

Protocolul Post Office – Versiunea 3**Statutul acestui Memo**

Acest document specifica un protocol Internet standard obisnuit pentru comunitatea Internet si solicita discutii si sugestii pentru imbunatatiri. Vrea sa mentioneze editia curenta “Internet Official Protocol Standards” (STD1) pentru standardizarea acestui protocol. Distributia acestui Memo este nelimitata.

Cuprins

| | | |
|----|-----------------------------------|----|
| 1 | Introducere | 2 |
| 2 | Scurta divagatie | 2 |
| 3 | Operatie de baza | 3 |
| 4 | Starea AUTHORISATION | 4 |
| | Comanda QUIT | 5 |
| 5 | Starea TRANSACTION | 5 |
| | Comanda STAT | 6 |
| | Comanda LIST | 7 |
| | Comanda RETR | 8 |
| | Comanda DELE | 9 |
| | Comanda NOOP | 9 |
| | Comanda RSET | 10 |
| 6 | Starea UPDATE | 10 |
| | Comanda QUIT | 10 |
| 7 | Comenzile optionale POP3 | 11 |
| | Comanda TOP | 11 |
| | Comanda UIDL | 12 |
| | Comanda USER | 14 |
| | Comanda PASS | 15 |
| | Comanda APOP | 15 |
| 8 | Consideratii | 17 |
| 9 | Sumarul comenzilor POP3 | 19 |
| 10 | Exemplu de sesiune POP3 | 20 |
| 11 | Formatul Mesajului | 21 |
| 12 | Referinte | 21 |
| 13 | Securitate | 21 |
| 14 | Marturisiri | 22 |
| 15 | Adresa autorului | 22 |
| | Anexa A. Diferente de la RFC 1725 | 23 |
| | Anexa B. Sumarul comenzilor | 24 |

1. Introducere

Cu siguranta, tipurile nodurilor mai mici in Internet deseori nu sunt practice sa intretina un sistem de transport al mesajului (MTS). De exemplu, o statie de lucru este posibil sa nu dispuna de suficiente resurse (spatiu pe disc) cu scopul de a permite un server SMTP [RFC821] si asociaza un sistem local de trimitere mail pentru a fi tinut rezident si sa ruleze continuu. Similar, poate deveni costisitor (sau imposibil) sau mentii un computer interconectat la un IP-style retea pentru o perioada mai mare de timp (nodul duce lipsa de resursa cunoscuta ca "conectivitate").

In ciuda acestora, deseori este foarte util sa deservesti posta acestor noduri mai mici si deseori sprijina un utilizator agent (UA) sa ajute la manipularea postei electronice. Pentru a rezolva aceasta problema, un nod care intretine o entitate MTS ofera un serviciu maildrop pentru aceste noduri inzestrate mai putin. Post Office Protocol - Versiunea 3 (POP3) a intentionat sa permita unei statii de lucru acces dinamic la maildrop de pe un server gazda intr-un mod util. De obicei, aceasta inseamna ca protocolul POP3 este utilizat pentru a permite unei statii de lucru sa primeasca posta pe care serverul o stocheaza.

POP3 nu a intentionat sa furnizeze operatii extinse de manipulare a postei de pe server; normal posta este descarcata de pe server si apoi stearsa. Un protocol mai avansat (si mai complex), IMAP4, a fost discutat in [RFC1730].

In continuare, termenul "client gazda" (client host) se refera la o gazda ce utilizeaza serviciul POP3, cat timp termenul "server gazda" (server host) se refera la o gazda care ofera serviciul POP3.

2. Scurta Divagatie

Acest memo nu specifica cum un client gazda introduce posta intr-un sistem de transport, desi o metoda consecventa cu filozofia acestui memo este prezentata mai jos:

Cand agentul utilizator al unui client gazda doreste sa introduca posta in sistemul de transport, stabileste o conexiune SMTP cu gazda de retransmitere (relay gazda) si ii trimite toate mail-urile. Aceasta gazda de retransmitere ar putea fi, dar nu e nevoie, server gazda POP3 pentru clientul gazda. Bineinteles, gazda de retransmitere (relay host) trebuie

sa accepte mail-urile trimise arbitrar destinatarilor primitori, aceasta functionalitate nu este obligatorie pentru toate serverele SMTP.

3. Operatia de Baza

Initial, serverul gazda porneste serviciul POP3 ascultand TCP portul 110. Cand clientul gazda doreste sa utilizeze serviciul, este stabilita o conexiune TCP cu serverul gazda. Cand conexiunea s-a realizat, serverul POP3 trimite un salut. Clientul si serverul POP3 schimba comenzi si raspunsuri pana cand conexiunea este inchisa sau abandonata.

Comenzile in POP3 sunt formate din caractere (modul insenzitiv), posibil sa fie urmate de unul sau mai multe argumente. Toate comenzile sunt terminate prin perechea CRLF. Sirul de caractere ce formeaza comanda si argumentele sunt caractere ASCII. Comenzile si argumentele sunt separate printr-un singur caracter SPACE. Comenzile au lungimea de 3 sau 4 caractere. Fiecare argument poate avea lungimea pana la maxim 40 de caractere.

Raspunsurile in POP3 consta dintr-un indicator de status si o comanda, posibil urmata de informatii aditionale. Toate raspunsurile sunt terminate prin perechea CRLF. Raspunsurile pot fi de lungime de pana la 512 caractere, incluzand si CRLF. In mod curent, sunt doi indicatori de status: pozitiv (“+OK”) si negativ (“-ERR”). Serverul **trebuie** sa trimita “+OK” si “-ERR” scrise cu litere mari (upper case).

Raspunsurile la comenzi sunt multi-linie. In aceste cazuri, care sunt clar indicate mai jos, dupa trimiterea primei linii a raspunsului si a perechii CRLF , orice linie aditionala este trimisa si fiecare linie se termina cu perechea CRLF. Cand toate liniile raspunsului au fost trimise, este trimisa o linie finala, care formeaza un octet terminal (cod zecimal 046, “.”) si perechea CRLF. Daca orice linie a raspunsului multi-linie incepe cu acest octet terminal, linia este completata cu octeti terminali. Deci, un raspuns multi-linie se termina cu 5 octeti “CRLF.CRLF”. Cand examineaza un raspuns multi-linie, clientul verifica sa vada daca linia incepe cu octetul terminal. Daca da si ceilalti octeti sunt CRLF, primul octet al liniei (octetul terminal) este scos. Daca da si daca CRLF urmeaza imediat caracterul terminal, atunci raspunsul de la serverul POP este terminat si linia ce contine “.CRLF” nu este considerata parte a raspunsului multi-linie.

O sesiune POP3 evolueaza direct printr-un numar de stari in timpul vietii ei. O data ce conexiunea TCP a fost deschisa si severul POP3 a trimis salutul, sesiunea intra in stare de AUTHORIZATION. In aceasta stare, clientul trebuie sa se identifice serverului POP3. O data ce clientul a facut acest lucru cu succes, serverul isi formeaza resursele asociate in functie de maildrop-ul clientului, si sesiunea intra in starea de TRANSACTION. In aceasta stare, clientul cere actiuni serverului POP3. Cand clientul a emis comanda QUIT, sesiunea intra in starea de UPDATE. In aceasta stare, serverul POP3 elibereaza orice resursa dobandita in timpul starii de TRANSACTION si spune "goodbye". Apoi conexiunea TCP este inchisa.

Un serverul **trebuie** sa raspunda la o nerecunoastere, neimplementare sau o comanda invalida printr-un indicator de stare negativ. Serverul **trebuie** sa raspunda unei comenzi cerute cand sesiunea este intr-o stare incorecta printr-un indicator de stare negativ. Nu exista o metoda generala pentru un client care sa distinga un server ce nu are implementata o comanda optionala, de un server care nu doreste sau nu poate sa proceseze o comanda.

Un server POP3 poate avea timp de inactivitate (autologout). Ca timp trebuie sa fie cel putin 10 minute. Primirea oricarei comenzi de la client in timpul acelu interval este de ajuns sa reseteze "autologout timer". Cand timpul expira sesiunea nu poate intra in starea de UPDATE – serverul ar trebui sa inchida conexiunea TCP fara a sterge nici un mesaj sau fara a trimite vreun raspuns clientului.

4. Starea AUTHORIZATION

O data ce conexiunea TCP a fost deschisa de un client POP3, serverul POP3 emite o linie de salut. Acesta poate fi orice raspuns pozitiv. Un exemplu poate fi:

S: +OK POP3 server ready

Sesiunea POP3 este acum in starea de AUTHORIZATION. Clientul trebuie acum sa se identifice si sa se autentifice serverului POP3. Doua mecanisme posibile pentru aceasta sunt descrise in acest document, combinatia comenzilor USER si PASS si comanda APOP. Ambele mecanisme sunt descrise in acest document. Mecanisme suplimentare de autentificare sunt descrise in [RFC1734]. Cat timp exista mai multe mecanisme de

autentificare acestea sunt cerute de toate serverele POP3, un server POP3 trebuie sa suporte, bineinteles, cel putin unul din aceste mecanisme.

O data ce serverul POP3 a fost determinat complet, utilizarea oricarei comenzi de autentificare a clientului ar trebui sa i se dea acces la maildrop-ul potrivit, serverul POP3 dobandeste acces exclusiv pentru blocarea maildrop-ului, fiind necesara prevenirea modificarii si stergerii mesajelor inainte ca sesiunea sa intre starea UPDATE. Daca blocajul este dobandit cu succes, serverul POP3 raspunde cu un indicator de stare pozitiv. Sesiunea POP3 intra acum in starea TRANSACTION, cu nici un mesaj marcat pentru stergere. Daca maildrop-ul nu a putut fi deschisa din diferite motive (ex. blocajul nu a putut fi realizat, clientul nu are acces la maildrop, sau maildrop-ul nu poate fi citit), serverul POP3 raspunde cu un indicator de stare negativ. (Daca s-a realizat blocajul si serverul POP3 intentioneaza sa raspunda cu un indicator de stare negativ, atunci el trebuie sa se deblocheze inainte de respingerea comenzii). Dupa returnarea negativa a indicatorului de stare, serverul poate inchide conexiunea. Daca serverul nu inchide conexiunea, clientul poate emite fie o noua comanda de autentificare si sa porneasca din nou, fie poate emite comanda QUIT.

Dupa ce serverul POP3 a deschis maildrop-ul, este asociat un numar fiecarui mesaj si se noteaza marimea fiecarui mesaj in octeti. Primului mesaj din maildrop ii este asociat numarul de mesaj "1", celui de-al doilea "2", si asa mai departe, astfel incat celui de al n-lea mesaj ii este asociat numarul de mesaj "n". In POP3 comenzile si raspunsurile, toate numerele de mesaje si marimea mesajelor sunt exprimate in baza 10 (decimal).

Iata un rezumat al comenzii QUIT in starea AUTHORIZATION:

QUIT

Argumente: nici unul

Restrictii: nici una

Raspunsuri posibile:

+OK

Example:

C: QUIT

S: +OK dewey POP3 server signing off

5. Starea TRANSACTION

O data ce clientul s-a identificat cu succes serverului POP3 si serverul POP3 a fost blocat si a deschis maildrop-ul corespunzator, sesiunea POP3 este acum in starea de TRANSACTION. Clientul poate emite in acest moment oricare dintre urmatoarele comenzi POP3, in mod repetat. Eventual, clientul emite comanda QUIT si sesiunea POP3 intra in starea de UPDATE.

Prezentam comenzile POP3 valide in starea TRANSACTION:

STAT

Argumente: nici unul

Restrictii: Poate fi data doar in starea TRANSACTION

Comentariu:

Serverul POP3 emite un raspuns pozitiv intr-o linie care contine informatii pentru maildrop. Aceasta linie este numita "drop listing" pentru acea casuta postala.

Cu scopul de a simplifica analiza, toate serverele POP3 au nevoie sa utilizeze un format sigur pentru "drop listing"-s. Raspunsul pozitiv consta din "+OK" urmat de un singur spatiu, numarul de mesaje din maildrop, un singur spatiu, marimea maildrop-ului in octeti. Acest memo nu determina nici o conditie ce urmeaza dupa marimea maildrop-ului. Implementarile minimale ar trebui doar sa sfarseasca linia de raspuns cu perechea CRLF. Implementari mai avansate pot include si alte informatii.

Nota: Acest memo descurajeaza **puternic** implementarile care furnizeaza informatii suplimentare in "drop listing". Alte facilitati optionale ce permit clientului analiza mesajelor din maildrop sunt discutate mai tarziu.

De observat ca acele mesaje marcate pentru stergere nu sunt numarate in total.

Raspunsuri posibile:

+OK nn mm

Example:

C: STAT

S: +OK 2 320

LIST [msg]***Argumente:***

Un numar de mesaj (optional), care, daca este prezent, nu poate sa se refere la un mesaj marcat pentru stergere.

Restrictii: Pot fi date doar in starea TRANSACTION

Comentariu:

Daca a fost dat un argument serverul POP3 emite un raspuns pozitiv cu o linie ce contine informatii pentru acel mesaj. Aceasta linie este numita “scan listing” pentru mesajul respectiv.

Daca nici un argument nu a fost dat, serverul POP3 emite un raspuns pozitiv, atunci raspunsul dat este multi-linie. Dupa +OK initial, pentru fiecare mesaj din maildrop, serverul POP3 raspunde cu o linie ce contine informatii despre acel mesaj. Aceasta linie mai este numita “scan listing” pentru acel mesaj. Daca nu sunt mesaje in maildrop, atunci serverul POP3 raspunde fara “scan listings” – emite un raspuns pozitiv urmat de o line continant octetul terminal si perechea CRLF.

In scopul simplificarii analizei, toate serverele POP3 sunt conditionate sa utilizeze un format sigur pentru “scan listings”. Un “scan listing” contine numarul de mesaj al mesajului, urmat de un singur spatiu si marimea exacta a mesajului in octeti. Metode pentru calcularea exacta a marimii mesajului sunt descrise in sectiunea Formatul Mesajului. Acest memo nu determina nici o conditie referitoare la ce urmeaza dupa marimea mesajului in “scan listig”. Implimentarile minimale ar

trebui sa termine acea linie de raspuns cu perechea CRLF. Implementarile mai avansate pot include si alte informatii, in urma analizei mesajului.

Nota: Acest memo descurajeaza puternic implementarile ce furnizeaza informatii suplimentare in "scan listing". Alte facilitati optionale ce permit clientului sa analizeze mesajele din maildrop sunt discutate mai tarziu.

De observat ca mesajele marcate pentru stergere nu sunt listate.

Raspunsuri posibile:

+OK scan listing follows

-ERR no such message

Example:

C: LIST

S: +OK 2 messages (320 octets)

S: 1 120

S: 2 200

S: .

...

C: LIST 2

S: +OK 2 200

...

C: LIST 3

S: -ERR no such message, only 2 messages in maildrop

RETR msg

Argumente:

Un numar de mesaj (obligatoriu) ce nu se refera la un mesaj marcat pentru stergere.

Restrictii: Poate fi data doar in faza de TRANSACTION

Comentariu:

Daca serverul POP3 emite un raspuns pozitiv, atunci raspunsul dat este multi-linie. Dupa +OK intial, serverul POP3 trimite mesajul corespunzator numarului de mesaj, fiind atent la completarea caracterului terminal.

Raspunsuri posibile:

+OK urmat de mesaj

-ERR no such mesaj

Example:

C: RETR 1

S: +OK 120 octets

S: <the POP3 server sends the entire message here>

S: .

DELE msg

Argumente:

Un numar de mesaj (obligatoriu) care nu poate sa se refere la un mesaj marcat pentru stergere.

Restrictii: Poate fi data doar in starea de TRANSACTION

Comentariu:

Serverul POP3 markeaza mesajele ca sterse. Orice viitoare referinta la numarul asociat mesajului intr-o comanda POP3 genereaza eroare. Serverul POP3 nu sterge efectiv mesajul pana cand sesiunea POP3 nu intra in starea UPDATE.

Raspunsuri posibile:

+OK message deleted

-ERR no such message

Example:

C: DELE 1

S: +OK message 1 deleted

...

C: DELE 2

S: -ERR message 2 already deleted

NOOP

Argumente: nici unul

Restrictii: Poate fi data doar in starea TRANSACTION

Comentariu:

Serverul POP3 nu face nimic, doar raspunde cu raspunsuri pozitive.

Raspunsuri posibile:

+OK

Exemple:

C: NOOP

S: +OK

RSET

Argumente: nici unul

Restrictii: Poate fi data doar in starea TRANSACTION

Comentariu:

Orice mesaj marcat de serverul POP3 pentru stergere este demarcat. Serverul POP3 apoi raspunde cu un raspuns pozitiv.

Raspunsuri posibile:

+OK

Exemple:

C:RSET

S: +OK maildrop has 2 message (320 octets)

6. Starea UPDATE

Cand clientul emite comanda QUIT din starea TRANSACTION, sesiunea POP3 intra in starea UPDATE. (De observat ca, daca clientul emite comanda QUIT din starea AUTHORIZATION, sesiunea POP3 se termina, dar **nu** intra in starea UPDATE).

Daca o sesiune se termina din anumite motive, altele decat emiterea comenzii QUIT, sesiunea POP3 nu intra in starea UPDATE si nu sterge nici un mesaj din maildrop.

QUIT

Argumente: nici unul

Restrictii: nici una

Comentariu:

Serverul POP3 sterge toate mesajele marcate pentru stergere din maildrop si raspunde cu privire la starea acestei operatii. Daca exista o eroare, ex. resursa lipsa, intampinata in timpul stergerii mesajelor, s-ar putea ca niste mesaje sau nici unul din cele marcate pentru stergere sa nu fie sterse.

Chiar daca operatia s-a realizat cu succes sau nu, serverul elibereaza orice acces exclusiv si inchide conexiunea TCP.

Raspunsuri posibile:

+OK

-ERR some deleted message not removed

Exemple:

C: QUIT

S: +OK dewey POP3 server signing off (maildrop empty)

...

C: QUIT

S: +OK dewey POP3 server signing off (e messages left)

...

7. Comenzi POP3 optionale

Comenzile POP3 discutate mai sus trebuie sa fie suportate de toate implementarile minimale de server POP3.

Comenzile POP3 discutate mai jos permit clientului POP3 o mai mare libertate in lucrul cu mesajele, pastrand o implementare simpla de server POP3.

Nota: Acest memo incurajeaza puternic implementari care sa suporte aceste comenzi in locul celor ce dezvoltat marirea listelor “drop” si “scan”. In cateva cuvinte, filozofia acestui memo este de a pune inteligenta de partea clientului POP3 si nu a serverului POP3.

TOP msg n

Argumente:

Un numar de mesaj (obligatoriu) care nu poate sa se refere la un mesaj marcat pentru stergere si un numar pozitiv de linii (obligatoriu).

Restrictii: Poate fi data doar in faza TRANSACTION

Comentariu:

Daca serverul POP3 emite un raspuns pozitiv, atunci raspunsul dat este multi-linie. Dupa initialul +OK, serverul POP3 trimite headerele mesajului, o linie goala separand headerele de corp si apoi un numar de linii separate indicand corpul mesajului, fiind atent la completarea caracterul terminal.

De observat ca daca numarul de linii cerute de clientul POP3 este mai mare decat numarul de linii ale corpului mesajului, atunci serverul POP3 trimite intregul mesaj.

Raspunsuri posibile:

+OK top of message follows

-ERR no such message

Exemple:

C: TOP 1 10

S: +OK

S:<the POP3 server sends the headers of the message, a blank line, and the first 10 lines of the body of message>

S: .

...

C: TOP 100 3

S: -ERR no such message

UIDL [msg]***Argumente:***

Un numar de mesaj (optional), care, daca e prezent, nu poate sa se refere la un mesaj marcat pentru stergere.

Restrictii: Poate fi data doar in starea TRANSACTION

Comentariu:

Daca un argument a fost dat, serverul emite un raspuns pozitiv cu o linie continand acel mesaj. Aceasta linie este numita “unique-id listing” pentru acel mesaj.

Daca nu a fost dat nici un argument si serverul emite un raspuns pozitiv, atunci raspunsul dat este multi-linie. Dupa +OK initial, pentru fiecare mesaj din maildrop, serverul POP3 raspunde cu o linie ce contine informatii despre acel mesaj.

In scopul simplificarii analizei, toate serverele POP3 sunt obligate sa utilizeze un format sigur pentru “unique-id listing”. O lista cu id-ul unic consta dintr-un numar de mesaj al mesajului, urmat de un singur spatiu si de id-ul unic al mesajului. Nu urmeaza nici o informatie id-ului mesajului din lista de id-uri unice.

Id-ul unic al mesajului este un string determinat arbitrar de server, continand 70 de caractere intre 0x21 – 0x7E, care identifica unic un mesaj in cadrul unui maildrop si care persista in timpul sesiunii. Aceasta persistenta este obligatorie chiar daca o sesiune se termina fara a intra in stare UPDATE. Serverul nu ar trebui sa reutilizeze un id unic intr-un maildrop anume, atat timp cat entitatea ce utilizeaza id-ul unic respectiv exista.

De observat ca mesajele marcate pentru stergere nu sunt listate.

Desi, in general, este preferabil ca implementarile pentru server sa pastreze id-urile unice asignate arbitrar in maildrop, aceasta specificare intentioneaza sa permita ca id-urile unice sa fie calculate [ca a hash of the message](#). Clientii ar trebui sa poata trata situatia in care doua copii identice ale unui mesaj din maildrop au acelasi id unic.

Raspunsuri posibile:

+OK urmat de lista de id-uri unice

-ERR no such message

Exemple:

C: UIDL

S: +OK

S: 1 whqtswo00WBw418f9t5JxYwZ

S: 2 QhdPYR:00WBwPh7x7

S: .

...

C: UIDL 2

S: +OK 2 OhdPYR:00WBw1Ph7x7

...

C: UIDL 3

S: -ERR no such message, only 2 messages in maildrop

USER nume

Argumente:

Un sir de caractere identificand o casuta postala (obligatoriu), care este semnificativ doar serverului.

Restrictii:

Poate fi data doar in starea de AUTHORIZATION dupa mesajului de salut al serverului POP3 sau dupa una din comenzile USER sau PASS terminate cu eroare.

Comentariu:

Pentru autentificare utilizand comenzile USER si PASS, clientul trebuie sa emita mai intai comanda USER. Daca serverul POP3 raspunde cu un indicator pozitiv (“+OK”), atunci clientul poate emite fie comanda PASS sa completeze autentificarea, fie comanda QUIT sa termine sesiunea POP3. Daca serverul POP3 raspunde cu un indicator negativ de stare (“-ERR”)

pentru comanda USER, atunci clientul poate emite fie o comanda noua de autentificare, fie comanda QUIT.

Serverul poate returna un raspuns pozitiv chiar daca nu exista nici o casuta postala. Serverul poate returna un raspuns negativ daca casuta postala exista, dar nu permite autentificare de parola tip plaintext.

Raspunsuri posibile:

+OK nume is a valid mailbox

-ERR never heard of mailbox nume

Example:

C: USER frated

S: -ERR sorry, no mailbox for frated here

...

C: USER mrose

S: +OK mrose is a real hoopy frood

PASS sir caractere

Argumente:

O parola de server/casuta postala (obligatoriu).

Restrictii:

Poate fi data doar in starea de AUTHORIZATION imediat dupa o comanda USER incheiata cu succes.

Comentariu:

Cand un client emite comanda PASS, serverul POP3 utilizeaza perechea de argumente de la USER si comenzile PASS sa determine daca clientului ar trebui sa i se permita accesul la maildrop-ul respectiv.

Deoarece comanda PASS are exact un argument, serverul POP3 poate trata spatiile in argument ca parte a parolei, in loc de separatoare de argument.

Raspunsuri posibile:

+OK maildrop locked and ready
-ERR invalid password
-ERR unable to lock maildrop

Exemple:

C: USER mrose
S: +OK mrose is a real hoopy frood
C: PASS secret
S: -ERR maildrop already locked
...
C: USER mrose
S: +OK mrose is a real hoopy frood
C: PASS secret
S: +OK mrose's maildrop has 2 messages (320 octets)

APOP nume rezumat***Argumente:***

Un sir de caractere identificand casuta postala si un rezumat MD5 (amandoua obligatorii).

Restrictii:

Poate fi data doar in starea de AUTHORIZATION dupa salutul serverului POP3 sau dupa una din comenzile USER sau PASS terminate cu insucces.

Comentariu:

In mod normal, fiecare sesiune POP3 incepe cu USER/PASS. Aceasta sfarseste serverul / id-ul user-ului specific, parola fiind trimisa in retea. Multe implementari de client POP3 se conecteaza la un server POP3 in mod obisnuit – pentru a verifica mail-ul nou. In plus intervalul sesiunii initiale poate fi de 5 minute. Deci, riscul capturarii parolei este mare.

Este necesara o metoda alternativa de autentificare, care sa furnizeze cele doua metode originale de autentificare si protejare a raspunsului, dar

care sa nu implice trimiterea parolei neprotejate in retea. Comanda APOP furnizeaza aceasta functionalitate.

Un server POP3 care implementeaza comanda APOP va include o marca de timp in banner-ul mesajului de salut. Sintaxa acestei marcare a timpului corespunde lui "msg-id" din [RFC822] si **trebuie** sa fie diferita de fiecare data cand serverul POP3 emite un banner de salut. De exemplu, intr-o implementare UNIX in care sunt utilizate procese UNIX separate pentru fiecare instanta a serverului POP3, sintaxa unei marci de timp poate fi:

[<process-ID.clock@hostname>](#)

unde "process-ID" este o valoare zecimala a PID-ului procesului, "clock" este o valoare zecimala a timpului sistemului si "hostname" este numele complet al domeniului corespunzator gazdei unde ruleaza serverul POP3.

Clientul POP3 ia la cunostinta de aceasta marca de timp si apoi emite comanda APOP. Parametrul "nume" are aceasi semantica ca parametrul "nume" din comanda USER. Parametrul "rezumat" este calculat prin aplicare algoritmului MD5 [RFC1321] unui sir de caractere compus din marca de timp (incluzand parantezele – unghiulare) urmat de informatia secreta. Informatia secreta (shared secret) este un sir de caractere cunoscut numai de clientul si serverul POP3. Mare atentie ar trebui acordata pentru a impiedica o dezvaluire neautorizata a secretului, cunoasterea secretului va permite oricarei entitati sa se ascunda sub acel nume de user. Parametrul "rezumat" este o valoare pe 16 octeti care este trimisa in format hexazecimal, utilizand caracterele ASCII lower-case.

Cand serverul POP3 primeste comanda APOP verifica rezumatul furnizat. Daca rezumatul este corect serverul POP3 emite un raspuns pozitiv si sesiunea POP3 intra in starea TRANSACTION. Altfel, un raspuns negativ este emis si sesiunea POP3 ramane in starea AUTHORIZATION.

De observat ca, lungimea informatii secrete creste, deci dificultatea. Ca atare, informatiile secrete ar trebui sa fie de lungime mare (mult mai mult de 8 caractere ca in ex. de mai jos).

Raspunsuri posibile:

+OK maildrop locked and ready
-ERR permission denied

Exemplu:

S: +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>

C: APOP mrose c4c9334bac560ecc979e58001b3e22fb

S: +OK maildrop has 1 message (369 octetes)

In acest exemplu, informatia secreta este sirul “tan-staaf”. Deci, algoritmul MD5 este aplicat sirului:

<1896.697170952@dbc.mtview.ca.us>tanstaaf

care produce o valoare rezumat a:

c4c9334bac560ecc979e58001b3e22fb

8. Consideratii

De cand caracteristicile principale descrise mai sunt au fost adaugate la protocolul POP3, s-a acumulat experienta in utilizarea lor pe scara larga in operatii de “post office” unde cei mai multi utilizatori nu se cunosc unii cu ceilalti. In aceste situatii si altele, utilizatorii si vanzatorii de clienti POP3 au descoperit ca o combinatia intre comanda UIDL si neemiterea comenzii DELE pot furniza o versiune slaba de “depozit maildrop semi-permanent” avand o functionalitate normala asociata cu IMAP. Desigur alte calitati IMAP, asa cum verificand o conexiune existenta pentru mesajele noi sosite si suportand foldere multiple pe server, nu sunt prezente in POP3.

Cand aceste facilitati sunt utilizate ocazional de catre utilizatori, exista o tendinta de recitirea mesajelor acumulate pe server fara limita. Acesta este clar un tip de comportament nedorit din punctul de vedere al operatorului de server. Aceasta situatie este agravata de faptul ca posibilitatile limitate ale POP3-ului nu permit manipularea eficienta a maildrop-urilor care au mii de mesaje.

In consecinta, este recomandat ca operatorii de servere multi-users la scara larga, in special cei care au acces la maildrop doar via POP3, sa considere urmatoarele alternative:

- Impunand alocarea de spatiu de depozitare a maildrop-ului

Un dezavantaj al acestei optiuni este ca acumularea de mesaje poate provoca neputinta utilizatorului de a primi noi mesaje in maildrop. In situatiile in care se alege aceasta optiune ar trebui sa se asigure informarea utilizatorilor asupra acestui impediment sau epuizarea spatiului, poate prin inserarea unui mesaj potrivit in maildrop-ul userului.

- Impunand o polita de asigurare privind pastrarea pe server.

Utilizatorii sunt liberi sa stabileasca aceasta polita de asigurare privind depozitarea si pastrarea mesajelor pe server, cele citite si cele necitite. De exemplu, un utilizator poate sterge mesajele necitite de pe server dupa 60 de zile si pe cele citite dupa 7 zile. Stergerile de mesaj sunt in afara protocolului POP3 si nu sunt considerate o violare de protocol.

Operatorii de server impunand politile de asigurare cu privire la stergerea mesajelor ar trebui sa aiba grija sa faca toti utilizatorii constienti de puterea acestora.

Clientii nu trebuie sa presupuna ca o polita va sterge automat mesajele, si ar trebui sa continue sa stearga explicit mesajele utilizand comanda DELE cand este cazul.

De notat ca impunerea acestor polite de asigurare de stergere poate fi confuza pentru utilizatorii simpli, deoarece clientul lor POP3 poate contine optiuni de configurare de a sterge mail-ul de pe server, care nu va fi de fapt suportat de server.

Un caz special al politelor este ca mesajele pot fi doar downloadate odata de pe server si sunt sterse dupa ce acesta a terminat operatia. Aceasta ar putea fi implementata de un server POP3 prin urmatorul mecanism: "urmarind un login de client POP3 care a terminat prin QUIT, sterge toate mesajele downloadate in timpul sesiunii cu comanda RETR". Este important sa nu se stearga mesajele daca conexiunea s-a incheiat printr-un eveniment anormal (ex. daca QUIT nu a fost primit de la client) deoarece clientul poate nu a primit sau nu a salvat cu succes mesajele). Serverele ce implementeaza politele downloadeaza-si-sterge pot deasemenea sa doreasca sa dezactiveze sau sa limiteze comanda optionala

TOP, desi ar putea fi utilizata ca un mecanism alternativ pentru a downloada toate mesajele.

9. Sumarul comenzilor POP3:

Comenzi minimale POP3:

1. valide in starea de AUTHORIZATION:

USER nume
PASS sir_caractere
QUIT

2. valide in starea de TRANSACTION

STAT
LIST [msg]
RETR msg
DELE msg
NOOP
RSET
QUIT

Comenzi optionale POP3:

10. valide in starea de AUTHORIZATION

APOP nume rezumat

11. valide in starea de TRANSACTION

TOP msg n
UIDL [msg]

Raspunsuri posibile:

+OK
-ERR

De observat ca, cu exceptia comenzilor STAT, LIST si UIDL raspunsul dat de serverul POP3 la orice comanda este "+OK" sau "-ERR". Si orice text aparut dupa acest raspuns poate fi ignorat de client.

12. Exemplu de sesiune POP3

S: <wait for connection on TCP port 110>
C: <open connection>
S: +OK POP2 server ready <1896.697170952@dbc.mtview.ca.us>
C: APOP mrose c4c9334bac560ecc97e58001b3e22fb
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: RETR 2
S: +OK 200 octets
S: <the POP3 server sends message 2>
S: .
C: DELE 2
S: +OK message 2 deleted
C: QUIT
S: +OK dewey POP3 server signing off (maildrop empty)
C: <close connection>
S: <wait for next connection>

13. Formatul Mesajului

Toate mesajele transmise in timpul sesiunii POP3 sunt sumate conform standardului pentru formatul textelor mesajelor pentru Internet [RFC822].

Este important de observat ca numararea octetului pentru un mesaj de pe un server gazda poate diferi de numararea octetului asignat mesajului datorita conventiilor locale pentru desemnarea sfarsitului de linie (end-of-line). De obicei, in timpul starii de AUTHORIZATION a unei sesiuni POP3, serverul POP3 poate calcula marimea fiecarui mesaj in octeti cand deschide maildrop-ul. De exemplu, daca serverul gazda POP3 numara fiecare aparitie a acestui caracter ca doi octeti. Acele linii din mesaj care incep cu octetul terminal nu au nevoie (si nu trebuie) numarate de doua ori, deoarece clientul POP3 va sterge toate caracterele de terminale cand primeste un raspuns multi-linie.

14. Referinte

- [RFC821] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, USC/Information Sciences Institute, August 1982
- [RFC822] Crocker, D., "Standard for the Format of ARPA-Internet Text Messages", STD 11, RFC822, University of Delaware, August 1982
- [RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, MIT Laboratory for Computer Science, April 1992
- [RFC1730] Crispin, M., "Internet Message Access Protocol –Version 4", RFC 1730, University of Whashington, December 1994
- [RFC1734] Myers, J., "POP3 AUTHENTICATION command", RFC 1734, Carnegie Mellon, December 1994

15. Securitate

Se intuieste ca utilizarea comenzii APOP furnizeaza identificarea si protejarea raspunsului pentru o sesiune POP3.

Deci un server POP3 care implementeaza ambele comenzi, PASS si APOP, ar trebui sa nu permita ambele metode de acces pentru un utilizator dat; adica, pentru un nume de casuta postala dat este permisa fie secventa de comenzi USER/PASS sau comanda APOP, dar nu ambele.

Mai mult, se observa ca o crestere a lungimii informatiei secrete, face dificila deducerea ei.

Serverele care raspund “-ERR” la comanda USER dau potentialilor atacatori indicatii despre validitatea numelor (care nume sunt valide).

Utilizarea comenzii PASS are ca efect trimiterea de parole direct in retea.

Utilizarea comenzilor RETR si TOP au ca efect trimiterea de mail direct in retea.

Alte cazuri de securitate nu sunt discutate in acest memo.

16. Marturisiri

Familia POP are o istorie lunga. Desi o revizie minora a RFC-ului 1460, POP3 este bazat pe ideile prezentate in RFC-urile 918, 937 si 1081.

In plus, Alfred Grimstad, Keith McCloghrie si Nei Ostroff au furnizat comentarii semnificative referitoare la comanda APOP.

17. Autori si Adrese

John G. Myers

Carnegie-Mellon Univesity

5000 Forbes Ave

Pittsburgh, PA 15213

Email: jgm+@cmu.edu

Marshall T. Rose

Dover Beach Consulting, Inc.

420 Whisman Court

Mountain View, CA 94043-2186

Email: mrose@dbc.mtview.ca.us

Anexa A: Diferente fata de RFC 1725

Acest memo este o revizie a RFC-ului 1725 (a Draft Standard).

Face urmatoarele modificari:

- clarifica faptul ca, comenzile sunt scrise case-insensitive;
- specifica ca serverele trebuie sa trimita "+OK" si "-ERR" scrise cu litere mari;
- specifica ca salutul initial este un raspuns pozitiv, in loc de orice sir de caractere care ar putea fi un raspuns pozitiv;
- specifica comportamentul pentru comenzile neimplementate;
- face comenzile USER si PASS optionale;
- clarifica set de posibile raspunsuri la comanda USER;
- schimba ordinea exemplurilor din comenzile USER si PASS, pentru a reduce confuzia;
- clarifica faptul ca, comanda PASS poate fi data doar imediat dupa ce comanda USER s-a incheiat cu succes;
- clarifica persistenta cerintelor UID si adauga cateva observatii;
- specifica limitare lungimii UID de la unul la 70 de octeti;
- specifica un indicator de stare de lungime limitata la 512 octeti, incluzand CRLF;
- clarifica ca LIST fara argumente pentru o casuta postala goala returneaza succes;
- adauga o referinta de la comanda LIST la sectiunea Formatul Mesajului;
- clarifica comportamentul comenzii QUIT in caz de esec;
- adauga referinte catre RFC-urile 1730 si 1734;
- clarifica metoda prin care UA poate introduce un mail in sistemul de transport;
- clarifica ca al doilea argument al comenzii TOP este numarul de linii;
- schimba ideea in sectiunea **Securitate** conform careia un server sa nu accepte ambele comenzi PASS si APOP pentru un utilizator, de la "trebuie" la "ar trebui".

Anexa B: Indexul Comenzilor

| | | |
|------|-------|----|
| APOP | | 15 |
| DELE | | 9 |
| LIST | | 7 |
| NOOP | | 9 |
| PASS | | 15 |
| QUIT | | 5 |
| QUIT | | 10 |
| RETR | | 8 |
| RSET | | 10 |
| STAT | | 6 |
| TOP | | 11 |
| UIDL | | 12 |
| USER | | 14 |