CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost IMAP protokola

NCERT-PUBDOC-2010-05-300

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

IMAP je protokol za dohvat elektroničke pošte s udaljenog poslužitelja na lokalno računalo. Uz POP3, najčešće je korišten protokol za ovu vrstu usluge na Internetu. Podržavaju ga brojni besplatni i komercijalni poslužitelji i klijenti. Osim samog dohvata pošte, IMAP podržava napredne mogućnosti kao što su:

- dodavanje i brisanje poruka s poslužitelja,
- dohvat dijelova poruka preko MIME struktura,
- pretraživanje pretinaca na poslužitelju i slično.

Sigurnost ovog protokola vezana je prvenstveno uz mehanizme autentikacije i enkripcije. Prvi osigurava pristup pretincima elektroničke pošte samo ovlaštenim korisnicima, dok drugi osigurava zaštitu podataka koji se šalju preko mreže. IMAP u svojoj specifikaciji nudi veći broj sigurnosnih mehanizama. Često se koristi u kombinaciji sa SSL protokolom, koji brine o sigurnosti na nižoj razini. SSL veza otklanja potrebu za sigurnosnim mehanizmima na razini IMAP aplikacije.

U dokumentu su opisani principi rada i funkcionalnosti IMAP protokola. Dani su primjeri jednostavnih primjena i načina rada, predstavljeni su sigurnosni mehanizmi i njihova problematika te je dana usporedba sa POP3 protokolom.

2. IMAP

IMAP (eng. *Internet Message Access Protocol*) je protokol aplikacijskog sloja OSI modela koji služi za dohvat elektroničke pošte s udaljenog poslužitelja. Riječ je o otvorenom protokolu kojeg podržava većina klijenata elektroničke pošte (Mozilla Thunderbird, Outlook, Eudora…). Za razliku od srodnog protokola POP, IMAP nudi veći raspon mogućnosti za rad s elektroničkom poštom. U odnosu na POP, IMAP protokol podržava manji broj ISP (eng. Internet Service Provider) organizacija. Jedna od glavnih značajki IMAP-a je mogućnost istovremenog pristupanja istom poštanskom pretincu za veći broj klijenata, tj. sa više lokacija.

2.1. Povijest i razvoj

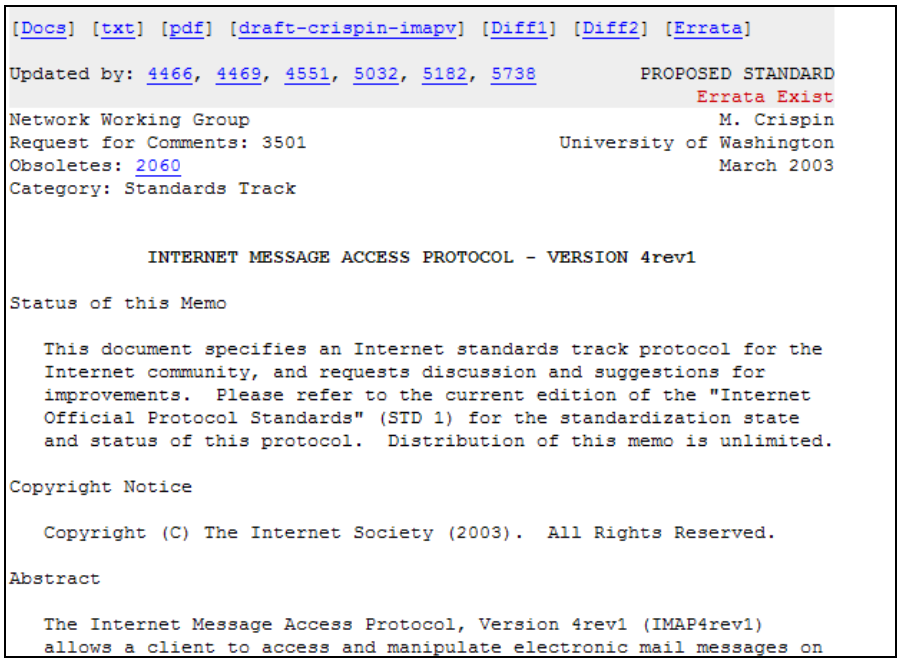
Prva inačica IMAP-a je razvijena 1986. godine, a izvorni naziv protokola bio je *Interim Mail Access Protocol*. Druga inačica protokola nazvana je IMAP2. Uvela je novi naziv *Interactive Mail Access Protocol* i oznake za zahtjeve klijenata i odgovore poslužitelja. Također, ova inačica dokumentirana je u RFC dokumentima RFC 1064 i RFC 1176 te javno distribuirana.

IMAP2bis specifikacija uvodi niz novih mogućnosti u IMAP protokol koje uključuju rad s MIME strukturama i napredno rukovanje poštanskim pretincem. Neke od tih mogućnosti su:

- brisanje poruka,
- stvaranje poruka,
- izmjena poruka i
- postavljanje poruka na poslužitelj.

Specifikacija ove inačice nikada nije dobila status standarda jer je preimenovana u IMAP4 kad je njezin razvoj preuzela IETF radna grupa. Početkom 1990-ih izašao je dokument RFC 1730 u kojem je predložena specifikacija IMAP4 protokola. Tada je i naziv protokola dobio današnji oblik: *Internet Message Access Protocol*. Godine 1996. izašla je revizija - IMAP4rev1 u dokumentu RFC 3501, koja je do danas ostala IMAP standard. Protokol se može koristiti sa starijim protokolima IMAP2 i IMAP2bis, no ne može se koristiti s izvornim protokolom IMAP upravo zbog spomenutih oznaka za zahtjeve i odgovore koje izvorna inačica nema. Bez obzira na usklađenost, starije inačice se praktički uopće ne koriste.

Posljednja specifikacija protokola (IMAP4rev) uvela je obavezu sigurne autentifikacije. Prethodno je bilo moguće slati lozinke kao čisti tekst preko mreže. Također, omogućena je i zaštita poruka koje se šalju u okviru IMAP protokola enkripcijom.



[Docs] [txt] [pdf] [draft-crispin-imapv] [Diff1] [Diff2] [Errata]

Updated by: 4466, 4469, 4551, 5032, 5182, 5738 PROPOSED STANDARD
Errata Exist

Network Working Group M. Crispin
Request for Comments: 3501 University of Washington
Obsoletes: 2060 March 2003
Category: Standards Track

INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

The Internet Message Access Protocol, Version 4rev1 (IMAP4rev1) allows a client to access and manipulate electronic mail messages on

Slika 1. Isječak IMAP4rev specifikacije
Izvor: IETF

Praćenjem i dokumentiranjem IMAP protokola bavi se radna skupina organizacije IETF (eng. *The Internet Engineering Task Force*). Riječ je o organizaciji čiji je cilj rast i održavanje kvalitete Interneta oblikovanjem i objavljivanjem dokumenata kao i specifikacija internetskih usluga. Praćenje i poštivanje IETF standarda omogućuje komunikaciju između programa i usluga razvijenih u različitim tvrtkama. Tako primjerice podrška za IETF specifikaciju IMAP protokola omogućuje preuzimanje pošte s Microsoft Exchange Server poslužitelja jednako programu Microsoft Outlook (koji koristi specifičan protokol) kao i programu Mozilla Thunderbird preko IMAP protokola.

Inačica protokola	Osobitosti
IMAP	Izvorna specifikacija protokola, neusklađen za korištenje s drugim inačicama
IMAP2	Uvedene oznake zahtjeva i odgovora – prva distribuirana inačica
IMAP2bis	Dodana potpora za MIME, omogućen rad s pretincima (dodavanje pretinaca i poruka, brisanje, preimenovanje pretinaca)
IMAP4	Nema novih funkcionalnosti, popravljen dizajn IMAP2bis
IMAP4rev1	Obavezno korištenje sigurnih autentikacijskih mehanizama, moguća IMAP komunikacija preko TLS kanala (STARTTLS)

Tablica 1. IMAP specifikacije

2.2. Osobitosti i primjena protokola

IMAP protokol koristi se za dohvat elektroničke pošte na lokalno računalo s udaljenog poslužitelja. Pritom korisnik može mijenjati sadržaj pretinca brisanjem, stvaranjem i dodavanjem poruka. Više klijenata istovremeno može pristupati istom pretincu koji se kroz poruke oznake statusa sinkroniziraju (npr. kad jedan klijent doda poruku u pretinac, ona postaje vidljiva i drugim klijentima). IMAP funkcionira kroz naredbe koje klijent šalje poslužitelju, nakon čega ih on obrađuje i šalje odgovor nazad klijentu.

Slika 2. Shema IMAP komunikacije
Izvor: IETF RFC 3501

Na gornjoj slici prikazana je shema IMAP komunikacije prema RFC specifikaciji. Koraci na slici slijede nakon uspostavljanja veze (eng. *connection established*):

1. povezivanje bez autentikacije,
2. povezivanje s autentikacijom,
3. odbijen zahtjev za povezivanjem,
4. uspješna prijava,
5. uspješan pristup pretincu,
6. izlaz iz pretinca ili neuspjeli pristup pretincu i
7. odjava ili zatvaranje veze.

2.2.1. Funkcionalnosti

Osim funkcionalnosti već navedenih u uvodu, IMAP omogućuje i:

- rad s MIME formatom poruka i dohvat pojedinih MIME dijelova s poslužitelja (npr. korisnik dohvaća tekstualni dio poruke, ali ne dohvaća privitak),
- tzv. *online* i *offline* način rada,
- dohvat statusa poruke (pročitana, nepročitana i sl.) i stvaranje vlastitih oznaka poruke,
- korištenje više poštanskih pretinaca i slanje poruka između njih te korištenje javnih ili dijeljenih mapa,
- dodavanje funkcionalnosti u specifikaciju protokola posebnim mehanizmima koji ne zahtijevaju izmjenu osnovnog protokola,
- pretraživanje pretinca prema različitim kriterijima (pritom se pretraživanje izvodi na poslužitelju prema nekom algoritmu) i
- označavanje poruka jedinstvenim rastućim identifikatorima koje olakšava pretraživanje pretinca i rukovanje porukama.

Zadnja mogućnost predstavlja i potencijalni problem jer se, u slučaju loše riješenog pitanja pretraživanja, na poslužitelju može trošiti puno resursa.

2.2.2. Naredbe

IMAP API (eng. *Application Interface*) uključuje 30 - 50 naredbi koje se koriste za komunikaciju između klijenta i poslužitelja. Format naredbi je fiksan, a svaka naredba prima posebno definirane argumente. Neke od naredbi može slati klijent koji nije prošao provjeru identiteta, a za neke je autentifikacija preduvjet (npr. naredbe za rad s porukama u pretincu).

Primjerice naredba LOGIN omogućuje autentikaciju korisnika pomoću korisničkog imena i lozinke koji se šalju kroz mrežu u tekstualnom obliku. Zbog rizika koji predstavlja za sigurnost, njezina se uporaba ne preporuča. LOGIN kao ulazne parametre prima:

- korisničko ime i
- lozinku korisnika.

Poslužitelj kao odgovor vraća:

- OK za uspješnu prijavu,
- NO za neuspješnu prijavu ili
- BAD za loše oblikovanu naredbu (npr. krive argumente).

Primjer korištenja je sljedeći:

```
KLIJENT: a001 LOGIN MMILIC TAJNA!LOZINKA
POSLUŽITELJ: a001 OK LOGIN completed
```

Za razliku od naredbe LOGIN, AUTHENTICATE podrazumijeva sigurne autentikacijske mehanizme. O njima će biti riječi u poglavlju 3.1.

Naredba SELECT izvodi se nakon provjere identiteta korisnika, a njome korisnik odabire pretinac kojem će pristupiti. Naredba kao ulazni argument prima ime pretinca.

Odgovori poslužitelja isti su kao za LOGIN:

- OK - za uspješan pristup pretincu,
- NO - za nepostojeći ili nedostupan pretinac i
- BAD - za loše oblikovanu naredbu

U odgovoru poslužitelj vraća:

- oznake poruka (FLAGS),
- broj poruka u pretincu (EXISTS) i
- broj novih poruka (RECENT).

Odgovor može, ali ne mora uključivati i sljedeće informacije:

- broj prve neviđene poruke (UNSEEN),
- oznake poruka koje korisnik može trajno mijenjati (PERMANENTFLAGS) i
- identifikatore UIDNEXT i UIDVALIDITY.

Identifikatori se porukama dodjeljuju u rastućem nizu, a prema iznosu UIDNEXT klijent može pretpostaviti da će sve poruke koje će ubuduće stizati u pretinac imati identifikator veći od iznosa UIDNEXT ili jednak njemu. UIDVALIDITY je jedinstvena oznaka pretinca, koja se također stvara kao rastući niz. Ove dvije vrijednosti skupa omogućuju jedinstveno identificiranje svake pristigle poruke.

Primjer korištenja naredbe SELECT dan je u sljedećem kodu:

```
KLIJENT: A142 SELECT INBOX
POSLUŽITELJ: * 172 EXISTS
POSLUŽITELJ: * 1 RECENT
POSLUŽITELJ: * OK [UNSEEN 12] Message 12 is first unseen
POSLUŽITELJ: * OK [UIDVALIDITY 3857529045] UIDs valid
```

```
POSLUŽITELJ: * OK [UIDNEXT 4392] Predicted next UID
POSLUŽITELJ: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
POSLUŽITELJ: * OK [PERMANENTFLAGS (\Deleted \Seen \*)] Limited
POSLUŽITELJ: A142 OK [READ-WRITE] SELECT completed
```

Naredba koju može izvesti bilo koji klijent, neovisno o tome je li provjeren njegov identitet ili nije, je CAPABILITY. Ovom naredbom se dohvaćaju mogućnosti podržane na korištenom IMAP poslužitelju.

```
KLIJENT: abcd CAPABILITY
POSLUŽITELJ: * CAPABILITY IMAP4rev1 STARTTLS AUTH=GSSAPI
LOGINDISABLED
KLIJENT: abcd OK CAPABILITY completed
```

Naredbe STARTTLS i LOGINDISABLED mora podržavati svaki poslužitelj. STARTTLS omogućuje kriptiranje komunikacije TLS protokolom, a LOGINDISABLED onemogućuje korištenje nesigurne naredbe LOGIN. AUTH=GSSAPI je naziv mehanizma sigurne autentikacije pomoću GSSAPI protokola.

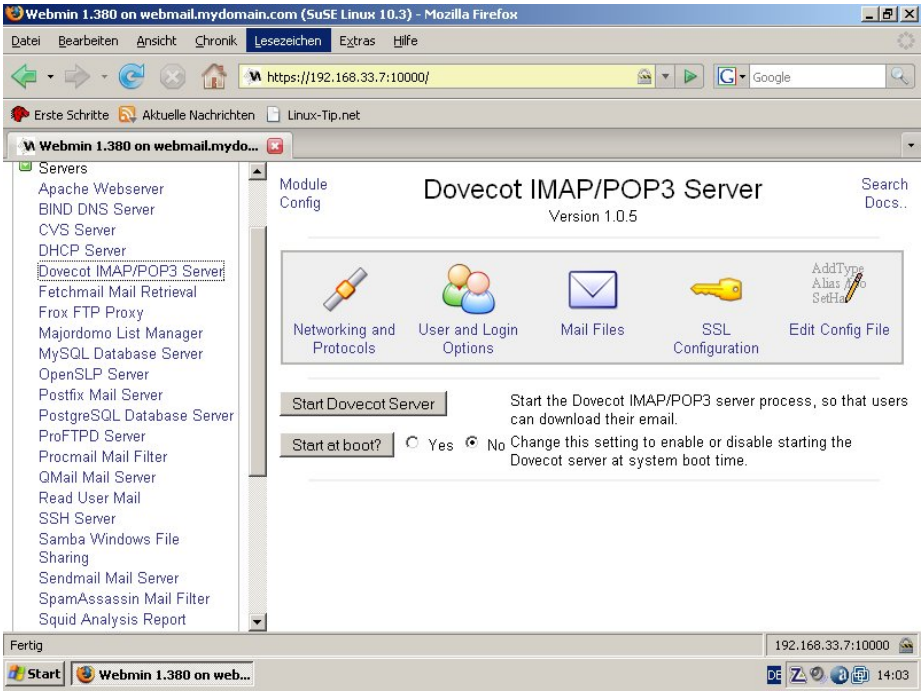
Naredba	Opis naredbe
Naredbe koje klijenti mogu slati prije provjere identiteta	
STARTTLS	Uspostavljanje TLS veze
AUTHENTICATE	Autentikacija sigurnim mehanizmima
LOGIN	Jednostavna autentikacija imenom i lozinkom
Naredbe koje klijenti mogu slati nakon provjere identiteta	
SELECT	Odabir pretinca elektroničke pošte
EXAMINE	Pregledavanje sadržaja pretinca
DELETE	Brisanje pretinca
RENAME	Preimenovanje pretinca
CREATE	Stvaranje pretinca
SUBSCRIBE	Aktiviranje pretinca
UNSUBSCRIBE	Deaktiviranje pretinca
LIST	Dohvaća određeni podskup iz liste dostupnih pretinaca
LSUB	Dohvaća podskup liste aktivnih pretinaca
STATUS	Dohvaća stanje pretinca
APPEND	Dodaje poruku u pretinac
CHECK	Prazna naredba
CLOSE	Briše sve poruke označene kao obrisane i izlazi iz pretinca
EXPUNGE	Briše sve poruke označene kao obrisane i šalje odgovor za svaku poruku
SEARCH	Pretražuje pretinac prema zadanom kriteriju
FETCH	Dohvaća poruke iz pretinca
STORE	Mijenja podatke o poruci
COPY	Kopira poruku i sprema je u odabrani pretinca
UID	Pretražuje, kopira ili dohvaća poruke prema jedinstvenoj oznaci
Naredbe koje ne ovise o provjeri identiteta klijenta	
CAPABILITY	Dohvaća mogućnosti pretinca
NOOP	Prazna naredba – ne čini ništa
LOGOUT	Odjava klijenta

Tablica 2. Popis IMAP naredbi

2.2.3. Poslužitelji

IMAP poslužitelji rade tako da od MTA (eng. *Message Transfer Agent*) programa primaju poštu. Pritom se poruke mogu odlagati u dijeljeni prostor u formatu razumljivom IMAP poslužitelju. Drugo moguće rješenje je da IMAP poslužitelj osluškuje zahtjeve za povezivanje MTA agenta preko SMTP ili LMTP protokola za slanje elektroničke pošte. Osim samih poruka, poslužitelji koriste opisne podatke o porukama (eng. *metadata*) kao i autentikacijske, konfiguracijske, dnevničke i privremene datoteke. Osim osnovne sistemske podrške (jezgra, biblioteke, programi operacijskog sustava), IMAP poslužitelji koriste SSL podršku za zaštitu komunikacije enkripcijom. Mogu koristiti i baze podataka za čuvanje opisnih i autentifikacijskih podataka (npr. BerkeleyDB). Neki od besplatnih IMAP poslužitelja su:

- Cyrus,
- Dovecot,
- Courier-IMAP.



Slika 3. Sučelje Dovecot IMAP poslužitelja
Izvor: LINUX TIP

2.2.4. Klijenti

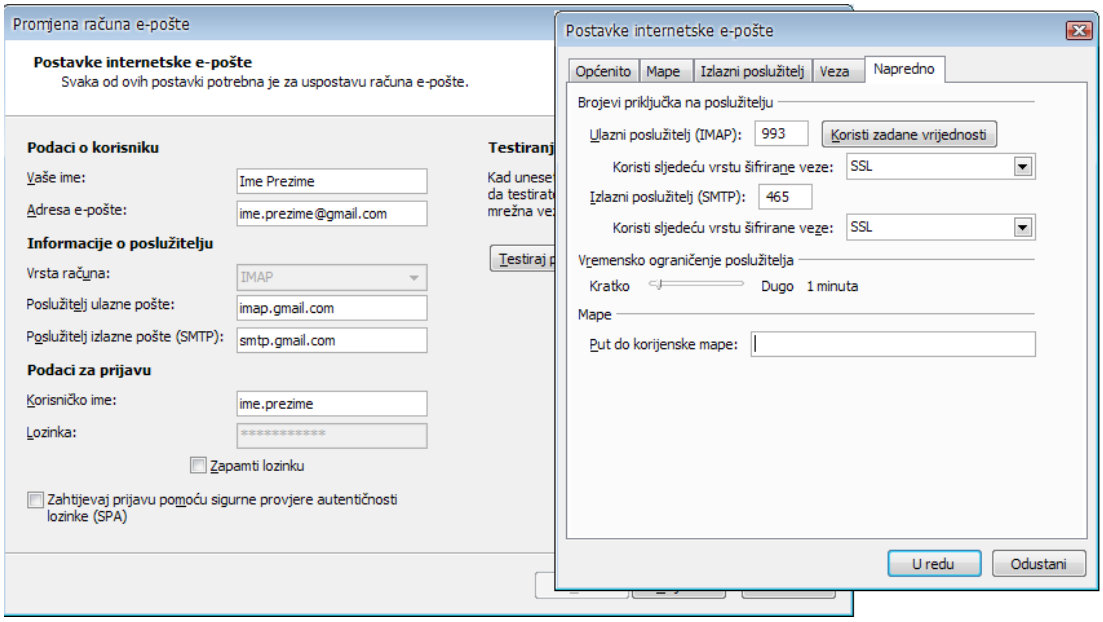
IMAP klijenti omogućuju slanje zahtjeva IMAP poslužiteljima i dohvat podataka. Većina klijenata elektroničke pošte podržava IMAP protokol, a mogu komunicirati sa svim poslužiteljima koji podržavaju taj protokol. Neki od poznatijih programa koji podržavaju IMAP protokol su:

- Microsoft Outlook,
- Mozilla Thunderbird i
- Apple Mail.

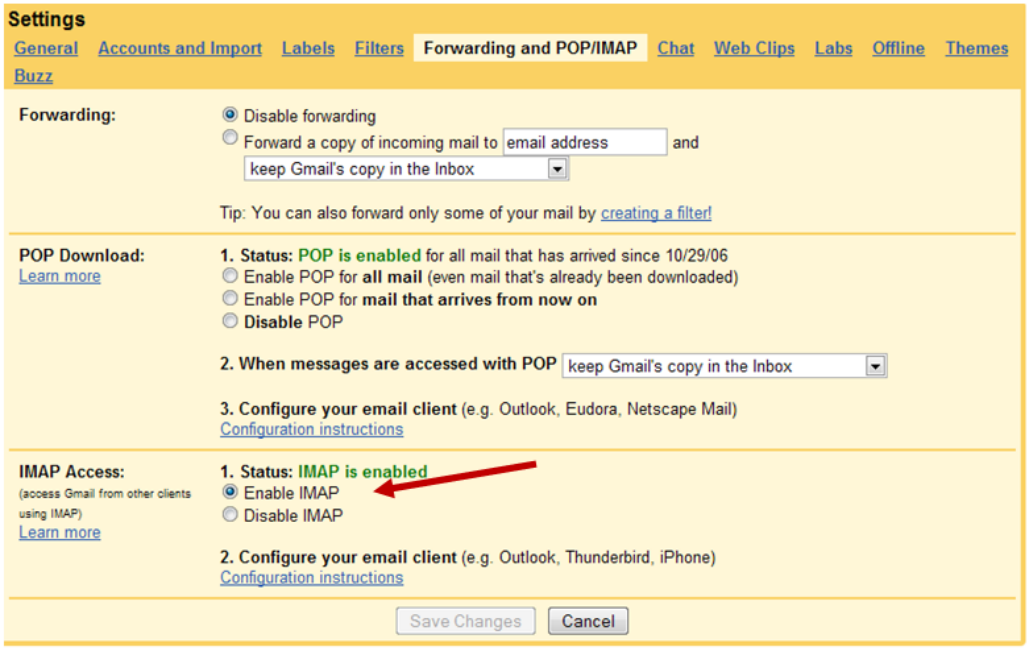
Klijenti šalju zahtjeve na priključak (eng. *port*) na kojem poslužitelj osluškuje zahtjeve:

- 143 - IMAP,
- 585 - IMAP4-SSL (s ugrađenom SSL enkripcijom) ili
- 993 - IMAP preko SSL kanala.

Na sljedećim slikama dan je primjer uspostavljanja IMAP veze između poslužitelja GMail i Outlook klijenta. Na GMailu je potrebno omogućiti IMAP protokol, a na klijentu definirati postavke poslužitelja i korisničkog računa.



Slika 4. Postave Outlooka za IMAP



Slika 5. Postavke GMaila za IMAP

3. Sigurnost IMAP protokola

Sigurnost IMAP protokola prvenstveno se odnosi na autentikaciju korisnika i enkripciju podataka. Pod autentikacijom se podrazumijeva proces prijave korisnika i provjere njegova identiteta. Ona je važna jer osigurava pravo pristupa poslužitelju i pretincu samo ovlaštenom korisniku. Enkripcija se odnosi na zaštitu podataka koji se šalju mrežom. Ukoliko je autentikacija sigurna, podaci se svejedno mogu otkriti ako se mrežom šalju u čitljivom obliku. Također, enkripcija se može odnositi na zaštitu podataka na poslužitelju. To je pak teže iskoristiva ranjivost jer napadač prvo mora pronaći i iskoristiti ranjivost samog poslužitelja da bi stekao neovlašten pristup.

3.1. Autentikacija

Već je spomenuto kako se autentikacija na IMAP poslužitelju može provesti jednostavnom LOGIN naredbom. Problem kod ove vrste prijave na sustav jest taj što se podaci šalju nezaštićeni kroz mrežu. Napadač koji ih uspije otkriti može iskoristiti korisničko ime i lozinku za krađu identiteta korisnika. IMAP zato nudi naprednije mehanizme autentikacije kroz naredbu AUTHENTICATE i SASL mehanizme.

3.1.1. AUTHENTICATE

Naredba AUTHENTICATE prima samo jedan argument koji sadrži ime autentikacijskog mehanizma.

Poslužitelj može vratiti negativan odgovor (NO) ako mehanizam nije podržan ili BAD ako je naredba krivo oblikovana. U slučaju ispravnog zahtjeva poslužitelj šalje odgovor koji traži dodatne podatke kako bi se obavila autentikacija navedenim protokolom. Uspješna autentikacija završit će odgovorom OK, a neuspješna odgovorom NO ili BAD, ovisno o vrsti pogreške. Primjer PLAIN mehanizma, koji slično kao LOGIN, šalje samo korisničko ime i lozinku kao čisti tekst dan je u nastavku:

```
---uspostavljena je TLS veza---
KLIJENT: A01 AUTHENTICATE PLAIN
POSLUŽITELJ: +
KLIJENT: dGVzdAB0ZXN0AHRlc3Q=
POSLUŽITELJ: A01 OK Success (tls protection)
```

Drugi primjer može biti korištenje GSSAPI (eng. *Generic Security Services Application Program Interface*) sučelja preko kojeg se mogu koristiti različiti sigurnosni protokoli (npr. Kerberos autentikacijski protokol).

```
KLIJENT: A001 AUTHENTICATE GSSAPI
POSLUŽITELJ: +
KLIJENT: YIIB+wYJKoZIhvcSAQICAQBuggHqMIIB5qADAgEFoQMCAQ6iBw
   MFACAAAACjggEmYYIBIjCCAR6gAwIBBaESGxB1Lndhc2hpbmd0
   b24uZWR1oi0wK6ADAgEDoSQwIhsEaW1hcBsac2hpdmFtcy5jYW
   Mud2FzaGluZ3Rvbi5lZHWjgdMwgdCgAwIBAaEDAgEDooHDBIHA
   cS1GSa5b+fXnPZNmXB9SjL8Ollj2SKyb+3S0iXMljen/jNkpJX
   AleKTz6BQPzj8duz8EtoOuNfKgweViyn/9B9bccy1uuAE2HI0y
   C/PHXNNU9ZrBziJ8Lm0tTNc98kUpjXnHZhsMcz5Mx2GR6dGknb
   I0iaGcRerMUsWOuBmKKKRmVMMdR9T3EZdpqsBd7jZCNMWotjhi
   vd5zovQlFqQ2Wjc2+y46vKP/iXxWIuQJuDiisyXF0Y8+5GTpAL
   pHDc1/pIGmMIGjoAMCAQGigZsEgZg2on5mSuxoDHEA1w9bcW9n
   FdFxDKpdrQhVGVRDIzcCMCTzvUboqb5KjY1NJKJsfjRQiBYBdE
   NKfzK+g5DlV8nrw81uOcP8NOQCLR5XkoMHC0Dr/80ziQzbNqhx
   O6652Npft0LQwJvenwDI13YxpwOdMXzkWZN/XrEqOWp6GCgXTB
   vCyLWLlWnbaUkZdEYbKHBPjd8t/1x5Yg==
POSLUŽITELJ: + YGgGCSqGSIb3EgECAgIAb1kwV6ADAgEFoQMCAQ+iSzBJoAMC
     AQGiQgRAtHTEuOP2BXb9sBYFR4SJlDZxmg39IxmRBOhXRKdDA0
     uHTCOT9Bq3OsUTXUlk0CsFLoa8j+gvGDlgHuqzWHPSQg==
KLIJENT:                              (prazan odgovor)
POSLUŽITELJ: + YDMGCSqGSIb3EgECAgIBAAD/////6jcyG4GE3KkTzBeBiVHe
```

```
     ceP2CWY0SR0fAQAgAAQEBAQ=
KLIJENT: YDMGCSqGSIb3EgECAgIBAAD/////3LQBHXTpFfZgrejpLlLImP
         wkhbfa2QteAQAgAG1yYwE=
POSLUŽITELJ: A001 OK GSSAPI authentication successful
```

U dokumentu RFC 4959 (*IMAP Extension for Simple Authentication and Security Layer – SASL, Initial Client Response*) opisan je dodatak protokolu koji omogućuje da klijenti u AUTHENTICATE zahtjev dodaju drugi argument koji će uz ime metode dodati i potrebne podatke za provođenje autentikacije (npr. korisničko ime i lozinku). Na taj način izbjegava se slanje dodatnog zahtjeva poslužitelja za podacima i još jednog odgovora klijenta. Prethodni primjer AUTHENTICATE PLANE (spomenut je kao alternativa LOGIN naredbi, a uključuje samo korisničko ime i lozinku) izveden prema ovoj specifikaciji izgledao bi ovako:

```
C: C01 CAPABILITY
S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN
S: C01 OK Completed
C: A01 AUTHENTICATE PLAIN dGVzdAB0ZXN0AHRlc3Q=
S: A01 OK Success (tls protection)
```

U ovom primjeru pridodana je i CAPABILITY naredba, preko koje klijent doznaje da je dostupan *Initial Client Response* mehanizam (SASL-IR). Osim toga znakovni niz prikazan je u *base64* kodiranju.

3.1.2. SASL

SASL (eng. *Simple Authentication and Security Layer*) je strukturirano sučelje koje omogućuje autentikaciju i korištenje sigurnosnih mehanizama u komunikacijskim protokolima. Autentikacijski mehanizmi koje SASL podržava mogu se koristiti u svim protokolima koji imaju SASL podršku. Ti mehanizmi mogu uključivati i zaštitu integriteta i tajnosti podataka. Primjer takvog SASL mehanizma je DIGEST-MD5. Sučelje se često koristi u kombinaciji sa TLS protokolom za kriptografsku zaštitu podataka.

Definirani SASL mehanizmi su:

- EXTERNAL – implicitna autentikacija kod protokola koji sami po sebi koriste zaštitu (npr. IPsec, TLS),
- ANONYMOUS – anonimni klijenti,
- PLAIN – obična prijava korisničkim imenom i lozinkom koji se šalju u čitljivom obliku,
- OTP – mehanizam jednokratne lozinke,
- SKEY – S/KEY mehanizam,
- CRAM-MD5 i DIGEST-MD5 – autentikacija na temelju kriptografskog sažetka,
- NTLM – autentikacijski protokol,
- GSSAPI – generičko sučelje za Kerberos V5 autentikacijski protokol i
- GateKeeper mehanizam.

Naredba AUTHENTICATE IMAP protokola koristi SASL sučelje. Primjer EXTERNAL autentikacije, u slučaju korištenja TLS protokola, može biti sljedeći:

```
---Uspostavljena je TLS veza---
KLIJENT: A01 AUTHENTICATE EXTERNAL
POSLUŽITELJ: +
KLIJENT:
POSLUŽITELJ: A01 OK Success (tls protection)
```

3.2. Enkripcija

Enkripcija podataka štiti njihovu tajnost bilo da se oni nalaze na nekom poslužitelju ili da se šalju kroz mrežu. Kod IMAP protokola poruke iz korisničkog pretinca šalju se klijentu mrežom. Pritom napadač može otkriti njihov sadržaj ukoliko ih tijekom prijenosa uspije dohvatiti. Kako bi se onemogućila ova vrsta zlouporabe koristi se enkripcija.

3.2.1. STARTTLS

STARTTLS naredba, koju klijent šalje poslužitelju, zahtjeva uspostavljanje kriptirane veze iznad TLS protokola To znači da svi podaci koje šalje IMAP, prije stvarnog slanja kroz mrežu, prolaze „kroz obradu" TLS protokolom. TLS (eng. *Transport Layer Security*) je nasljednik SSL (eng. *Secure Socket Layer*) kriptografskog protokola. Riječ je o protokolima transportnog sloja koji osiguravaju enkripciju podataka prije nego se isti pošalju preko mreže. Svaki korisnik kriptografskog protokola mora imati svoj privatni i javni ključ. Javni ključ koristi se za šifriranje podataka koji se šalju, a pomoću pripadnog tajnog ključa te podatke je moguće dešifrirati. Budući da je tajni ključ poznat jedino njegovom vlasniku, on će jedini moći pročitati poslane podatke. Za dodjelu javnih ključeva i njihovu distribuciju drugim korisnicima danas se najčešće koristi PKI (eng. *Public Key Infrastructure*) infrastruktura. Ona se zasniva na općem povjerenju u certifikacijska tijela (eng. CA - Certificate Authorities) koja dodjeljuju i distribuiraju ključeve. Osim toga, moguće je korištenje tzv. „mreže povjerenja" kao kod na primjer PGP (eng. *Pretty Good Privacy*) sustava. Navedeni mehanizmi razlikuju se po tome što kod CA korisnici ključeve traže od povjerljivih trećih strana dok PGP pretpostavlja mrežu u kojoj korisnici ključeve saznaju od drugih korisnika, a pritom povjerenje u nečiju vjerodostojnost opada s udaljenošću u mreži. Primjerice najpouzdaniji je ključ saznat direktno od njegovog vlasnika, a manje pouzdani su ključevi koji nisu dobiveni izravno od vlasnika već preko nekih drugih korisnika (poznanik vlasnika ključa, poznanik poznanika itd.) .

TLS protokol u svakom slučaju zahtjeva posjedovanje vlastitog certifikata i tajnog ključa te certifikata druge strane komunikacije.

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
        70:47
```

Slika 6. Digitalni certifikat

Sama STARTTLS naredba ne prima nikakve argumente, a vraća OK ako je pokrenuto uspostavljanje TLS veze na nižem sloju ili BAD ako je naredba krivo oblikovana. Nakon završetka naredbe, započinje uspostavljanje TLS veze koje se odvija na nižem sloju sustava. IMAP je protokol višeg, aplikacijskog sloja, dok se TLS odvija na transportnom sloju, odmah iznad IP mreže.

```
KLIJENT: a001 CAPABILITY
POSLUŽITELJ: * CAPABILITY IMAP4rev1 STARTTLS LOGINDISABLED
KLIJENT: a001 OK CAPABILITY completed
POSLUŽITELJ: a002 STARTTLS
POSLUŽITELJ: a002 OK Begin TLS negotiation now
               ---Uspostavljanje TLS veze---
KLIJENT: a003 CAPABILITY
POSLUŽITELJ: * CAPABILITY IMAP4rev1 AUTH=PLAIN
POSLUŽITELJ: a003 OK CAPABILITY completed
KLIJENT: a004 LOGIN ime prezime
POSLUŽITELJ: a004 OK LOGIN completed
```

U gornjem primjeru programskog koda dan je primjer IMAP poslužitelja koji ne dozvoljava LOGIN naredbu ako je veza nesigurna. Uspostavljanjem sigurne TLS veze, omogućuje se PLAIN autentikacija korisničkim imenom i lozinkom koji se šalju kao čitljivi tekst, tj. podaci se šalju kao čitljivi tekst s aplikacijskog sloja, ali zbog TLS veze se kriptiraju na transportnom sloju pa tako njihova tajnost ostaje zaštićena. Na slici 4. prikazano je zahtijevanje SSL zaštite kod povezivanja na GMail IMAP poslužitelj.

3.2.2. Tuneliranje

Ukoliko IMAP poslužitelj ne podržava SSL u svojoj implementaciji, moguće je vezu zaštititi tuneliranjem. *Stunnel* je primjer alata koji omogućuje zaštitu nesigurnog protokola SSL kriptiranjem na nižoj, transportnoj razini. Primjerice, na UNIX sustavima za SSL tuneliranje potrebno je instalirati OpenSSL biblioteku koja sadrži implementaciju SSL protokola. Spomenuto je kako SSL zahtjeva posjedovanje SSL certifikata. Uspostava SSL tunela za IMAP na poslužitelju može izgledati ovako:

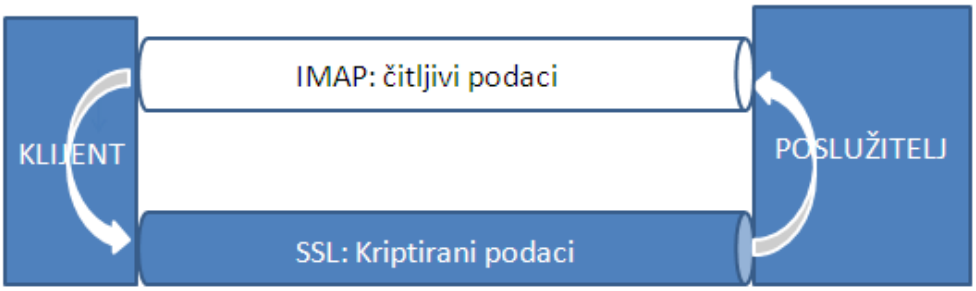
```
stunnel –d 993 –p /usr/local/certs/stunnel.pem –r localhost:imap
```

993 je priključak na kojem se čekaju zahtjevi koji se šalju preko SSL veze, a *stunnel.pem* je datoteka koja sadrži digitalni certifikat poslužitelja.

Tuneliranje na klijentu uspostavlja se naredbom:

```
stunnel –c –d 143 –p –r imap_posluzitelj:993
```

143 je priključak IMAP protokola, a *imap_posluzitelj* IP adresa ili ime poslužitelja.



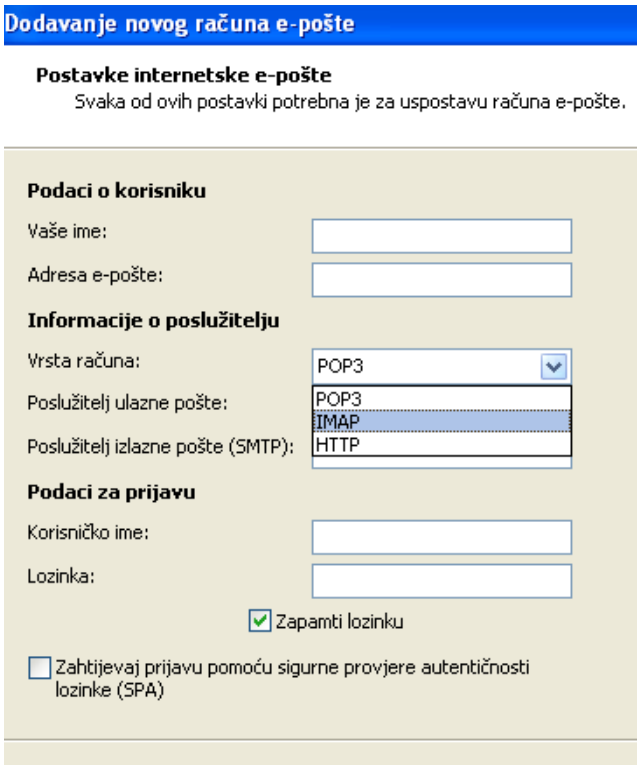
Slika 7. Skica SSL tuneliranja za IMAP

4. Alternative

Postoji veći broj protokola koji se koriste za dohvat elektroničke pošte. Većina njih vezana je uz komercijalna rješenja. Tako komercijalni poslužitelji i klijenti, (npr. Microsoft, IBM i Apple), koriste vlastite protokole za dohvat pošte. Ipak, jedini protokol koji se u pravom smislu može uspoređivati s IMAP-om je POP, jer su oba otvorena i vrlo raširena. Zbog toga su podržani u brojnim besplatnim, ali i komercijalnim poslužiteljima i klijentima elektroničke pošte.

4.1. POP3

Kao i IMAP, POP omogućuje dohvat elektroničke pošte s udaljenog poslužitelja. Trenutna standardna inačica POP-a je POP3. IETF specifikacija protokola nalazi se u RFC dokumentu 1939. U izvornoj inačici POP3 je podržavao samo jednostavnu autentikaciju korisnika korisničkim imenom i lozinkom, bez zaštite enkripcijom. Do danas je uvedena podrška za SASL koja omogućuje autentikaciju sigurnijim protokolima kao što je Kerberos. AUTH mehanizam koji uvodi ovu podršku dostupan je kao dodatak protokolu. Osim toga dostupan je i APOP mehanizam koji uvodi tzv. „challenge/response" autentikaciju temeljenu na MD5 algoritmu za izradu digitalnih sažetaka (eng. *hash*).



Slika 8. Izbor protokola u Outlooku

4.1.1. Funkcionalnost

Prema funkcionalnosti, IMAP je napredniji protokol. POP primjerice nema podršku za MIME ugrađenu u svojoj specifikaciji. Također, kod POP protokola poruke mogu imati isti identifikator što može usporiti dohvat novih poruka u slučaju velikih pretinaca. Primjerice, IMAP razmatra samo poruke s većim ID-om od posljednje zabilježenog. Kod POP-a takva selekcija nije moguća. POP se, za razliku od IMAP-a, povezuje na poslužitelj samo kad dohvaća poruke i nema trajno uspostavljenu vezu tijekom koje može dohvaćati poruke na zahtjev. Također, POP u osnovi ne podržava rad s porukama na poslužitelju pa nema sinkronizacije klijenta i poslužitelja. Zato jednom pretincu može pristupati samo jedan klijent.

Iz većih mogućnosti IMAP protokola proizlazi i njegov nedostatak - veća složenost. Primjerice, IMAP klijenti moraju održavati TCP/IP vezu s poslužiteljem. Pretraživanje na poslužitelju može oduzeti puno vremena ukoliko se koriste loši algoritmi.

4.1.2. Sigurnost

Prema sigurnosnim obilježjima IMAP i POP razlikuju se prema tome što se kod POP-a za sigurnu autentikaciju moraju koristiti APOP ili SASL mehanizmi koji su dostupni kao dodatak. IMAP u svojoj specifikaciji podržava SASL. Što se enkripcije tiče, u POP-u je dostupna STLS naredba kojom se uspostavlja SSL/TLS enkripcija podataka kao što se kod IMAP koristi STARTTLS. Oba protokola moguće je tunelirati preko SSL veze. Jedino se za POP koriste drukčiji priključci:

- 110 - POP,
- 995 - SSL-POP.

IMAP sam po sebi nudi nešto više ugrađenih mogućnosti. Ovisno o potrebama korisnika, može se odabrati IMAP s više funkcija ili jednostavan POP. Sa stanovišta sigurnosti, protokoli su podjednako sigurni, s tim da IMAP u svojoj osnovnoj specifikaciji podrazumijeva više sigurnosnih mehanizama. Većina ozbiljnih i češće korištenih poslužitelja u slučaju bilo kojeg od ova dva protokola zahtjeva određenu razinu zaštite (npr. uspostavljanje veze povrh SSL kanala). Za administratore poslužitelja važno je da ih ispravno konfiguriraju, a za klijente da znaju koje su važne sigurnosne postavke i moguće posljedice ukoliko se one zaobiđu.

4.2. Budućnost

Zadnja inačica IMAP RFC 3501 specifikacije nije se mijenjala od 2003. godine. Nadograđena je s nekoliko dokumenata koji uvode nove naredbe. Među njima je i spomenuto proširenje AUTHENTICATE mehanizma s argumentom koji sadrži odgovor klijenta na predstojeći zahtjev poslužitelja za podacima. Posljednja nadogradnja specifikacije izašla je ove godine, a uvodi podršku za UTF-8 znakove u korisničkim imenima, zaglavljima i adresama elektroničke pošte (RFC 5738). Ona se još uvijek tretira kao eksperimentalna. Standard je još u kontinuiranom razvoju te se njegove novije i revidirane inačice predviđaju i u samoj specifikaciji.

5. Zaključak

IMAP protokol preporuča se korisnicima koji žele raditi s elektroničkom poštom na lokalnom računalu, a mogućnosti koje nudi POP3 nisu im dostatne. Nema zapravo ključne razlike između ova dva protokola koja bi bilo koji od njih učinila univerzalno boljim po pitanju sigurnosti. I jedan i drugi protokol nude sigurnosne mehanizme za zaštitu podataka. Prednošću IMAP-a može se smatrati to što on upotrebu tih mehanizama zahtjeva u samoj svojoj specifikaciji dok je kod POP-a ona uvedena kroz dodatke protokolu kao što je APOP. Bez obzira na to, neoprezna primjena i konfiguracija bilo kojeg IMAP ili POP3 poslužitelja, odnosno klijenta, može predstavljati sigurnosni rizik.

Kod IMAP-a sigurnost se može postići na više načina i više razina. Moguće je korištenje sigurnih složenih protokola za provjeru identiteta korisnika preko SASL sučelja i AUTHENTICATE naredbe. Klasičnu autentikaciju korisničkim imenom i lozinkom moguće je zaštiti slanjem podataka preko SSL kanala. SSL protokol također se koristi za zaštitu poruka koje se s poslužitelja šalju klijentu. Pomoću STARTTLS naredbe SSL enkripcija integrirana je u sam IMAP protokol. Alternativno moguće ju je provesti SSL tuneliranjem.

Zaključak je da IMAP nudi dovoljno sigurnosnih mehanizama za zaštitu podataka što se odnosi i na provjeru identiteta korisnika i na zaštitu tajnosti i integriteta podataka koji se šalju mrežom. A kako bi se dostupna zaštita na prikladan način iskoristila važna je uloga samog korisnika u odabiranju sigurnih postavki prilikom konfiguriranja i korištenja IMAP klijenta, odnosno poslužitelja.

6. Reference

[1] Wikipedia: Internet Message Access Protocol, http://en.wikipedia.org/wiki/Imap, svibanj 2010.

[2] Wikipedia: Post Office Protocol, http://en.wikipedia.org/wiki/Post_Office_Protocol, svibanj 2010.

[3] IMAP Security - encryption and authentication, http://www.coruscant.demon.co.uk/mike/imap/security.html, svibanj 2010.

[4] Roberto Cecchini: Secure IMAP (and POP3), http://security.fi.infn.it/tools/stunnel/index-en.html, svibanj 2010.

[5] Chaos Golubitsky – Carnegie Mellon University: Toward an Automated Vulnerability Comparison of Open Source IMAP Servers, http://www.usenix.org/event/lisa05/tech/golubitsky/golubitsky.pdf, svibanj 2009.