuje cestu k certifikačnímu souboru.
Další je v pořadí parametr -C, který způsobuje volání funkce, pro načtení certifikátu.
Funkce má tvar `SSL_CTX_load_verify_locations(ctx, nullptr, f.certAddr.c_str())`, kde proměnná `certAddr` z globální ptocedury, obsahuje cestu k adresáři certifikátů. V Systému Unix se tahhle složka nachází v `/etc/ssl/certs`. V případě kdy pro tenhle účel chceme vybrat jinou složku, je potřeba ve vybrané složce s certifikáty provést příkaz `c_rehash` [5]. V případě kombinace obou parametrů se provede nejprve -c a poté -C. Poslední možností je, že není zadán ani jeden certifikační parametr a proto je nutné tenhle krok provést pomocí funkce `SSL_CTX_set_default_verify_paths` z knihovny `openssl/ssl.h`.
Na závěr proběhne ověření certifikátu a celkového výsledku SSL připojení. Pokud nastane chyba, program se ukončí s hodnotou 1 a na standartní chybový výstup se vypíše příčina chyby [6][7][4] [8].

5.3 Komunikace se servrem

Probíhá ve funkci `communication`. Dochází zde k odesílání požadavků na server a přijímání jednořádkových odpovědí ze servru. K odeslání požadavku se volá funkce `sendMessage`, která má jako parametr požadavek na server. K samotnému odeslání je určena funkce `send` z knihovnky `socket.h`. V případě použití parametru -T je použita funkce `SSL_write` z knihovny `openssl/ssl.h`.
K příjimání jednořádkových zpráv je zde použita funkce `receive_message`, která k samotnému příjmání zpráv používá funkci `recv` z knihovny `socket.h`. V případě použití parametru -T je použita funkce `SSL_read` z knihovny `openssl/ssl.h` [6][4].

5.4 Manipulace se zprávami

Ve funkci `communication` se zjistí počet zpráv na serveru a použije se jako parametr volané funkce `processingMessage`. V téhle funkci se podle přepínačů z globální struktury zjistí, jestli dojde k mazání, nebo stahování zpráv. V případě použití parametru -n se budou stahovat pouze zprávy, které nejsou uloženy ve výstupním adresáři. Nebo budou mazaný ze serveru ty zprávy, které již máme uložené ve výstupním adresáři, tudíž na serveru zůstanou pouze námi nepřečtené zprávy.
Pro vyhledávání zpráv v adresáři se používá funkce `findInFolder` [9].

5.4.1 Identifikace zpráv

Zprávy je nutné identifikovat, abychom je mohli pojmenovat a případně porovnávat se zprávami ve výstupním adresáři. Identifikace dochází `getMessageId`. Jako první se zjistí, zda server podporuje UID. V případě pozitivní odpovědi ze strany serveru, se bude pro identifikaci zpráv používat UID. Jelikož UID nemusí být podporované u všech serveru, je tu druhý způsob. Pomocí regulárních výrazů se stáhne Message-ID a použije se pro identifikaci zprávy. Tenhle způsob je méně efektivní, protože se u něho musí stahovat celá zpráva. Může nastat i to, že zpráva nebude mít Message-ID. Pro tento případ se zprávě vygeneruje název "WithoutID"a číslo zprávy a proto nebude korektně pracovat s použitým parametrem -n [3].

5.4.2 Úprava podoby zprávy

Před uložením je nutné zprávu připravit do podoby, aby splňovala Internet Message Format. Ve funkci `processingMessage` dojde k odstranění začátku zprávy za první výskyt CRLF. Dále odstranění zakončovacího znaku ".CRLF". Nakonec dojde k detekci, případně mazání zdvojených teček na začátku řádku [3] [10]. Ukládní probíhá do zvoleného adresáře pomocí parametru -o.

5.5 Ukončení zpráv

Ve funkci `main` se odešle na server příkaz QUIT, kvůli korektnímu způsobu ukonečení spojení ze serverem [3].

Reference

[1] *Parsing program options using getopt*. Dostupné na: <https://www.gnu.org/software/libc/manual>.

[2] *A List of SMTP and POP3 Server*. Dostupné na: <https://www.arclab.com/en/kb/email>.

[3] MYERS, J. G. a ROSE, M. T. *Post Office Protocol - Version 3* [Internet Requests for Comments]. [b.m.]: RFC Editor, May 1996. STD, 53. <http://www.rfc-editor.org/rfc/rfc1939.txt>. Dostupné na: <http://www.rfc-editor.org/rfc/rfc1939.txt>.

[4] PARZIALE, L., BRITT, D. T., DAVIS, C. et al. *TCP/IP Tutorial and Technical Overview 8th Edition*. [b.m.]: Vervante, 2006. ISBN 0738494682.

[5] *C rehash*. Dostupné na: <https://www.openssl.org/docs/man1.0.2/apps/c-rehash.html>.

[6] *Openssl*. Dostupné na: <https://wiki.openssl.org/index.php>.

[7] *Secure programming with the OpenSSL API*. Dostupné na: <https://www.ibm.com/developerworks/library/l-openssl/>.

[8] NEWMAN, C. *Using TLS with IMAP, POP3 and ACAP* [Internet Requests for Comments]. [b.m.]: RFC Editor, June 1999. RFC, 2595. <http://www.rfc-editor.org/rfc/rfc2595.txt>. Dostupné na: <http://www.rfc-editor.org/rfc/rfc2595.txt>.

[9] *Opendir*. Dostupné na: <ttp://man7.org/linux/man-pages/man3/opendir.3.html>.

[10] RESNICK, P. W. *Internet Message Format* [Internet Requests for Comments]. [b.m.]: RFC Editor, October 2008. RFC, 5322. <http://www.rfc-editor.org/rfc/rfc5322.txt>. Dostupné na: <http://www.rfc-editor.org/rfc/rfc5322.txt>.