HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Simple Authentication and Security Layer - SASL

CCERT-PUBDOC-2005-06-125

CARNet CERT u suradnji s LS&S

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

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

CARNet 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 4

2. SASL – SIMPLE AUTHENTICATION AND SECURITY LAYER 5

2.1. KONCEPT IDENTITETA 5
2.2. AUTENTIKACIJA 5
2.2.1. Odabir mehanizma autentikacije 6
2.2.2. Sigurnosni sloj 7
2.3. ZAHTJEVI PROTOKOLA 7
2.4. SASL MEHANIZMI 7

3. PRIMJER KORIŠTENJA SASL PODRŠKE U SMTP PROTOKOLU 9

4. ZAKLJUČAK 13

5. REFERENCE 13

1. Uvod

Uobičajeno je da definicija protokola zadovoljava samo jedan konkretan dio neke funkcionalnosti. Kao primjer se može navesti SMTP protokol koji isključivo služi za prijenos poruka elektroničke pošte između poslužitelja. Kod procesa autentikacije potreban je drukčiji pristup. Prvi razlog tomu je nepostojanje savršenog autentikacijskog mehanizma. Uvijek postoji određena razina kompromisa između faktora kao što su prilagodljivost korisniku, mrežna sigurnost, lakoća upravljanja, te efikasnost. Ovo dovodi do postojanja izbora više autentikacijskih mehanizama s različitim karakteristikama. Drugi razlog je da se izbor sigurnog autentikacijskog mehanizma mijenja kako se mehanizmi razvijaju s obzirom na povećane računalne sposobnosti, sigurnosne zahtjeve i nove tehnologije. Potrebno je prepoznati da će i dalje biti više različitih pristupa procesu autentikacije, te se ne može očekivati prevladavanje samo jednog jedinstvenog mehanizma autentikacije.

SASL (engl. *Simple Authentication and Security Layer*) je standard koji definira način dodavanja autentikacijske podrške različitim protokolima. SASL nije protokol, već samo okvir koji aplikacijskim protokolima omogućuje pregovaranje o autentikacijskom mehanizmu koji će biti korišten. U ovisnosti o podržanim mehanizmima, SASL omogućuje autentikaciju klijenta poslužitelju, autentikaciju poslužitelja klijentu, te povjerljivost podataka. Za svaki protokol koji SASL koristi, postoji specifikacija načina kako taj protokol koristi ovaj apstraktni sloj. Ovo znači da SASL može biti korišten u velikom broju protokola, te može biti detaljno adaptiran za svakog od njih.

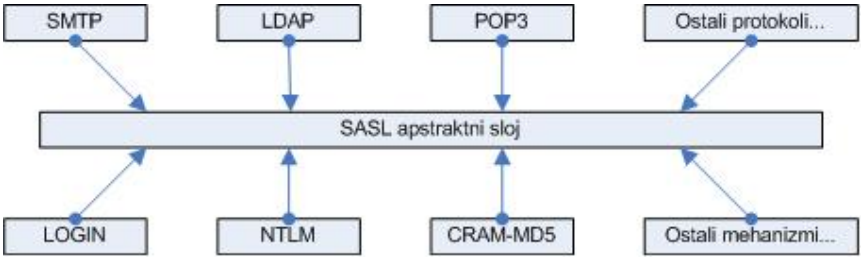
Sistem administratorima SASL omogućava podešavanje upravo one razine sigurnosti koja je neophodna za mrežne aplikacije u njihovom okruženju. Dio protokola koji je vezan uz sigurnost ponaša se kao dinamički učitani modul: poslužitelj nudi dostupne metode, dok klijent odabire koja će od njih biti korištena. Lista mehanizama je proširiva, čime se rješava problem okruženja s različitim zahtjevima, te uključivanje novih i efikasnijih metoda autentikacije.

U ovom dokumentu opisana je SASL tehnologija, te je dan primjer konfiguracije SMTP poslužitelja koji koristi SASL podršku.

2. SASL – Simple Authentication and Security Layer

SASL je apstraktni sloj koji omogućuje autentikaciju i povjerljivost podataka u protokolima koji se baziraju na konekcijama putem izmjenjivih mehanizama. SASL sloj pruža strukturirano sučelje između protokola i mehanizama za autentikaciju. SASL je osmišljen na taj način da omogućuje novim protokolima korištenje postojećih mehanizama autentikacije bez potrebe za redizajnom mehanizma, te također da postojećim protokolima omogućuje korištenje novih mehanizama bez ikakvih promjena na protokolu.

SASL je konceptualno samo okvir koji definira apstraktni sloj između protokola i mehanizama, kao što je prikazano na slici 1.



Slika 1. SASL apstraktni sloj

Kroz sučelje ovog apstraktnog sloja protokolima je omogućeno korištenje bilo kojeg mehanizma. Iako ovaj sloj skriva posebnosti protokola od mehanizama autentikacije, i obrnuto, za programska ostvarenja protokola, mehanizmi moraju biti detaljno definirani. Ovome je razlog što različiti mehanizmi zahtijevaju različite podatke da bi ispravno funkcionirali. Dok jedni mehanizmi koriste autentikaciju koja se bazira na zaporkama, nekima od njih je potrebna i informacija o domeni, certifikatu, Kerberos oznakama itd. Za ispravno izvršavanje postupka autorizacije, programska ostvarenja poslužitelja moraju imati implementirano raspoznavanje autentikacijskih identiteta, koji ovise o mehanizmu, i autorizacijskih identiteta koji ovise o protokolu. Koncept identiteta je detaljnije opisan u poglavlju 2.1.

Svaki protokol koji želi koristiti SASL podršku mora definirati metodu kojom se identificira koji će se mehanizam koristiti, metodu izmjene izazova (engl. *Challenge*) poslužitelja i klijentskih odgovora (*engl. Response*), te metodu za izmjenu rezultata autentikacije.

Svaki SASL mehanizam definira niz izazova poslužitelja i odgovarajućih klijentskih odgovora kojima se definira uspješnost usluga autentikacije i kojima se pregovaraju usluge koje pružaju povjerljivost podataka. Nešto više o zahtjevima za SASL mehanizme moguće je pročitati u poglavlju 2.3.

2.1. Koncept identiteta

Procesi autentikacije i autorizacije mogu posjedovati različite, zasebne identitete. SASL koristi dvije vrste identiteta:

- identitet vezan uz autentikacijski proces (autentikacijski identitet),
- identitet pod kojim korisnik izvršava naredbe na sustavu (autorizacijski identitet).

Klijent šalje svoj autentikacijski identitet, te potencijalno i dodatni znakovni niz koji predstavlja autorizacijski identitet. Ako je ovaj niz prazan, podrazumijeva se da klijent želi izvršavati radnje na sustavu s ovlastima identiteta koji je isti kao i autentikacijski identitet (autentikacijski i autorizacijski identitet su isti). Poslužitelj je odgovoran za provjeru ovih identiteta, te će doći do neuspješne SASL izmjene ako bilo koja od ove dvije provjere ne uspije.

Specifikacija SASL mehanizma definira oblik autentikacijskog identiteta (npr. Kerberos oznaka, X.509 certifikat, korisničko ime/zaporka), te sintaksu i semantiku istog identiteta gdje je to potrebno. Za oblik autorizacijskog identiteta je zadužena specifikacija protokola koji želi koristiti SASL podršku.

2.2. Autentikacija

Proces autentikacije započinje klijent, slanjem poruke u kojoj od poslužitelja zahtjeva početak autentikacije putem određenog mehanizma. Klijent specificira željeni mehanizam njegovim imenom u

poruci zahtjeva. Slijedi izmjena parova izazova poslužitelja i odgovora klijenta. Nakon što je autentikacijska izmjena završila, poslužitelj šalje rezultat klijentu o uspješnosti autentikacije.
Konceptualni pregled procesa autentikacije:

```
C: Zahtjev za autentikacijom
S: Inicijalni izazov
C: Inicijalni odgovor
<dodatne izazov/odgovor poruke>
S: Rezultat autentikacije
```

U navedenom primjeru oznaka 'C' predstavlja klijenta (engl. *Client*) , dok oznaka 'S' predstavlja poslužitelj (engl. *Server*).
Ako je ishod autentikacije uspješan, a korišten je mehanizam koji omogućava sigurnosni sloj i ujedno je dogovoreno njegovo korištenje, slijedi instalacija ovog podatkovnog sloja.
Slijed poruka koje se izmjenjuju u procesu autentikacije se razlikuje od mehanizma do mehanizma. Neki mehanizmi zahtijevaju od klijenta da uz zahtjev za autentikacijom pošalje i neke dodatne podatke. Da li će ovi podaci biti poslani u dodatnom polju zahtjeva, ili tek nakon što poslužitelj pošalje prazan izazov, ovisi o protokolu unutar kojeg se koristi ovakav mehanizam:

```
1. način:

C: Zahtjev za autentikacijom + inicijalni odgovor
<dodatne izazov/odgovor poruke>
S: Rezultat autentikacije

2. način:

C: Zahtjev za autentikacijom
S: Prazan izazov
C: Inicijalni odgovor
<dodatne izazov/odgovor poruke>
S: Rezultat autentikacije
```

Slijed poruka se može razlikovati i zbog nekih drugih dodatnih zahtjeva mehanizama, kao što su dodatni podaci koje poslužitelj šalje klijentu uz rezultat autentikacije. Ukupan broj izmijenjenih poruka opet će ovisiti o specifikaciji protokola i formatima poruka koje određeni protokol podržava. Kroz izmjenu poruka mehanizam može:

- autenticirati klijenta poslužitelju,
- autenticirati poslužitelja klijentu,
- prenijeti znakovni niz s autorizacijskim identitetom,
- dogovoriti sigurnosni sloj,
- osigurati neke druge servise koje mehanizam podržava.

Klijent ili poslužitelj mogu u bilo kojem trenutku prekinuti autentikaciju ukoliko ne mogu ili ne žele nastaviti. Klijent može prekinuti autentikaciju slanjem poruke koja je specifična za svaki protokol zasebno, kojom ukazuje na prekid izmjene autentikacijskih podataka. Isto vrijedi ukoliko je poslužitelj taj koji želi obustaviti autentikaciju. Osim dobrovoljnog prekida autentikacije, moguće je da proces autentikacije ne uspije zbog jednog od slijedećih razloga:

- autentikacijski identitet nije prošao provjeru,
- znakovni niz autorizacijskog identiteta nije formiran u ispravnom obliku,
- autentikacijski identitet nema ovlasti za željeni autorizacijski identitet,
- sigurnosni sloj je nedovoljan,
- poslužitelj iz bilo kojeg razloga ne želi pružiti usluge klijentu.

2.2.1. Odabir mehanizma autentikacije

Pregovori poslužitelja i klijenta o mehanizmu koji će biti korišten za proces autentikacije ovise o protokolu i njegovoj specifikaciji. Uobičajeno je da protokol specificira naredbu kojom poslužitelj oglašava podržane mehanizme. Na klijentu je da odabere mehanizam kojeg i on sam podržava, te mu ujedno najviše odgovara.
Pregovori koji se vode o odabiru mehanizma nisu zaštićeni, te ukoliko se žele izbjeći potencijalni napadi na ovaj segment SASL procedure potrebno je uvesti zaštitu iz nekog drugog izvora. Napad koji

se može provesti vezan uz odabir mehanizma je modifikacija presretnutog zahtjeva i odabir slabijeg mehanizma od onog kojeg je klijent sam odabrao.

2.2.2. Sigurnosni sloj

Tijekom autentikacije vrši se i pregovaranje da li će se u komunikaciji koristiti neka vrsta zaštite podataka. O kojoj vrsti zaštite se radi ovisi o SASL mehanizmu, međutim uobičajene usluge su zaštita povjerljivosti i integriteta podataka. Postoje i mehanizmi koji ne pružaju nikakav oblik zaštite, odnosno sigurnosnog sloja.

Sigurnosni sloj koji je dogovoren postaje aktivan na poslužitelju onog trena kada poslužitelj javi uspješan ishod autentikacije, dok na klijentu ovaj sloj postaje aktivan nakon što klijent primi potvrdan odgovor. Nakon što sigurnosni sloj započne svoje djelovanje na podatkovnom nizu protokola, on je aktivan sve dok se ne dogovori novi sigurnosni sloj ili dok se konekcija ne prekine.

Sigurnosni sloj procesira sve podatke u zaštićene pakete. Svaki takav paket zaštićenih podataka se prenosi kao niz okteta koji uvijek započinju s poljem (duljine četiri okteta) u kojem je navedena veličina cijelog paketa. Ova veličina ne smije prelaziti maksimalnu dogovorenu veličinu, te bi se konekcija pri pojavi takvog slučaja trebala prekinuti kako bi se izbjegli potencijalni napadi.

2.3. Zahtjevi protokola

Protokol može ponuditi SASL usluge samo ako njegova specifikacija definira slijedeće informacije:

- Naziv usluge, koji mora biti identičan nazivu koji je registriran na IANA (*engl. Internet Assigned Numbers Authority*) stranicama,
- Definiciju poruka koje služe za izmjenu autentikacijskih podataka; one uključuju poruke zahtjeva za početak autentikacije (kao parametar mora biti naveden naziv mehanizma koji se zahtjeva), poruke izazova i odgovora, te poruke za javljanje ishoda autentikacije,
- Definicija sintakse i semantike za znakovne nizove koje sadrže autorizacijski identitet,
- Precizna definicija trenutka u kojem sigurnosni sloj započinje s radom u oba smjera.

Neki od protokola koji pružaju SASL podršku:

- LDAP (Internet Standard Lightweight Directory Access Protocol)
- SMTP (Internet Standard Simple Mail Transfer Protocol)
- POP3 (Internet Standard Post Office Protocol v3)
- IMAP (Internet Standard Internet Mail Access Protocol)
- XML bazirani protokoli: XMPP (Extensible Messaging and Presence Protocol), BEEP (Blocks Extensible Exchange Protocol).

2.4. SASL mehanizmi

Mehanizam može postati registrirani SASL mehanizam ukoliko autor mehanizma podnese zahtjev za registracijom, te ukoliko taj mehanizam zadovoljava sve zahtjeve koji se postavljaju. Zahtjev je javno dostupan, a lista podržanih registriranih mehanizama se nalazi na stranicama IANA organizacije.

Zahtjevi koji se postavljaju na mehanizme su slijedeći:

- ime mehanizma mora odgovarati propisanoj sintaksi,
- izazovi poslužitelja i odgovori klijenta moraju biti definirani, uz napomenu da li se od klijenta očekuje da prvi šalje podatke i da li se od poslužitelja očekuju neki dodatni podaci nakon što je autentikacija završena,
- mora biti definirano da li mehanizam podržava zasebne autorizacijske identitete,
- mora biti definirano da li postoji mogućnost korištenja sigurnosnog sloja, te ukoliko je to moguće mora se specificirati koje su usluge nude i na koji se način implementiraju.

Trenutna lista registriranih SASL mehanizama broji više od 20 mehanizama, od kojih su neki vrlo rijetko korišteni ili zastarjeli. U slijedećoj tablici se nalazi popis SASL autentikacijskih mehanizama koji se trenutno najčešće koriste.

Mehanizam	Standard	Namjena
PLAIN	RFC 2595	Zaporka u tekstualnom obliku
LOGIN	De facto	Alternativa PLAIN mehanizmu
CRAM-MD5	RFC 2195	MD5 sažetak za autentikaciju klijenta
DIGEST-MD5	RFC 2831	Dodaje autentikaciju poslužitelja i povjerljivost CRAM-MD5 mehanizmu
EXTERNAL	RFC 2222	Za korištenje uz SSL/TSL podršku i X.509 digitalne potpise
NTLM	Microsoft	Microsoft inačica CRAM-MD5 mehanizma
OTP	RFC 2444	Za jednokratne zaporke (engl. *One Time Password*)
ANONYMOUS	RFC 2245	Za anonimno korištenje resursa sustava
GSSAPI	RFC 2222	Za podršku Kerberos autentikaciji
KERBEROS_V4 KERBEROS_V5	RFC 2222	Za podršku Kerberos autentikaciji

3. Primjer korištenja SASL podrške u SMTP protokolu

Za testiranje rada SASL podrške odabran je SMTP protokol, protokol za prijenos poruka elektroničke pošte. Njegova jedina namjena je da uspješno i pouzdano prenosi poruke elektroničke pošte između poslužitelja, te stoga samo osigurava mehanizme za prijenos navedenih poruka. SMTP protokol ne nudi nikakve sigurnosne usluge, te se sva komunikacija odvija bez ikakve zaštite, kao što se ni ne provodi autentikacija korisnika. SMTP standard definira ključne riječi koje se koriste za izvršavanje naredbi na sustavu. Da bi se uključila i podrška za nekakav oblik autentikacije naknadno je definirana dodatna ključna riječ 'AUTH'. Naredbom 'AUTH' klijent zahtjeva autentikaciju, te kao argument navodi željeni mehanizam:

```
AUTH argument
```

Argument ove naredbe je znakovni niz koji sadrži registrirano ime SASL mehanizma. Nakon što poslužitelj uspješno izvrši ovu naredbu, ponavljanje ove naredbe nije dozvoljeno, te poslužitelj odbija sve daljnje pokušaje. Ako poslužitelj podržava željeni mehanizam, on izvršava autentikacijski proces kako bi se korisnik uspješno prijavio na sustav. Ako odabrani mehanizam podržava i sigurnosni sloj, tada se obavlja i dogovor oko svih postavki ovog sloja. 'AUTH' naredba se odbija ukoliko poslužitelj ne podržava mehanizam koji korisnik zahtjeva.

Za testiranje SASL podrške u SMTP protokolu odabran je sustav s Linux Debian operacijskim sustavom, posljednje stabilne inačice koja nosi naziv *Sarge*. Kao SMTP poslužitelj odabran je *Postfix* programski paket, dok je SASL podrška osigurana instalacijom *Cyrus* SASL programskog paketa.

Za instalaciju potrebnih paketa korištena je `apt-get` naredba.

```
# apt-get install libsasl2 libsasl2-modules
# apt-get install postfix
```

U slučaju korištenja nekih drugih Linux distribucija moguće je ove programske pakete instalirati iz izvornog programskog kôda.

Nakon što je instalirana neophodna programska podrška potrebno je podesiti odgovarajuće elemente sustava. U direktoriju `/etc/postfix/` nalaze se sve potrebne konfiguracijske datoteke vezane za Postfix programski paket. Potrebno je napraviti novi direktorij pod nazivom `sasl`, te u njemu kreirati `smtpd.conf` datoteku.

```
/etc/postfix# mkdir sasl
/etc/postfix# cd sasl
/etc/postfix# vi smtpd.conf
```

Datoteka `smtpd.conf` sadrži konfiguracijske postavke koje se odnose samo na nadolazeće *smtpd* autentikacijske sjednice. Ukoliko *Postfix* poslužitelj nije konfiguriran da koristi ikakav oblik autentikacije, *smtpd* procesi će se odvijati bez obzira na sadržaj ove datoteke, i bez korištenja autentikacije. Kreiranje i postavljanje ovih konfiguracijskih postavki je tek priprema za uključivanje SASL podrške u *Postfix* poslužitelj.

Prva direktiva `smtpd.conf` datoteke je ujedno najvažnija i jedina obavezna. Radi se o direktivi `pwcheck_method`, koja instaliranoj SASL podrški odgovara gdje je moguće pronaći autentikacijske podatke. Podržane su slijedeće metode:

- `pwcheck` – autenticiranje na temelju baze korisnika sustava. Za provjeru korisnika zadužen je `pwcheck` *daemon* proces koji mora imati ovlasti čitanja nad datotekama sustava za pohranu korisnika i njihovih zaporki. Preporučljivo je kreiranje specijalne grupe kojoj će biti dane ovlasti čitanja nad potrebnim datotekama, te pridruživanje korisnika *Postfix* u tu grupu.
- `saslauthd` – identičan način autenticiranja kao kod metode `pwcheck`, razlika je tek u *daemon* procesu koji je zadužen za čitanje autentikacijskih datoteka. `Saslauthd` *daemon* program je novijeg datuma, te će u narednim inačicama SASL podrške `pwcheck` biti izbačen. Funkcionalnih razlika, osim onih u načinu implementacije, između ova dva procesa gotovo da i nema. Važno je napomenuti da korištenjem jednog od ova dva načina provjere zaporke, lista podržanih mehanizama je ograničena samo na PLAIN i LOGIN mehanizme.
- `auxprop` – ova metoda koristi SASL datoteku sa zaporkama `/etc/sasldb2`. Dodavanje novih korisnika i održavanje ove baze se odvija putem `saslpasswd2` sistemske naredbe. Za korištenje dodatnih mehanizama poput CRAM-MD5 i DIGEST-MD5 nužno je koristiti ovu

metodu provjere SASL korisnika. Uz odabir ove metode moguće je definirati direktivu `auxprop_plugin` koja označava da li će se neka vanjska metoda, već prisutna na sustavu, koristiti za provjeru korisnika.

Osim direktive koja služi za odabir načina provjere korisnika, moguće je definirati i listu podržanih mehanizama. Svi SASL mehanizmi koji su instalirani kroz SASL module se automatski nalaze na ovoj listi, te stoga ova direktiva nije obavezna. U nekim slučajevima poželjno je eksplicitno definirati sve metode koje sustav podržava. Direktiva koja sadrži listu svih SASL mehanizama koje poslužitelj podržava je `mech_list`. Prilikom definiranja mehanizama bitno je da je autentikaciju zaista moguće provesti putem svih oglašenih mehanizama od strane poslužitelja. Kao primjer se može navesti odabir `saslauthd` metode koja podržava samo PLAIN i LOGIN mehanizme. Bez korištenja `mech_list` direktive, poslužitelj će obavijestiti korisnika da je autentikaciju moguće izvršiti i pomoću MD5 mehanizma, jer je uobičajeno da ovaj mehanizam dolazi u standardnoj distribuciji SASL podrške. Korisnik može odabrati ovu metodu jer mu je ona i ponuđena, međutim autentikaciju putem ovog mehanizma neće biti moguće izvršiti jer `saslauthd` proces ne provjerava `sasldb2` datoteku gdje bi za MD5 mehanizme trebali biti pohranjeni autentikacijski podaci korisnika.

Primjeri sadržaja `smtpd.conf` datoteke:

```
pwcheck_method: saslauthd
mech_list: plain login

...

pwcheck_method:  auxprop
mech_list: plain login cram-md5 digest-md5

...

pwcheck_method:  auxprop
auxprop_plugin:  sql
sql_engine: mysql
mech_list: plain login cram-md5 digest-md5
```

Nakon što su podešene postavke koje se tiču SASL procesa, potrebno je podesiti i *Postfix* poslužitelj. Sve promjene koje je potrebno uvesti se nalaze u `/etc/postfix/main.cf` datoteci. Dodatne direktive:

- `smtpd_sasl_auth_enable` – omogućavanje autentikacije SMTP protokola.
- `smtpd_sasl_security_options` – definiranje dodatnih sigurnosnih opcija. Ovo je samo mjera predostrožnosti kojom je moguće eksplicitno zabraniti anonimno prijavljivanje na sustav. Ukoliko je `mech_list` direktiva ostala nedefinirana, poslužitelj će podržavati i ANONYMOUS mehanizam. *Postfix* tretira ovaj mehanizam kao da nema autentikacije. Kako mail klijenti uglavnom redom prolaze kroz podržane mehanizme, moguće je da dođu i do ANONYMOUS mehanizma, te se stoga autentikacija zapravo i ne izvrši. Postavljanjem ove direktive na `noanonymous` zabranjuje se anonimno prijavljivanje na sustav. Ovu opciju je također moguće postaviti na `noplaintext` koja će zabraniti mehanizme koji koriste zaporke u nekriptiranom obliku (PLAIN i LOGIN).
- `broken_sasl_auth_clients` – ovaj parametar služi za rad s klijentima koji ne podržavaju 'AUTH' naredbu u trenutno definiranom standardu (RFC 2554), već zastarjeli oblik ove naredbe 'AUTH='. Primjeri ovakvih klijenata su Microsoft Outlook Express 4, te Microsoft Exchange 5.
- `smtpd_recipient_restrictions` – ove restrikcije se provjeravaju prilikom primitka svake nove poruke elektroničke pošte kako bi se znalo tko sve može proslijediti pristiglu poruku. Uobičajene opcije su `permit_mynetworks` koja dozvoljava prosljeđivanje svima koji su definirani kroz `mynetworks` direktivu, te `permit_sasl_authenticated` koja dozvoljava prosljeđivanje svima sa bilo koje lokacije koji koriste SMTP autentikaciju.

U ovom primjeru korištene su slijedeće postavke `main.cf` konfiguracijske datoteke *Postfix* poslužitelja:

```
# Opcije potrebne za SASL podršku Postfix poslužitelja
```

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
   permit_sasl_authenticated,
   permit_mynetworks
```

Nakon što su podešene sve opcije, potrebno je ponovno pokrenuti Postfix poslužitelj:

```
# postfix reload
postfix/postfix-script: refreshing the Postfix mail system
```

Moguće je provjeriti da li *Postfix* poslužitelj sada zaista podržava autentikaciju, i kojim mehanizmima:

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 leona.zesoi.fer.hr ESMTP Postfix (Debian/GNU)
EHLO leona
250-leona.zesoi.fer.hr
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
```

Nakon spajanja telnet servisom na TCP port 25 na kojem je pokrenut mail poslužitelj, naredbom 'EHLO' moguće je dobiti listu opcija instaliranog poslužitelja. Ispisom linija koje započinju s 'AUTH' i 'AUTH=' poslužitelj javlja da podržava autentikaciju i to putem samo dva mehanizma, LOGIN i PLAIN. Ovo je stoga što je u `smtpd.conf` datoteci odabran način provjere putem `saslauthd` procesa, a kako on podržava samo ova dva mehanizma, lista podržanih mehanizama je i ograničena samo na njih. Ukoliko direktiva `mech_list` ne bi bila podešena, poslužitelj bi ponudio i MD5 mehanizme autentikacije koji se ne bi mogli izvršiti.

Odabirom `auxprop` metode provjere korisnika, listu mehanizama je moguće proširiti:

```
# smtpd.conf:
pwcheck_method: auxprop
mech_list: plain login cram-md5 digest-md5

...

# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 leona.zesoi.fer.hr ESMTP Postfix (Debian/GNU)
EHLO leona
250-leona.zesoi.fer.hr
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH LOGIN PLAIN CRAM-MD5 DIGEST-MD5
250-AUTH=LOGIN PLAIN CRAM-MD5 DIGEST-MD5
250 8BITMIME
```

Konkretan primjer pokušaja autenticiranja korisnika 'test' sa zaporkom 'zaporka':

```
# perl -MMIME::Base64 -e 'print encode_base64("test\0test\0zaporka");'
a29yaXNuaWsAa29yaXNuaWsAemFwb3JrYQ==
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 leona.zesoi.fer.hr ESMTP Postfix (Debian/GNU)
EHLO leona
```

```
250-leona.zesoi.fer.hr
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
AUTH PLAIN a29yaXNuaWsAa29yaXNuaWsAemFwb3JrYQ==
235 Authentication successful
QUIT
221 Bye
Connection closed by foreign host
```

Prije samog spajanja na mail poslužitelj, obavljeno je pretvaranje znakovnog niza oblika 'korisnik\0korisnik\0zaporka' u base64 kodirani niz. U gornjem primjeru korišten je korisnik s korisničkim imenom 'test' i zaporkom 'zaporka'. Za base64 kodiranje korištena je perl naredba. Odabrani mehanizam autentikacije je PLAIN, te nakon slanja korisničkog imena i zaporke poslužitelj javlja uspješnu autentikaciju porukom '*235 Authentication successful*'.

4. Zaključak

SASL podrška protokolima baziranim na konekcijama omogućuje podizanje razine sigurnosti. Konkretna sigurnosna zaštita ovisi o odabranom mehanizmu autentikacije. Bitno je napomenuti da SASL kao standard samo pruža apstraktni okvir unutar kojeg je moguće vrlo lako uključiti nove i naprednije mehanizme kako oni postaju dostupni. Kroz SASL apstraktni sloj osigurana je sposobnost zajedničkog rada postojećih i tek nadolazećih protokola i mehanizama autentikacije bez ikakvih modifikacija. Mnogi postojeći mehanizmi autentikacije koji su u širokoj upotrebi ne zadovoljavaju neke osnovne sigurnosne zahtjeve, te, iako je moguće odabrati pouzdanije mehanizme, razina sigurnosti će ipak ovisiti o ispravnoj konfiguraciji postojećih servisa i njihove SASL podrške. Ukoliko računalni sustav već posjeduje definiranu i instaliranu autentikacijsku podršku (npr. Kerberos, LDAP), SASL standard omogućuje uključivanje postojeće metode autentikacije za one protokole koje inače ne bi imali mogućnost autentikacije korisnika ovim putem. Za dodatno podizanje razine sigurnosti preporučljivo je i korištenje drugih sigurnosnih slojeva i protokola, pri čemu se TLS/SSL podrška nameće kao kvalitetno i jednostavno rješenje.

5. Reference

[1] SASL RFC, http://www.ietf.org/rfc/rfc2222.txt
[2] SMTP RFC http://www.ietf.org/rfc/rfc0821.txt
[3] SMTP Service Extension for Authentication RFC http://www.ietf.org/rfc/rfc2554.txt
[4] Postfix SMTP Authentication http://www.thecabal.org/~devin/postfix/smtp-auth.txt