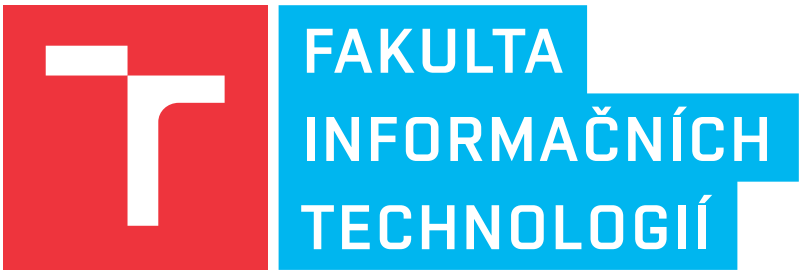
Vysoké učení technické v Brně
Fakulta informačních technologií



Dokumentácia pre predmet Síťové aplikace a správa sítí

Klient POP3 s podporou TLS

15. října 2017

Juraj Korček, xkorce01@stud.fit.vutbr.cz

Obsah

1 Úvod

Táto dokumentácia, ktorá vznikla pre potreby predmetu Síťové aplikace a správa sítí sa zaoberá vysvetlením pojmov súvisiacich s protokolom POP3, princípom činnosti tohoto protokolu, priblížením implementácie vlastného POP3 klienta, ako aj jeho použitím. Taktiež popisuje činnosť a implementáciu šifrovanej komunikácie na transportnej vrstve za použitia knižnice OpenSSL. Pri programovaní boli využité BSD sokety, čo obmedzuje použitie programu na operačné systémy UNIX/LINUX.

2 Dôležité pojmy

2.1 POP3

Protokol POP3 alebo Post Office Protocol je protokol pracujúci na aplikačnej vsrtve ISO/OSI modelu zabezpečujúci príjímanie elektronickej pošty. Tento protokol je nezabezpečený a využíva protokol transportnej vrstvy TCP a port s číslom 110. Používanie nezabezpečenej komunikácie je náchylné na odposluchy a preto sa v zásade neodporučuje.

Protokol POP3 funguje na princípe posielania štandardizovaných požiadavkov POP3 serveru, ktorý následne posiela odpoveď klientovi. Správy sú na strane klienta zobrazované offline, čím užívateľovi zaberajú nemalú časť z diskového priestoru. Značnou nevýhodou tohoto protokolu je fakt, že standardne sú spravý po stiahnutí zo servera zmazané, čo má za následok obtiažnejšie fungovanie poštovej schránky na viacerých zariadeniach a nemožnosť filtrovania prijatých správ(spam).

2.2 POP3 s TLS a STARTTLS

Keďže je protokol POP3 nezabezpečený, môže technicky zdatný človek bez väčších problémov odchytávať komunikáciu medzi klientom a serverom. Tento problém je v praxi riešený tunelovaním transportného spojenia za pomoci TLS, protokol SSL nie je z bezpečnostných dôvodov vhodné dnes používať [4]. Pri použití protokolu TLS sa štandardne využíva port 995 transportného protokolu TCP, spojenie POP3 a SSL/TLS sa často označuje ako POP3S.

Ako je už z predošlích informácií zrejmé, protokol POP3 môže štandardne fungovať na 2 portoch, zabezpečenom a nezabezpečenom. Tento fakt môže znamenať problém pre správcov POP3 servera, preto je možne používať iba jeden port napr. 110 pre šifrovanú aj nešifrovanú komunikáciu. Princíp fungovania je jednoduchý, klient naviaže nešifrované spojenie so serverom na porte 110 a následne klient pošle serveru požiadavku STARTTLS príkazom STLS, vytvorí sa šifrované spojenie a od tohoto okamihu je komunikácia zabezpečená proti odposluchu ako pri použití TLS a portu 995.

2.3 Diagram komunikácie POP3

Ako je možné vidieť na príslušnom obrázku (Obr. 1), protokol POP3 odpovedá na požiadavky klienta úvodným prefixom správy `+OK` v prípade úspešného rozpoznania a spracovania požiadavky alebo správou `-ERR`. Príkaz `QUIT` je dôležitý pri ukončovaní spojenia najmä v prípade mazania správ na serveri, pri vynechaní tohoto príkazu sa správy nezmažú.

```
S:    +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C:    APOP mrose c4c9334bac560ecc979e58001b3e22fb
S:    +OK mrose's maildrop has 2 messages (320 octets)
C:    STAT
S:    +OK 2 320
C:    LIST
S:    +OK 2 messages (320 octets)
S:    1 120
S:    2 200
S:    .
C:    RETR 1
S:    +OK 120 octets
S:    <the POP3 server sends message 1>
S:    .
C:    DELE 1
S:    +OK message 1 deleted
C:    QUIT
S:    +OK dewey POP3 server signing off (maildrop empty)
```

Obr. 1: Prehľad komunikácie servera a klienta protokolu POP3 [5]

2.4 POP3 príkazy

Príkazy pre POP3 server sú definované v RFC1939 [1], nie všetky príkazy sú však povinne implementované. Všetky príkazy, teda povinné aj voliteľné je možné vidieť na nasledujúcom obrázku (Obr. 2).

Příkaz	**Význam**
`USER`	jméno identifikující poštovní schránku
`PASS`	heslo pro přístup ke schránce/serveru
`APOP`	bezpečné přihlášení ke schránce pomocí MD5
`CAPA`	server pošle podporované algoritmy pro zabezpečení SASL
`AUTH`	zahájení SASL autentizace
`STAT`	počet zpráv ve schránce + jejich velikost
`LIST`	seznam zpráv ve schránce a jejich velikost
`RETR`	server pošle požadovanou zprávu klientovi
`DELE`	nastaví u zprávy příznak "deleted"
`RSET`	smaže příznak "deleted" u zpráv označených pro zrušení
`TOP`	server pošle klientovi hlavičku a zadaný počet řádek zprávy
`UIDL`	server vypíše jednoznačný identifikátor zprávy (MsgId)
`NOOP`	prázdný příkaz
`QUIT`	uzavření spojení, smaže zprávy označené "deleted"

Obr. 2: Prehľad príkazov protokolu POP3 [5]

3 Návrh programu

Aplikácia `popcl` sa po spustení pripojí na POP3 server na buď štandardnom porte, alebo porte definovanom užívateľom. K prihláseniu na server použije príkazy USER/PASS, pričom meno a heslo bude vyčítané zo súboru definovanom na príkazovom riadku. Následne skontroluje počet správ na serveri. Pokiaľ je zadaný prepínač na stiahnutie iba nových správ, stiahne iba

tie. Podrobný popis overovania nových správ je popísaný v implementácií. Každá správa sa uloží do separátneho súboru vo formáte IMF [3], pričom názov súboru je vytvorený z MsgId, v prípade nepodporovania príkazu `UIDL` zo sekvenčného čísla unikátneho pre danú zložku. Z dôvodu vyššieho zabezpečenia program `popcl` podporuje iba protokol TLS verzie 1.2. Pri úspešnom stiahnutí správ aplikácia vypíše jeden riadok s textom, koľko správ bolo stiahnutých. V prípade chyby počas behu sa aplikácia ukončí s chybovým hlásením.

4 Implementácia

Na tvorbu aplikácie bol použitý programovací jazyk C++ s mnohými štandardnými knižnicami pre prácu so vstpom a výstupom, ďalej knižnice pre prácu s BSD soketami a knižnica OpenSSL poskytujúca funkcie na bezproblémovú implementáciu zabezpečeného spojenia na L4 vrstve. Program je členený do modulov, no nie je písany objektovo napriek použitiu jazyka C++.

4.1 Detekcia nových správ

V tejto implementácií sa pod pojmom nové správy rozumejú správy, ktoré sa zatiaľ nenachádzajú vo výstupnom adresári. Keďže protokol POP3 neumožňuje označovanie nových správ ako protokol IMAP, je nutné vymyslieť mechanizmus, ktorý by takéto správanie napodobňoval. Kľúčovým prvkom implemnetácie v aplikácií `popcl` je fakt, že každý e-mail je ukladaný do separátneho súboru, pričom meno tohoto súboru je dané indetifikátorom správy MsgId poskytnutého serverom.

V aplikácií `popcl` je takéto správanie napodobnené nasledovne:

1. Aplikácia požiada server o identifikačné čísla e-mailov príkazom UIDL.
2. Do jednorozmerného pola `uid_email_tab` si uloží identifikačné čísla e-mailov.
3. Jednotlivé položky pola `uid_email_tab[i]` sa porovnávajú so správami už stiahnutými v priečinku definovanom užívateľom pri spustení programu.
4. Pokiaľ sa niektoré e-maily zo servera nachádzajú v lokálnom priečinku, tak sa jednotlivé položky pola `uid_email_tab` prepíšu na reťaze pola `OK`.
5. Aplikácia `popcl` porovná položky pola `uid_email_tab` a tie, v ktorých sa nachádza reťazec `OK` sa zo servera nestiahnu.

Výhodou tejto implemntácie je, že nie je nutné udržiavať žiaden pomocný súbor s identifikátormi správ, ktoré už boli stiahnuté. Možné nedostatky sú popísane v Obmedzeniach.

4.2 Mazanie spáv

Mazanie správ pri použití protokolu POP3 je v mnohým implemntáciách rozdielne. Niektorí klienti mažú správy po stiahnutí, iní po odstránení z lokálnej zložky. V aplikácií `popcl` sa pri stiahnutí správy nemažú, pokiaľ nie je nastavený prepínač `-d`. Pri použití tohoto prepínača sa mažú všetky správy z POP3 servera nehľadiac na fakt, či je alebo nie je zadaný prepínač `-n` sťahujúci iba nové správy.

4.3 Overenie platnosti certifikátu

Pri použití zabezpečeného pripojenia je nutné overiť platnoť certifikátu predloženého serverom. Na tento účel slúžia dva prepínače `-c` a `-C`, ktoré definujú buď súbor s certifikátom, alebo adresár obsahujúci cerifikáty. V implementácií `popcl` je pri neúspešnom nájdení certifikačného súboru prehľadávaný aj adresár. Overenie platnosti serverom predloženého certifikátu je uskutočňované funkciou
`SSL_get_verify_result`, kedy pri neúspešnom overení je program ukončeny s odpovedajúcim chybovým hlásením.

5 Obmedzenia

Príkaz UIDL patrí v protokole POP3 medzi voliteľné, takže jeho funkčnosť nemusí byť zaistená u každého POP3 serveru [1]. To značne komplikuje situáciu hlavne pri detekcii nových správ. Detekcia nových správ však nie je stopercentne zaručená ani pri implementácií tohoto príkazu.

Ako vyplýva z RFC1939 [1], jednoznačné identifikačné číslo správy sa nemôže znovu použiť, pokiaľ je v mailboxe správa s daným identifikačný číslo. To znamená, že po zmazaní správy s určitým identifikačným číslom môže byť identifikačné číslo znova využité. V implementácií programu `popcl` to znamená, že ak je zvolené sťahovanie iba nových správ, tak nová správa môže byť považovaná za stiahnutú a naopak pri nepoužití funkcie sťahovania nových správ, môže dôjst k premazaniu starej správy novou s iným obsahom, ale rovnakým identifikačným číslom.

Sťahovanie nových správ je založené na podpore príkazu `UIDL` na strane POP3 servera. Pri pokuse o stiahnutie iba nových správ na severi nepodporujúcom príkaz `UIDL` bude program ukončený a uživateľovi sa zobrazí zodpovedajúce chybové hlásenie, pri vynechaní tohoto prepínača budú správy stiahnuté. Tento typ riešenia bol zvolený z dôvodu, aby si užívateľ uvedomil, že nesťahuje iba nové správy, ale všetky, ktoré su v mailboxe.

Pokiaľ server nepodporuje príkaz `UIDL`, nie je možné zaistiť, že správy nebudú ukladané duplicitne. Jediným spôsobom, ako toho dosiahnuť je použitie prepínaču `-d`, ktorý správy po stiahnutí zmaže zo servera. Keďže nie je možné jednoznačne definovať mená správ pri absencii podpory príkazu UIDL a teda pri opakovanom stiahnutí ich prepísať rovnakými, sú pri nepoužití prepínača `-d` a následnom stiahnutí ukladané radšej duplicitne, ako keby mali byť prepísané. Mnoho z vyššie popísaných nedostatkov pramení z pôvodne navrhnutého sťahovania správ protokolu POP3, ktoré počíta so zmazaním správ ihneď po ich stiahnutí, eliminácia týchto nedostatkov by bola možná pri použití protokolu IMAP.

6 Použitie aplikácie

Program sa spúšťa z príkazového riadku s 3 povinnými parametrami a 7 voliteľnými, pričom na poradí parametrov nezáleží.

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

Povinné parametre programu:

<server> – ip adresa alebo doménove meno servera.

-a <auth_file> – vynucuje autentizáciu a špecifikuje cestu k súboru s autentizačnými údajmi.

-o <out_dir> – špecifikuje výstupný adresár, do ktorého sa majú ukladať správy. Pokiaľ adresár neexistuje, program sa ukončí s chybovým hlásením.

Voliteľné parametre programu:

-d – zašle serveru príkaz pre zmazanie správ.

-n – sťahovanie iba nových správ, v prípade, že server nepodporuje príkaz UIDL, program končí chybou.

-p <port> - špecifikuje číslo portu, v prípade TLS je použitý port 995 a STLS 110.

-T – zapína šifrovanie komunikácie (pop3s).

-S – naviaže nešifrované spojenie a príkazom STLS prejde na šifrovanú variantu protokolu.

-c <certfile> – definuje súbor s certifikátmi potrebný pre overenie platnosti certifikátu predloženého serverom. Použitie je možné iba s parametrom ***-T*** alebo ***-S***.

-C <certaddr> – definuje adresár, v ktorom sa majú vyhľadať certifikáty potrebné pre overenie platnosti certifikátu predloženého serverom. Použitie je možné iba s parametrom ***-T*** alebo ***-S***.

-h – zobrazí nápovedu programu.

7 Záver

Aplikácia bola testovaná na operačnom systéme Debian 9 a prekladaná prekladačom g++ za pomoci súboru Makefile. Testovanie prebiehalo na POP3 serveroch spoločností Websupport, Seznam a Atlas, pričom neboli zistené žiadne nedostatky v implemetácií.

Literatúra

[1] IETF: RFC1939: Post Office Protocol - Version 3. [online], 2017, [cit. 10. 10. 2017]. URL "https://tools.ietf.org/html/rfc1939"

[2] IETF: RFC2595: Using TLS with IMAP, POP3 and ACAP. [online], 2017, [cit. 10. 10. 2017]. URL "https://tools.ietf.org/html/rfc2595"

[3] IETF: RFC5322: Internet Message Format. [online], 2017, [cit. 10. 10. 2017]. URL "https://tools.ietf.org/html/rfc5322"

[4] IETF: RFC7568: Internet Message Format. [online], 2017, [cit. 10. 10. 2017]. URL "https://tools.ietf.org/html/rfc7568"

[5] Matoušek, P.: *Síťové aplikace a jejich architektura*. Brno: VUTIUM, 2014, ISBN 978-80-214-3766-1.

[6] Wikipedia: Post Office Protocol. [online], 2017, [cit. 10. 10. 2017]. URL "https://en.wikipedia.org/wiki/Post_Office_Protocol"

[7] Wikipedia: Transport Layer Security. [online], 2017, [cit. 10. 10. 2017]. URL "https://en.wikipedia.org/wiki/Transport_Layer_Security"