



Siet'ové aplikácie a správa sietí  
**projekt - Klient POP3 s podporou TLS**

21. října 2021

Filip Brna (xbrnaf00)

# Obsah

<b>1</b>	<b>Úvod</b>	<b>2</b>
1.1	POP3 protokol . . . . .	2
1.2	príklad formátu ako je uložená správa v súbore . . . . .	2
1.3	príklad formátu konfiguračného súboru . . . . .	2
<b>2</b>	<b>Implementácia</b>	<b>3</b>
2.1	Základné informácie . . . . .	3
2.2	Main . . . . .	3
2.3	ProcessArgs . . . . .	3
2.4	CheckNextArg . . . . .	4
2.5	CheckoutDirAndFile . . . . .	4
2.6	SecureConnection . . . . .	4
2.7	NoSecureConnection . . . . .	4
2.8	BioLibFunctions . . . . .	4
2.9	DownloadEmails . . . . .	4
<b>3</b>	<b>Príklady spustenia</b>	<b>5</b>
<b>4</b>	<b>Testovanie</b>	<b>5</b>
<b>5</b>	<b>Zdroje</b>	<b>5</b>

# 1 Úvod

Cieľom projektu bolo vytvoriť program `popcl`, ktorý bude umožňovať čítanie elektronickej pošty cez protokol s rozšíreniami `POP3S` a `POP3 STARTTLS`. Program po spustení stiahne správy uložené na servery a uloží ich každú zvlášť do zadaného adresára. Na štandardný výstup vypíše počet stiahnutých správ. Programovú funkcionality je možné meniť pomocou dodatočných parametrov.

## 1.1 POP3 protokol

Post Office Protocol je internetový protokol na aplikačnej vrstve, ktorý sa využíva na prijímanie elektronickej pošty zo vzdialeného servera prostredníctvom TCP/IP spojenia. Poštový protokol je séria pravidiel o tom, ako sa má riadiť prenos elektronickej pošty medzi dvomi bodmi v sieti.

## 1.2 príklad formátu ako je uložená správa v súbore

```
Return-Path: test@mail.local
Received: from [127.0.0.1] (mail.local [127.0.0.1])
by test with ESMTPA
; Mon, 18 Oct 2021 16:22:08 +0200
Message-ID: ja645d9b6-143e-101e-f9ed-efcb3d86956a@mail.local;
Date: Mon, 18 Oct 2021 16:22:07 +0200
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
Thunderbird/91.2.0
Content-Language: sk
To: test@mail.local
From: test2 ;test2@mail.local;
Subject: test
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit
X-EsetId: 37303A29F9B99D67647261
```

Tu sa nachádza telo emailu, pred telom je hlavička a prázdny riadok.

## 1.3 príklad formátu konfiguračného súboru

Tento súbor má presne danú štruktúru a obsahuje meno a heslo k prihláseniu do emailovej schránky.

```
username = meno
password = heslo
```

## 2 Implementácia

### 2.1 Základné informácie

Projekt bol implementovaný v programovacom jazyku C++, pri implementácii som hlavne využil knižnicu `openssl`, ktorá implementáciu výrazne uľahčila keďže jadrom celého programu sú práve funkcie z tejto knihovne. Program obsahuje niekoľko globálnych premenných, ktoré sú potrebné hlavne pri priradovaní argumentov a taktiež aj pri následnom použití premenných v programe.

### 2.2 Main

Funkcia `main` na úvod volá funkciu `ProcessArgs` na spracovanie argumentov, nasleduje kontrola, či zadaný adresár alebo súbor existuje pomocou funkcie `CheckoutDirAndFile`. Ak bol program spustený s parametrom `-T` je ďalej volaná funkcia `SecureConnection`, ktorá nadväzuje so serverom šifrovanú komunikáciu, pokiaľ parameter `-T` zadaný nebol je volaná funkcia `NoSecureConnection`, ktorá nadväzuje nešifrovanú komunikáciu resp. pri použití parametru `-S` naviaže nešifrované spojenie so serverom a pomocou príkazu `STLS` prejde na šifrovanú variantu protokolu. Na konci mainu je na štandardný výstup vypísaná informácia o počte stiahnutých správ a program je ukončený s návratovým kodom 0.

### 2.3 ProcessArgs

Funkcia, ktorej účelom je kontrolovať argumenty programu a taktiež nastavenie globálnych premenných. Argumenty programu:

Použitie:

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

`<server>` - povinný argument, adresa zdroja z ktorého chceme správy sťahovať

`-p <port>` - voliteľný argument, `<port>` číslo portu

`-T` - voliteľný argument, zapína šifrovanie celej komunikácie

`-S` - voliteľný argument, naviaže nešifrované spojenie so serverom a pomocou príkazu `STLS` prejde na šifrovanú variantu protokolu

`-c <certfile>` - voliteľný argument, použitie iba s parametrom `-T`, alebo `-S`, definuje súbor `<certfile>` s certifikátmi, ktoré sa použijú pre overenie platnosti certifikátu SSL/TLS predloženého serverom

`-C <certaddr>` - voliteľný argument, použitie iba s parametrom `-T`, alebo `-S`, určuje adresár `<certaddr>`, v ktorom sa majú vyhľadávať certifikáty, ktoré sa použijú pre overenie platnosti certifikátu SSL/TLS predloženého serverom.

`-d` - zasiela serveru príkaz pre zmazanie správ

`-n` - bude pracovať iba s novými správami.

`-a <auth_file>` - povinný argument, `<auth_file>` obsahuje autentizačné údaje

`-o <out_dir>` - povinný argument, `<out_dir>` špecifikuje výstupný adresár

## 2.4 CheckNextArg

funkcia, ktorej účelom je skontrolovať nasledujúci parameter, ktorý sa má zadať pri spustení programu. Dochádza tu ku kontrole či za parametrami ako -p, -c, -C, -a, -o nasledujú im prisluchajúce dvojice v prípade, že nie, je program ukončený chybovým návratovým kódom a prisluchajúcou chybovou hláškou.

## 2.5 CheckoutDirAndFile

Funkcia na kontrolu, či existujú zadané adresáre/súbory, zistí a uloží meno a heslo z autentifikačného súboru. V prípade nesprávneho formátu autentizačného súboru alebo neexistujúceho adresára je program ukončený návratovým kódom 1 a príslušnou chybovou hláškou.

## 2.6 SecureConnection

Funkcia pre zabezpečené pripojenie k serveru, ak je zadaný argument -T, nasleduje kontrola certifikátov, ktoré sa nachádzajú v súbore z argumentov programu, pokiaľ neboli, sú nastavené predvolené certifikáty. Vo funkcii sú volané funkcie z knižnice openssl hlavne z openssl/bio.h.

## 2.7 NoSecureConnection

Funkcia pre nezabezpečené pripojenie k serveru, ak je zadaný argument -S, nasleduje prechod na šifrovanú variantu protokolu a kontrola certifikátov, ktoré sa nachádzajú v súbore z argumentov programu, pokiaľ neboli, sú nastavené predvolené certifikáty. Vo funkcii sú opäť volané hlavne funkcie z openssl/bio.h.

V tejto funkcii bola časť, ktorá je označená v kóde prevzatá z:

- otázka : OpenSSL: Promote insecure BIO to secure one
- odpoveď, autor : Martin Prikryl, datum - Mar 6 '18 at 13:54
- link: <https://stackoverflow.com/questions/49132242>

## 2.8 BioLibFunctions

V tejto funkcii prebieha takmer všetká komunikácia so serverom, ktorá pozostáva zo zasielania autentifikačných príkazov na server a následne sú kontrolované odpovede serveru. V prípade, že autentifikácia prebehne úspešne nasleduje zasielanie príkazu na sťahovanie/mazanie emailových správ. Ďalej sú z e-mailovej odpovede servera uložené informácie ohľadom ID konkrétnej správy, počet správ, celková veľkosť oktetov všetkých správ a taktiež aj veľkosť oktetov pre jednotlivé správy. V premennej `Msg` je uložená odpoveď servera na príkaz `RETR`, ktorá je neskôr použitá ako parameter pre funkciu `DownloadEmails`.

## 2.9 DownloadEmails


Úlohou tejto funkcie je vytvoriť súbor s názvom `messageID` a uložiť do neho správu z parametru `Msg`. V prípade, že bol program spúšťaný s parametrom `-n` sú stiahnuté iba správy s takým `messageID`, ktoré sa vo výstupnom adresári ešte nenachádza.

## 3 Príklady spustenia

```
./popcl mail.local -p 110 -o maildir -a testdir/authtest  
./popcl mail.local -n -o maildir -a testdir/authtest  
./popcl mail.local -d -o maildir -a testdir/authtest  
./popcl pop3.seznam.cz -o maildir -a testdir/authtestpop3seznam -S  
./popcl pop3.seznam.cz -o maildir -a pop3seznam -T -c testdir/pop3.centrum.sk.cert -C test2dir
```

## 4 Testovanie

Snímka obrazovky bola robená tak, aby bol zachytený program spúšťaný s rôznymi parametrami.



```
$ ./popcl mail.local -p 110 -o maildir -a testdir/authtest  
3 - email/s downloaded  
$ ./popcl mail.local -n -o maildir -a testdir/authtest  
2 - new email/s downloaded  
$ ./popcl mail.local -d -o maildir -a testdir/authtest  
3 - email/s deleted  
$ ./popcl pop3.seznam.cz -o maildir -a testdir/authtestpop3seznam -S  
2 - email/s downloaded  
$ ./popcl pop3.seznam.cz -o maildir -a testdir/authtestpop3seznam -T -c testdir/test2dir/2277025_pop3.cen  
trum.sk.cert -C testdir/test2dir  
2 - email/s downloaded  
$ ./popcl pop3.seznam.cz -o maildir -a testdir/authtestpop3seznam -c testdir/test2dir/2277025_pop3.cen  
Error: wrong program arguments  
$ ./popcl pop3.seznam.cz -o maildir  
Error: arguments missing
```

## 5 Zdroje

Informácie ohľadom toho ako pracuje pop3 klient som získaval z nasledujúcich zdrojov, taktiež sa tu nachádzajú aj zdroje odkiaľ som čerpal niektoré zdrojové kódy. Základne informácie a znalosti ohľadom knižnice OpenSSL som nadobúdal na týchto stránkach:

zadanie projektu vo WIS

openssl

— link: <https://www.openssl.org/docs/man1.0.2/man1/openssl.html>

— link: <https://developer.ibm.com/tutorials/l-openssl/>

s\_client

— link: [https://www.openssl.org/docs/man1.0.2/man1/s\\_client.html](https://www.openssl.org/docs/man1.0.2/man1/s_client.html)

Časť funkcie NoSecureConnection :

— otázka : OpenSSL: Promote insecure BIO to secure one

— odpoveď, autor : Martin Prikryl, datum - Mar 6 '18 at 13:54

— link: <https://stackoverflow.com/questions/49132242>