AAA u IMS i LTE sustavima

Pejić, Josip

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE,RAČUNARSTVA I

INFORMACIJSKIH TEHNOLOGIJA

Stručni studij

AAA u IMS i LTE sustavima

Završni rad

Josip Pejić

Osijek, 2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1S: Obrazac za ocjenu završnog rada na stručnom prijediplomskom studiju

Ocjena završnog rada na stručnom prijediplomskom studiju

Ime i prezime pristupnika:	Josip Pejić
Studij, smjer:	Stručni prijediplomski studij Računarstvo
Mat. br. pristupnika, god.	AR 4746, 19.07.2019.
JMBAG:	0165080472
Mentor:	mr. sc. Anđelko Lišnjić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	prof. dr. sc. Krešimir Grgić
Član Povjerenstva 1:	mr. sc. Anđelko Lišnjić
Član Povjerenstva 2:	izv. prof. dr. sc. Višnja Križanović
Naslov završnog rada:	%naziv_rada%
Znanstvena grana završnog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada:	AAA (Authentication Authorizationand Accounting) poslužitelj koji se koristi u telekomunikacijskim sustavima pruža pristup, kontrolu i sigurnost za mreže operatera podržavajući skup protokola koji posreduju i prate pristup korisnika provjeravanjem autentičnosti, autorizacijom i obračunom aktivnosti fiksnih i mobilnih korisnika. Zadatak je obraditi protokole koji se koriste u AAA poslužiteljima s posebnim naglaskom na sigurnosni aspekt cjelokupne komunikacije, i ako je moguće snimiti signalizaciju jednog u od tih protokola u realnom okruženju. Tema rezervirana za: Josip Pejić
Datum ocjene pismenog dijela završnog rada od strane mentora:	24.06.2024.
Ocjena pismenog dijela završnog rada od strane mentora:	Izvrstan (5)
Datum obrane završnog rada:	04.07.224.
Ocjena usmenog dijela završnog rada (obrane):	Izvrstan (5)
Ukupna ocjena završnog rada:	Izvrstan (5)
Datum potvrde mentora o predaji konačne verzije završnog rada čime je pristupnik završio stručni prijediplomski studij:	04.07.2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O IZVORNOSTI RADA

Osijek, 04.07.2024.

Ime i prezime Pristupnika:	Josip Pejić
Studij:	Stručni prijediplomski studij Računarstvo
Mat. br. Pristupnika, godina upisa:	AR 4746, 19.07.2019.
Turnitin podudaranje [%]:	5

Ovom izjavom izjavljujem da je rad pod nazivom**: AAA u IMS i LTE sustavima**

izrađen pod vodstvom mentora mr. sc. Anđelko Lišnjić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis pristupnika:

SADRŽAJ

1. UVOD

Brzo širenje telekomunikacijskih sustava povećalo je potražnju za robusnom kontrolom pristupa i sigurnosnim mehanizmima za zaštitu mreža operatera. Poslužitelji za autentikaciju, autorizaciju i administraciju (AAA) igraju ključnu ulogu u ovom kontekstu pružajući kontrolu pristupa, autentikaciju korisnika i funkcionalnost računovodstva. Ovi poslužitelji koriste skup protokola za posredovanje i nadzor korisničkog pristupa, osiguravajući integritet i sigurnost komunikacijskog procesa. Primarna funkcija AAA poslužitelja u telekomunikacijskim sustavima je autentikacija, autorizacija i obračun aktivnosti fiksnih i mobilnih korisnika. Autentikacija uključuje provjeru identiteta korisnika koji se pokušavaju spojiti na mrežu, osiguravajući da samo ovlašteni korisnici imaju pristup. Nasuprot tome, autorizacija se bavi dodjeljivanjem ili uskraćivanjem privilegija pristupa autentificiranim korisnicima na temelju unaprijed definiranih pravila kontrole pristupa. Naposljetku, administracija uključuje praćenje i bilježenje aktivnosti korisnika kako bi se olakšala naplata, revizija i nadzor mreže.

Protokoli koji se koriste u AAA poslužiteljima nisu imuni na sigurnosne prijetnje. Zlonamjerni akteri neprestano traže ranjivosti kako bi iskoristili i stekli neovlašteni pristup osjetljivim mrežnim resursima. Kao rezultat toga, ključno je obraditi ove protokole s fokusom na ukupnu sigurnost komunikacije.

Učinkovite protumjere za ublažavanje rizika i ranjivosti postižu se proučavanjem sigurnosnih izazova s kojima se suočavaju AAA poslužitelji, što je usko povezano s industrijskim standardima i najboljom praksom osiguranja AAA poslužitelja i uspješnom implementacijom sigurnosnih mjera u stvarnim scenarijima.

Kako bi se postigao ovaj cilj, obradit će se glavne komponente AAA poslužitelja, kao što su autentikacija, autorizacija i administracija, kao i protokole koji se obično koriste. Procijenit će se sigurnosne implikacije ovih protokola i navesti prednosti i nedostatke različitih metoda provjere autentičnosti, mehanizama kontrole pristupa i procesa obračuna podataka.

Cilj ovog rada je analizirati protokole koji se koriste u AAA poslužiteljima, s posebnim naglaskom na sigurnosni aspekt cjelokupnog komunikacijskog procesa i istražiti autentikaciju, autorizaciju i računovodstvene komponente AAA poslužitelja te procijeniti njihovu učinkovitost u osiguravanju kontrole pristupa mreži i zaštite od potencijalnih ranjivosti i prijetnji. Rad nastoji pružiti uvide i preporuke za poboljšanje sigurnosnih mjera

implementiranih u AAA poslužiteljima za zaštitu telekomunikacijskih sustava i korisničkih podataka.

2. KARAKTERISTIKE AAA POSLUŽITELJA

Poslužitelji za autentikaciju, autorizaciju i administraciju (AAA) kritične su komponente u telekomunikacijskim sustavima, pružajući mrežama operatera kontrolu pristupa i sigurnosne mjere.

AAA (*Authentication, Authorization, and Accounting*) poslužitelji djeluju kao centralizirana točka kontrole za mrežni korisnički pristup, provjeru identiteta korisnika, dodjelu ili uskraćivanje privilegija pristupa i praćenje aktivnosti korisnika. AAA poslužitelji sastoje se od tri glavne komponente [1]:

Komponenta autentikacije je zadužena za provjeru identiteta korisnika koji se pokušavaju spojiti na mrežu. Koristi se nekoliko metoda provjere autentičnosti, uključujući provjeru autentičnosti na temelju lozinke, provjeru autentičnosti na temelju certifikata i biometrijsku provjeru autentičnosti. S aspekta sigurnosti i upotrebljivosti, svaka metoda ima prednosti i nedostatke.

Provjera autentičnosti temeljena na lozinci zahtijeva od korisnika unos lozinke koja se uspoređuje s lozinkom pohranjenom u sigurnoj bazi podataka. Međutim, ova je metoda ranjiva na napade kao što je nasumično pogađanje lozinke. Da bi se riješili ti nedostaci, mogu se koristiti tehnike kao što je hash-iranje za poboljšanje sigurnosti lozinke.

Digitalni certifikati koje su izdala pouzdana tijela koriste se u autentikaciji temeljenoj na certifikatima. Ova metoda pruža veću sigurnost potvrđivanjem autentičnosti certifikata i osiguravanjem sigurne komunikacije između klijenta i poslužitelja. Uloga infrastrukture javnih ključeva (PKI *Public Key Infrastructure*) u implementaciji autentikacije temeljene na certifikatima je jako bitna iz razloga što pruža sigurnosnu infrastrukturu koja je neophodna za pouzdanu autentikaciju, zaštitu podataka i upravljanje identitetima u digitalnom svijetu.

Poboljšanu sigurnost pridonosi i biometrijska provjera autentičnosti koja se izvršava na terminalu koristeći jedinstvene fiziološke ili bihevioralne karakteristike pojedinca, kao što su otisci prstiju, uzorci šarenice ili prepoznavanje glasa. Budući da je biometrijske značajke teško krivotvoriti, ova metoda pridonosi većoj razini sigurnosti. Međutim, izazovi kao što su točnost, skalabilnost i problemi privatnosti moraju se pažljivo riješiti u implementaciji biometrijske autentikacije.

Nakon provjere identiteta korisnika u sustavu, autorizacijska komponenta određuje privilegije pristupa na temelju unaprijed definiranih politika i pravila kontrole pristupa. Kontrola pristupa temeljena na ulogama (RBAC - *Role based access control*) obično se koristi u AAA poslužiteljima, dopuštajući dodjelu prava pristupa na temelju uloge korisnika unutar organizacije.

Kategorizirajući korisnike u uloge i definirajući dopuštenja povezana sa svakom ulogom, RBAC pruža fleksibilan i skalabilan pristup kontroli pristupa. Ovo pojednostavljuje upravljanje korisničkim pravima pristupa i osigurava da korisnici imaju odgovarajuće privilegije na temelju njihovih odgovornosti. Međutim, kako bi se izbjegli problemi poput stvaranja previše uloga i složenosti hijerarhije uloga, implementacija RBAC-a zahtijeva pažljiv dizajn i administraciju.

Provedba politika kontrole pristupa još je jedan aspekt autorizacije u AAA poslužiteljima. Za definiranje i provedbu ovih pravila često se koriste popisi kontrole pristupa (ACL - *Access Control List*) i kontrola pristupa temeljena na atributima (ABAC - *Attribute-Based Access Control*). ACL-ovi definiraju dopuštenja dodijeljena određenim korisnicima ili grupama, dok ABAC temelji odluke o kontroli pristupa na atributima povezanim s korisnicima i resursima [1].

Administracija igra ključnu ulogu u osiguravanju odgovornosti i omogućavanju pravilne raspodjele resursa unutar telekomunikacijskog sustava. Prikupljanjem i analizom računovodstvenih podataka, operateri mogu točno naplatiti korisnicima na temelju njihove upotrebe usluge, nadzirati mrežni promet i performanse te identificirati sve neuobičajene ili sumnjive aktivnosti koje mogu ukazivati na sigurnosne propuste ili kršenje pravila.

Računovodstveni podaci obično uključuju informacije kao što su vrijeme početka i završetka sesije, količine prijenosa podataka, korištene mrežne usluge i druge relevantne metrike. Ove podatke prikuplja i pohranjuje AAA poslužitelj, omogućujući operaterima generiranje izvješća o korištenju, analizu obrazaca ponašanja korisnika i donošenje utemeljenih odluka u vezi s upravljanjem resursima i optimizacijom mreže.

Računovodstvena komponenta AAA poslužitelja oslanja se na specijalizirane protokole, kao što su RADIUS (*Remote Authentication Dial-In User Service*) i Diameter, kako bi se olakšalo prikupljanje, prijenos i pohranjivanje računovodstvenih podataka. Ovi protokoli osiguravaju sigurnu razmjenu računovodstvenih informacija između mrežnih elemenata i AAA poslužitelja.

Implementacijom robusnih računovodstvenih mehanizama, AAA poslužitelji omogućuju telekomunikacijskim operaterima da održavaju točnu evidenciju naplate, poštuju regulatorne zahtjeve, otkriju i istraže potencijalnu zlouporabu mrežnih resursa i analiziraju obrasce korištenja za planiranje kapaciteta i poboljšanje usluge. Povećava ukupnu odgovornost i transparentnost mreže, pridonoseći učinkovitom radu i upravljanju telekomunikacijskim sustavima [1].

3. PROTOKOLI PROVJERE AUTENTIČNOSTI U AAA POSLUŽITELJIMA

AAA poslužitelji oslanjaju se na protokole provjere autentičnosti kako bi osigurali sigurnu provjeru identiteta korisnika u telekomunikacijskim sustavima koristeći razne vrste autentikacije kao što su autentikacija temeljena na lozinci, temeljena na certifikatu i biometrijska autentikacija.

3.1. Autentikacija temeljena na lozinci

Jedna je od najčešće korištenih metoda na AAA poslužiteljima je autentikacija temeljena na lozinci. Tijekom procesa autentikacije, korisnici daju lozinku, koja se zatim uspoređuje s lozinkom pohranjenom u sigurnoj bazi podataka. Snaga provjere autentičnosti temeljene na lozinci leži u njezinoj lakoći korištenja i jednostavnosti. Međutim, ima nekoliko nedostataka. Lozinke se mogu lako pogoditi ili probiti napadima brutalnom silom ili iskorištavanjem loših izbora lozinki. Korisnici često ponovno koriste lozinke na više računa, povećavajući vjerojatnost ugrožavanja vjerodajnica.

Može se primijeniti nekoliko mjera za poboljšanje sigurnosti provjere autentičnosti temeljene na lozinci. Provođenje pravila o jakim lozinkama može znatno poboljšati sigurnost. To uključuje zahtjeve za složenim lozinkama s velikim i malim slovima, brojevima i posebnim znakovima. Implementacija isteka lozinke, zaključavanja računa nakon višestrukih neuspjelih pokušaja prijave i dvofaktorske provjere autentičnosti (koja zahtijeva dodatni faktor provjere kao što je jednokratna lozinka) može poboljšati ukupnu sigurnost provjere autentičnosti temeljene na lozinci [2].

3.2. Autentikacija temeljena na certifikatima

Digitalni certifikati koje su izdala ovlaštena tijela za izdavanje certifikata koriste se u autentikaciji temeljenoj na certifikatima. Ovi certifikati, koji sadrže javni ključ korisnika, koriste se za uspostavljanje sigurnog komunikacijskog kanala između klijenta i AAA poslužitelja. Provjera autentičnosti temeljena na certifikatu sigurnija je od provjere

autentičnosti temeljene na lozinci jer potvrđuje autentičnost certifikata i omogućuje šifriranu komunikaciju.

Klijent tijekom autentikacije prezentira svoj digitalni certifikat AAA poslužitelju koji provjerava njegovu autentičnost provjerom njegove valjanosti, vjerodostojnosti CA-a i digitalnog potpisa. Za upravljanje izdavanjem, distribucijom i opozivom digitalnih certifikata obično se koristi infrastruktura javnih ključeva (PKI).

Budući da je otporna na pogađanje zaporke i krađu, provjera autentičnosti temeljena na certifikatu pruža jaku sigurnost. Međutim, potrebne su odgovarajuće prakse upravljanja ključevima, kao što je sigurna pohrana privatnih ključeva i upotreba jakih algoritama šifriranja [3].

3.3. Biometrijska autentikacija

Biometrijska autentikacija nije sastavni dio AAA ali pomaže povećanju sigurnosti. Koristi jedinstvene fiziološke ili bihevioralne karakteristike pojedinaca za provjeru njihovog identiteta, kao što su otisci prstiju, uzorci šarenice, prepoznavanje glasa ili crte lica. Budući da je te karakteristike teško krivotvoriti ili replicirati, biometrija pruža visoku razinu sigurnosti.

Biometrijski podaci se bilježe tijekom autentikacije i uspoređuju s prethodno upisanim predlošcima pohranjenim u bazi podataka AAA poslužitelja. Autentikacija je uspješna ako se biometrijske značajke podudaraju. Korisnici imaju koristi od biometrijske provjere autentičnosti jer ne moraju pamtiti lozinke niti nositi fizičke tokene.

Biometrijski podaci smatraju se podacima koji otkrivaju identitet (PII - *Personally Identifiable Information*) i s njima se mora pažljivo rukovati kako bi se osigurala privatnost. Kako bi se spriječio neovlašteni pristup, biometrijske podatke treba pohranjivati i prenositi pomoću jake enkripcije. Lažni napadi, u kojima protivnik predstavlja umjetne ili izmijenjene biometrijske uzorke kako bi prevario sustav, još su jedna potencijalna ranjivost biometrijskih sustava. Tehnike za otkrivanje živosti, kao što je potvrda da je prezentirani biometrijski uzorak od žive osobe, mogu pomoći u smanjenju rizika lažiranja [4].

Nekoliko sigurnosnih mjera i najboljih praksi može se koristiti za poboljšanje cjelokupnog procesa autentikacije u AAA poslužiteljima [5]:

- *Multi-Factor Authentication* (MFA): Koristeći MFA, može se značajno ojačati proces autentikacije kombiniranjem više faktora autentikacije, kao što je nešto što korisnik zna (lozinka), nešto što korisnik ima (pametna kartica) ili nešto što korisnik jest (biometrija).
- Mehanizmi kontinuiranog nadzora omogućuju otkrivanje sumnjivih aktivnosti i potencijalnih sigurnosnih proboja. Anomalije u ponašanju korisnika ili neobični obrasci pristupa mogu uzrokovati slanje upozorenja na daljnju istragu.
- Jaka enkripcija: Korištenje jakih algoritama šifriranja za prijenos i pohranu osjetljivih podataka, kao što su lozinke i biometrijske informacije, štiti od neovlaštenog pristupa i povrede podataka.
- Redovita revizija i praćenje sigurnosnih sustava: Provođenje redovitih revizija i vođenje detaljnih dnevnika događaja provjere autentičnosti omogućuje otkrivanje bilo kakvih pokušaja neovlaštenog pristupa ili sumnjivih aktivnosti. Ovi se zapisnici mogu koristiti kao pomoć u forenzičkim analizama i istragama.

Protokoli provjere autentičnosti AAA poslužitelja ključni su za osiguranje sigurne verifikacije korisnika i kontrole pristupa u telekomunikacijskim sustavima. Metode provjere autentičnosti temeljene na lozinci, certifikatima i biometrijske provjere autentičnosti imaju prednosti i nedostatke. Proces autentikacije u AAA poslužiteljima može se poboljšati implementacijom odgovarajućih sigurnosnih mjera i najboljih praksi, pridonoseći ukupnoj sigurnosti telekomunikacijskih sustava.

4. AUTORIZACIJSKI PROTOKOLI U AAA POSLUŽITELJIMA

Protokoli za autorizaciju ključni su u AAA (*Authentication, Authorization, and Accounting*) poslužiteljima jer osiguravaju da korisnici imaju odgovarajuće privilegije pristupa resursima unutar telekomunikacijskog sustava. U nastavku će se pružiti detaljno objašnjenje protokola autorizacije koji se obično koriste u AAA poslužiteljima, s posebnim naglaskom na sigurnosna razmatranja autorizacije. Također objasniti će se mehanizmi i politike kontrole pristupa AAA poslužitelju, važnosti kontrole pristupa temeljene na ulogama (RBAC) i sigurnosnim mjerama i preporukama za poboljšanje autorizacije u AAA poslužiteljima.

4.1. Protokoli autorizacije u AAA poslužiteljima

AAA poslužitelji koriste različite protokole autorizacije za provedbu kontrole pristupa i utvrđivanje ima li korisnik pristup određenim resursima ili ne. Ti protokoli su [6]:

- RADIUS : AAA protokol za autentikaciju i autorizaciju mrežnog pristupa. Omogućuje udaljenim korisnicima sigurno povezivanje s mrežom omogućavanjem centralizirane provjere autentičnosti i autorizacije. Podržava različite mehanizme autorizacije, uključujući politike pristupa temeljene na korisničkim atributima kao što su korisničko ime, lozinka i korisničke uloge dodijeljene korisnicima.
- Diameter: Diameter je poboljšani nasljednik RADIUS-a koji je namijenjen prevladavanju ograničenja (skalabilnost, sigurnost, fleksibilnost i proširivost, pouzdanost i otkrivanje grešaka, podrška za kompleksne politike pristupa) uz poboljšanje sigurnosti i fleksibilnosti. To je proširivi AAA protokol koji se koristi u raznim scenarijima pristupa mreži, uključujući 3G/4G/5G mreže. Diameter uključuje poboljšane sigurnosne značajke kao što je zaštita integriteta poruke i podrška za robusnije metode provjere autentičnosti kao što su digitalni certifikati.

4.2. Sigurnosna razmatranja u autorizaciji

Kako bi se osigurao integritet i povjerljivost resursa, autorizacija AAA poslužitelja mora riješiti nekoliko sigurnosnih problema. Ti problemi su [5]:

- AAA poslužitelji koriste politike kontrole pristupa za definiranje pravila i uvjeta za odobravanje ili zabranjivanje pristupa na temelju korisničkih atributa, svojstava resursa i zahtjeva specifičnih za sustav. Ove politike trebaju biti dobro definirane, redovito pregledavane i usklađene sa sigurnosnim zahtjevima.
- Načelo najmanjih privilegija: Načelo najmanjih privilegija kaže da se korisnicima trebaju dodijeliti samo one privilegije koje su potrebne za dovršavanje njihovih zadataka. Ograničavanjem pristupa resursima uvelike se smanjuje potencijalni utjecaj neovlaštenog pristupa ili eskalacije privilegija.
- Raspodjela dužnosti: Zahtijevanjem višestrukih uloga ili odobrenja za kritične zadatke, jedan korisnik je spriječen da ima potpunu kontrolu nad osjetljivim operacijama. Ovo načelo pomaže smanjiti rizik od neovlaštenih radnji i zlouporabe privilegija.

4.3. Mehanizmi i pravila kontrole pristupa

Za kontrolu korisničkog pristupa resursima, AAA poslužitelji koriste različite mehanizme i pravila za kontrolu pristupa [1]:

- Diskrecijska kontrola pristupa (DAC): DAC omogućuje vlasnicima resursa da kontroliraju tko ima pristup njihovim resursima. DAC, s druge strane, može uzrokovati nedosljednosti i nedostaje mu centralizirana kontrola, što ga čini neprikladnim za velike sustave.
- Obavezna kontrola pristupa (MAC): MAC provodi dopuštenja pristupa na temelju sigurnosnih oznaka i pravila koja su unaprijed definirana. Ovaj model pruža veću sigurnost, ali zahtijeva pažljivo definiranje i upravljanje sigurnosnim oznakama i politikama.
- RBAC: RBAC je popularan model kontrole pristupa u AAA poslužiteljima. Povezuje korisničke uloge s odgovarajućim dopuštenjima pristupa. RBAC olakšava načelo najmanje privilegije pojednostavljivanjem administracije i pružanjem detaljne kontrole.

4.4. Kontrola pristupa temeljena na ulogama (RBAC)

RBAC je model kontrole pristupa koji je primjenjiv na AAA poslužitelje. Olakšava upravljanje pristupom povezivanjem dopuštenja pristupa s unaprijed definiranim ulogama i dodjeljivanjem korisnika tim ulogama. RBAC uključuje sljedeće komponente [7]:

- Uloge: Unutar organizacije uloge predstavljaju radne funkcije, odgovornosti ili nazive poslova. Za primjer to mogu biti "upravitelj", "administrator" i "zaposlenik".
- Ovlasti: definiraju akcije ili operacije koje korisnici mogu izvršiti na resursima. Povezani su s određenim ulogama i kontroliraju razinu dodijeljenog pristupa.
- Dodjela uloga: dodjeljuje korisnicima određene uloge, definirajući njihove privilegije pristupa sustavu.

RBAC pruža nekoliko prednosti, uključujući povećanu sigurnost, smanjene administrativne troškove i lakšu usklađenost s politikama kontrole pristupa. Implementacija RBAC-a, s druge strane, zahtijeva pažljivo planiranje i razmatranje strukture organizacije i zahtjeva za pristup.

Organizacije mogu primijeniti sigurnosne mjere i preporuke za poboljšanje procesa autorizacije u AAA poslužiteljima, a te mjere su [1]:

- Redovito pregledavanje i ažuriranje politike kontrole pristupa kako bi bili sigurni da su u skladu s trenutnim zahtjevima sigurnosti sustava.
- Snažni sustavi autentikacije: implementiranje robusnih mehanizama provjere autentičnosti, kao što je autentikacija s više faktora, kako bi se osiguralo da samo ovlašteni korisnici imaju pristup sustavu.
- Praćenje i nadzor: omogućivanje praćenja aktivnosti i nadzor za praćenje i otkrivanje pokušaja neovlaštenog pristupa, kršenja pravila i potencijalnih sigurnosnih proboja. Redovito pregledavanje zapisa radi uočavanja anomalija ili sumnjivih aktivnosti.
- Promjena ovlasti: implementiranje mehanizama za opozivanje privilegija pristupa kada više nisu potrebne ili kada se promijeni uloga korisnika unutar organizacije.

Autorizacijski protokoli u AAA poslužiteljima ključni su za kontrolu pristupa korisnika resursima u telekomunikacijskim sustavima. Organizacije mogu poboljšati sigurnost svojih AAA poslužitelja i osigurati da korisnici imaju odgovarajuću razinu privilegija pristupa implementacijom odgovarajućih mehanizama kontrole pristupa, politika i kontrole pristupa temeljene na ulogama.

5. ADMINISTRATIVNI PROTOKOLI UNUTAR AAA POSLUŽITELJA

AAA poslužitelj ključna je komponenta mrežne infrastrukture odgovorna za upravljanje korisničkim pristupom i aktivnostima [8].

RADIUS je široko korišten protokol za upravljanje mrežnim pristupom. Omogućuje centralizirano upravljanje autentikacijom, autorizacijom i administracijom za korisnike koji se povezuju i koriste mrežnu uslugu. Funkcije administriranja koje RADIUS protokol omogućuje su prikupljanje, praćenje i bilježenje korisničkih aktivnosti kao što su prijave, odjave, količine prijenosa podataka i trajanje sesija.

Usluga udaljene provjere autentičnosti biranjem (RADIUS) mrežni je protokol koji pruža centralizirano upravljanje autentikacijom, autorizacijom i obračunom (AAA) za korisnike koji se povezuju i koriste mrežne usluge. Obično se koristi u scenarijima gdje je potreban daljinski pristup mreži, kao što su dial-up veze, virtualne privatne mreže (VPN) i bežične mreže.

RADIUS upravlja autentikacijom korisnika provjerom korisničkih vjerodajnica u odnosu na centraliziranu bazu podataka, koja se nalazi na RADIUS poslužitelju. Ova centralizacija omogućuje jedinstvenu autentikaciju preko višestrukih pristupnih točaka i uređaja unutar mreže.

Nakon uspješne autentikacije, RADIUS određuje razinu pristupa koja je korisniku dopuštena na temelju unaprijed definiranih pravila i konfiguracija. To uključuje određivanje kojim resursima korisnik može pristupiti i koje radnje može izvesti.

RADIUS također prikuplja i bilježi informacije o aktivnostima korisnika, kao što su prijave, odjave, količine prijenosa podataka i trajanje sesije. Ovi računovodstveni podaci vrijedni su za reviziju, naplatu i praćenje upotrebe mreže i performansi.

On je dizajniran za učinkovito skaliranje za podršku velikom broju korisnika i mrežnih uređaja. To ga čini prikladnim za implementaciju u poslovnim okruženjima i okruženjima pružatelja usluga.

RADIUS uključuje različite sigurnosne mehanizme za zaštitu korisničkih vjerodajnica i osjetljivih podataka tijekom autentikacije i komunikacije između RADIUS klijenata i

poslužitelja. Ovi mehanizmi uključuju enkripciju, provjere integriteta poruka i podršku za snažne metode provjere autentičnosti.

RADIUS je široko prihvaćeni standardni protokol kojeg podržava širok raspon mrežne opreme i softverskih platformi. Ova interoperabilnost omogućuje RADIUS klijentima (kao što su poslužitelji za mrežni pristup) da neprimjetno komuniciraju s različitim RADIUS poslužiteljima, bez obzira na dobavljača ili implementaciju.

Širok spektar obilježja koje podržava RADIUS omogućuje organizacijama da prilagode njegovu implementacije svojim specifičnim zahtjevima i integriraju se s drugim sustavima i uslugama.

RADIUS je iznimno važan u osiguravanju sigurnosti, pouzdanosti i upravljivosti pristupa mreži u različitim okruženjima centraliziranjem funkcija provjere autentičnosti, autorizacije i računovodstva.

TACACS+ (*Terminal Access Controller Access Control System Plus*) je još jedan protokol koji se koristi za AAA usluge. Slično RADIUS-u, pruža usluge provjere autentičnosti, autorizacije i administracije. TACACS+ razdvaja autentikaciju, autorizaciju i administraciju u različite procese, nudeći veću fleksibilnost i granularnost u kontroli pristupa i administraciji u usporedbi s RADIUS-om.

Poput RADIUS-a, TACACS+ pruža okvir za kontrolu pristupa mrežnim resursima i upravljanje korisničkim aktivnostima. Međutim, postoje neke razlike između TACACS+ i RADIUS-a a one su sljedeće [9]:

- Razdvajanje usluga: TACACS+ razdvaja autentikaciju, autorizaciju i administraciju u različite procese, dok RADIUS kombinira ove funkcije u jedan protokol. Ovo odvajanje nudi veću fleksibilnost i preciznost u kontroli pristupa i računovodstvu.

- Enkripcija: TACACS+ šifrira cijelo tijelo paketa, uključujući zaglavlje, pružajući poboljšanu sigurnost u usporedbi s RADIUS-om, koji obično šifrira samo dio paketa za provjeru autentičnosti koji sadrži lozinku.

- Autorizacija naredbi: TACACS+ podržava autorizaciju naredbi, dopuštajući administratorima da kontroliraju koje naredbe korisnici smiju izvršavati na mrežnim uređajima. Ova precizna kontrola korisna je u okruženjima gdje je potrebna stroga kontrola pristupa na razini naredbi.

- Podrška za IPv6: TACACS+ ima ugrađenu podršku za IPv6, što ga čini prikladnim za moderna mrežna okruženja gdje je usvajanje IPv6 u porastu. RADIUS, s druge strane, ima ograničenu podršku za IPv6 i često zahtijeva dodatna proširenja ili rješenja kako bi pravilno funkcionirao u IPv6 mrežama.

- Podrška dobavljača: Dok je RADIUS šire prihvaćen i podržan u širem rasponu mrežne opreme i softverskih platformi, TACACS+ je prvenstveno povezan s Cisco mrežnim uređajima. Međutim, dostupne su implementacije TACACS+ treće strane i može se koristiti u heterogenim mrežnim okruženjima uz odgovarajuću konfiguraciju i integraciju.

TACACS+ se obično koristi u poslovnim okruženjima, posebno onima s fokusom na upravljanje i sigurnost mrežnih uređaja. Njegova podrška za autorizaciju na razini naredbi i enkripciju čine ga prikladnim za kontrolu administrativnog pristupa mrežnim uređajima i provođenje sigurnosnih pravila. Međutim, zbog njegove složenije implementacije i uže podrške dobavljača u usporedbi s RADIUS-om, organizacije mogu birati između TACACS+ i RADIUS-a na temelju svojih specifičnih zahtjeva i postojeće infrastrukture [9].

DIAMETER: Diameter je razvijena verzija RADIUS-a i dizajniran je za rješavanje nekih ograničenja RADIUS-a, posebno u pogledu skalabilnosti i sigurnosti. Kao i RADIUS, Diameter podržava autentikaciju, autorizaciju i računovodstvene funkcije. Koristi se u raznim mrežnim tehnologijama, uključujući 3G, LTE i 5G.

DIAMETER je protokol koji se prvenstveno koristi u telekomunikacijama i umrežavanju za usluge autentikacije, autorizacije i računovodstva (AAA), sličan RADIUS-u i TACACS+. Služi

kao evolucija i poboljšanje RADIUS-a, rješavajući neka od njegovih ograničenja, posebice u skalabilnosti, sigurnosti i podršci za moderne mrežne tehnologije. [10]

DIAMETER je dizajniran za učinkovitije skaliranje od RADIUS-a, posebno u velikim, distribuiranim mrežnim okruženjima. Podržava značajke kao što su *peer-to-peer* komunikacija i *proxying*, koje omogućuju bolju raspodjelu opterećenja i redundanciju, što ga čini prikladnim za implementacije na razini operatera u telekomunikacijskim mrežama.

DIAMETER uključuje značajke za pouzdanu isporuku poruka, uključujući podršku za ponovno slanje poruka, potvrde i rukovanje pogreškama. To osigurava da se AAA poruke pouzdano isporučuju i obrađuju, čak i u prisutnosti mrežnih kvarova ili zagušenja. Nudi poboljšane sigurnosne značajke u usporedbi s RADIUS-om, uključujući podršku za enkripciju *Transport Layer Security* (TLS) i međusobnu autentikaciju između ravnopravnih korisnika. To pomaže u zaštiti osjetljivih korisničkih podataka i vjerodajnica za autentikaciju od prisluškivanja i petljanja, osiguravajući integritet i povjerljivost AAA transakcija.

Dizajniran je da bude prilagodljiv, dopuštajući definiranje novih vrsta poruka, atributa i kodova naredbi za podršku dodatnim funkcionalnostima i aplikacijama. To omogućuje DIAMETER-u da se prilagodi rastućim mrežnim zahtjevima i tehnologijama, što ga čini svestranim protokolom za AAA usluge.

Mobilne i VoIP telekomunikacije koriste ga kao primarni protokol za AAA usluge, uključujući autentikaciju pretplatnika, upravljanje mobilnošću i naplatu.

Slično RADIUS-u, DIAMETER koristi parove atribut-vrijednost (AVP-ovi) za razmjenu informacija između klijenata i poslužitelja. DIAMETER pruža strukturiraniji i proširivi format za AVP-ove, omogućujući bolju interoperabilnost i podršku za složene tipove podataka.

Nudi robusniju, skalabilniju i sigurniju alternativu RADIUS-u za AAA usluge, a posebno u telekomunikacijskim mrežama mobilnih operatera. Njegova podrška modernim mrežnim tehnologijama i naglasak na pouzdanosti i proširivosti čine ga prikladnim za širok raspon primjena u telekomunikacijama, umrežavanju i šire.

Ovi protokoli igraju ključnu ulogu u osiguravanju sigurnosti i odgovornosti mrežnih resursa bilježenjem i nadzorom korisničkih aktivnosti, što se može koristiti za reviziju, naplatu i

sigurnosne svrhe. Specifična implementacija i konfiguracija računovodstvenih protokola unutar AAA poslužitelja može varirati ovisno o mrežnoj infrastrukturi i zahtjevima organizacije.

6. SIGURNOSNI ASPEKTI AAA

Iako su AAA poslužitelji iznimno važni u osiguravanju sigurnosti mrežnih resursa upravljanjem autentikacijom korisnika, autorizacijom i obračunom, oni sami mogu biti ranjivi na razne sigurnosne probleme [11]:

- Neovlašteni pristup: Ako napadač dobije neovlašteni pristup AAA poslužitelju, mogao bi kompromitirati osjetljive korisničke vjerodajnice, pravila kontrole pristupa i računovodstvene podatke. To može rezultirati neovlaštenim pristupom mrežnim resursima, povredom podataka i drugim sigurnosnim incidentima.

- Napadi uskraćivanjem usluge (DoS): AAA poslužitelji su ranjivi na DoS napade, gdje napadač može zatrpati poslužitelj velikim brojem autentikacijskih ili obračunskih zahtjeva, uzrokujući njegov prestanak rada ili rušenje. Ovo može ometati mrežne usluge, uskratiti legitimnim korisnicima pristup resursima i pogoršati ukupne performanse mreže.

- Slabi mehanizmi provjere autentičnosti: Korištenje slabih ili zastarjelih mehanizama provjere autentičnosti, poput lozinki u običnom tekstu ili zastarjelih kriptografskih algoritama, može izložiti korisničke vjerodajnice presretanju i neovlaštenom pristupu. Preporuča se korištenje snažnih metoda provjere autentičnosti, poput višefaktorske autentikacije i autentikacije temeljene na certifikatima, kako bi se smanjio ovaj rizik.

- Krađa vjerodajnica: Ako korisničke vjerodajnice pohranjene na AAA poslužitelju nisu adekvatno zaštićene, mogu biti podložne krađi putem tehnika poput provala u bazu podataka, napada SQL injekcijama ili prijetnji iznutra. Za zaštitu pohranjenih lozinki i drugih osjetljivih podataka treba koristiti jake algoritme šifriranja i raspršivanja.

- Pogrešna konfiguracija: Pogrešne konfiguracije u postavkama AAA poslužitelja, politikama kontrole pristupa ili mrežnoj integraciji mogu stvoriti sigurnosne ranjivosti koje napadači mogu iskoristiti za dobivanje neovlaštenog pristupa ili prekid usluga. Redovite sigurnosne revizije i pregledi konfiguracije potrebni su za identificiranje i rješavanje tih problema.

- Nedovoljno bilježenje i praćenje: Neadekvatno bilježenje i praćenje aktivnosti AAA poslužitelja može otežati otkrivanje sigurnosnih incidenata i pravovremeno reagiranje. Sveobuhvatno bilježenje pokušaja autentikacije, odluka o kontroli pristupa i računovodstvenih podataka ključno je za učinkovito otkrivanje prijetnji i forenzičku analizu.

- Nedostatak upravljanja zakrpama(zakrpa – naknadno ispravljanje postojećeg dijela neispravnog koda koji se otkrio tijekom korištenja): Neuspjeh u pravovremenoj primjeni sigurnosnih zakrpa i ažuriranja na softver AAA poslužitelja može ga učiniti ranjivim na poznate sigurnosne propuste i iskorištavanja. Implementacija redovitih postupaka upravljanja zakrpama osigurava da je poslužiteljski softver uvijek ažuran i siguran.

Rješavanje ovih sigurnosnih problema zahtijeva višeslojni pristup, uključujući implementaciju jakih kontrola pristupa, enkripcije, sustava za otkrivanje upada, redovite sigurnosne procjene i kontinuiranu obuku o sigurnosti za administratore i korisnike. Osim toga, organizacije bi trebale biti informirane o novim prijetnjama i najboljim praksama za osiguranje AAA poslužitelja i drugih ključnih komponenti mrežne infrastrukture.Za rješavanje sigurnosnih problema povezanih s AAA poslužiteljima, organizacije mogu implementirati niz rješenja i najboljih praksi usmjerenih na povećanje sigurnosti njihove AAA infrastrukture.

U nastavku su navedena neka od ključnih rješenja za sigurnosne probleme.

Kontrola pristupa i autentikacija

- Implementirati sigurnije mehanizme provjere autentičnosti, poput višefaktorske autentikacije (MFA) ili autentikacije temeljene na certifikatu, kako bi se smanjio rizik od neovlaštenog pristupa.
- Treba provesti stroge kontrole pristupa kako bi se ograničio administrativni pristup AAA poslužitelju i primijenilo načelo najmanje privilegije.
- Potrebno je koristiti sigurne komunikacijske protokole, poput TLS-a, za šifriranje komunikacije između AAA klijenata i poslužitelja, štiteći osjetljive informacije od presretanja i neovlaštenih izmjena.

Segmentacija mreže i vatrozid

- Segmentirati mrežu kako bi se izolirao AAA poslužitelj od drugih sustava i usluga, smanjujući površinu napada i ograničavajući utjecaj potencijalnih sigurnosnih proboja.
- Treba koristiti vatrozide i sustave za otkrivanje/sprečavanje upada kako bi se nadzirao i kontrolirao promet prema i od AAA poslužitelja, blokirajući pokušaje neovlaštenog pristupa i otkrivajući nenormalno ponašanje.

Sigurna konfiguracija i upravljanje zakrpama

- Slijediti najbolje sigurnosne prakse i preporuke dobavljača prilikom konfiguriranja AAA poslužitelja, osiguravajući promjenu zadanih postavki, onemogućavanje nepotrebnih usluga i pravilnu konfiguraciju kontrola pristupa.
- Potrebno je uspostaviti proces upravljanja zakrpama za redovito ažuriranje softvera AAA poslužitelja i operativnog sustava sigurnosnim zakrpama i ažuriranjima kako bi se rješavale poznate ranjivosti i ublažili potencijalni rizici.

Enkripcija i zaštita podataka

- Koristiti snažne algoritme šifriranja i sigurne mehanizme za pohranu kako bi se zaštitile osjetljive korisničke vjerodajnice i podaci o autentikaciji pohranjeni na AAA poslužitelju, smanjujući rizik od neovlaštenog pristupa i krađe vjerodajnica.
- Provesti mjere za sprječavanje gubitka podataka (DLP) kako bi se pratilo i kontroliralo prijenos osjetljivih informacija na i s AAA poslužitelja, sprječavajući curenje podataka i neovlašteno otkrivanje.

Bilježenje, praćenje i odgovor na incidente

- omogućiti opsežno bilježenje aktivnosti AAA poslužitelja, uključujući pokušaje autentikacije, odluke o kontroli pristupa i računovodstvene podatke, kako bi se olakšalo praćenje u stvarnom vremenu, forenzička analiza i odgovor na incidente.
- Treba implementirati sustave za otkrivanje i sprječavanje upada (IDPS) kako bi se otkrile i blokirale sumnjive aktivnosti i potencijalni sigurnosni proboji, te upozoravalo administratore na poduzimanje odgovarajućih mjera.
- Treba razviti i održavati plan odgovora na incidente koji opisuje postupke za rješavanje sigurnosnih incidenata vezanih uz AAA poslužitelj, uključujući zadržavanje, istragu, sanaciju i komunikaciju sa dionicima.

Redovite sigurnosne procjene sustava i obuka osoblja

- Treba provoditi redovite sigurnosne procjene, skeniranja ranjivosti i testove prodora kako bi se identificirale i ispravile sigurnosne slabosti i pogrešne konfiguracije u infrastrukturi AAA poslužitelja.
- Treba osigurati kontinuiranu obuku o sigurnosti za administratore i korisnike kako bi ih se educiralo o potencijalnim sigurnosnim rizicima, najboljim praksama i sigurnosnim politikama vezanim uz AAA usluge.

Implementacijom ovih rješenja uz uvažavanje iskustava, organizacije mogu poboljšati sigurnost svoje AAA infrastrukture, smanjiti rizik od sigurnosnih proboja i neovlaštenog pristupa te osigurati povjerljivost, integritet i dostupnost mrežnih resursa i korisničkih podataka [11].

7. PRAKTIČNI DIO RADA AAA POKUS

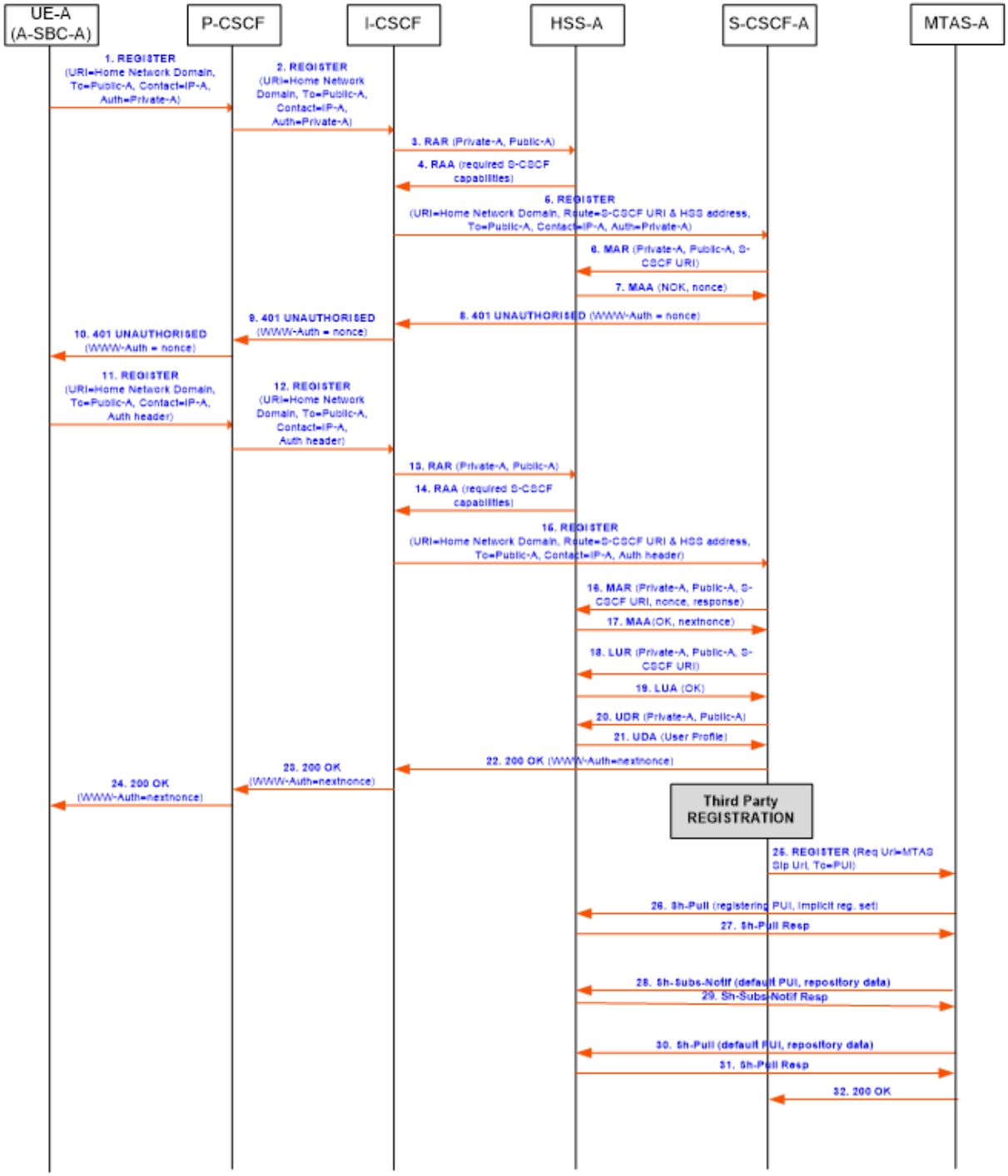
Za potrebe praktičnog dijela rada snimljena je u testnom okruženju jednog telekom operatera programom Wireshark signalizacija registracije i reregistracije korisnika na sustav i jedan uspješno ostvaren poziv. Format snimljene datoteke koja se dalje analizirala je PCAP (*Packet CAPture*).

Kako bi se filtrirao i analizirao cijeli tok prijave i autentikacije unutar PCAP datoteke u Wiresharku, potrebno je pratiti specifične protokole i poruke koje se koriste u procesu autentikacije u IMS i LTE sustavima.

Autentikacija u IMS i LTE sustavima uključuje nekoliko ključnih protokola, uključujući Diameter, SIP(*Session Initiation Protocol*) i EAP (*Extensible Authentication Protocol*).

Razlikuje se SIP registracija i reregistracija. SIP registracija i reregistracija ključni su procesi za uspostavljanje komunikacije u VoIP mrežama.

Registracija je proces kojim se prijavljuje na poslužitelj. Taj proces omogućuje da SIP poslužitelj zna IP adresu uređaja kako bi u daljnjim koracima mogao usmjeravati pozive prema njemu. Na slici 7.1. je prikazan pojednostavljen signalizacijski dijagram SIP registracije [12].



7. 1. Koraci SIP registracije.

SIP registracija se sastoji od sljedećih postupaka:

1. Korisnik A pokreće registraciju s UE-A (*User Equipment A*) koji šalje SIP REGISTER poruku prema mreži. REGISTER uključuje javnu adresu korisnika, privatnu adresu i IP

adresu uređaja. Poruka se šalje na P-CSCF (*Proxy Call Session Control Function*) što označava funkciju za kontrolu poziva proxy preko A-SC (*Application Server*).

2. P-CSCF pohranjuje IP adresu UE-A i dodaje Path header prije nego što proslijedi REGISTER poruku I-CSCF-u (*Interrogating Call Session Control Function*) dodavanjem *route header*-a. Path header sadrži P-CSCF-URI (*Uniform Resource Identifier*) kako bi S-CSCF (*Serving Call Session Control Function*) znao gdje usmjeriti buduće zahtjeve.

3. I-CSCF šalje Cx REGISTRATION AUTHORIZATION REQUEST (Diameter protokol) s privatnom i javnom adresom korisnika HSS-u (*Home Subscriber Server* - domaći pretplatnički poslužitelj).

4. HSS vraća potrebne informacije o S-CSCF i I-CSCF-u.

5. I-CSCF odabire S-CSCF i prosljeđuje REGISTER s relevantnim podacima. S-CSCF pohranjuje sadržaj Path headera i IP adresu UE-A.

6. S-CSCF zahtijeva Authentication Vector (AV - autentifikacijski vektor) od HSS-a za autentifikaciju korisnika.

7. HSS pohranjuje S-CSCF adresu i vraća AV s "nonce" vrijednošću 8-10. S-CSCF šalje 401 UNAUTHORIZED poruku UE-A s WWW-Authenticate headerom koji sadrži "nonce".

8. UE izračunava "response" i šalje novi REGISTER zahtjev s "nonce" vrijednošću natrag P-CSCF-u.

9. P-CSCF prosljeđuje REGISTER poruku I-CSCF-u.

10. I-CSCF šalje Cx REGISTRATION AUTHORIZATION REQUEST HSS-u.

11. HSS vraća S-CSCF URI (*Serving Call Session Control Function - Uniform Resource Identifier*).

12. I-CSCF prosljeđuje REGISTER zahtjev S-CSCF-u.

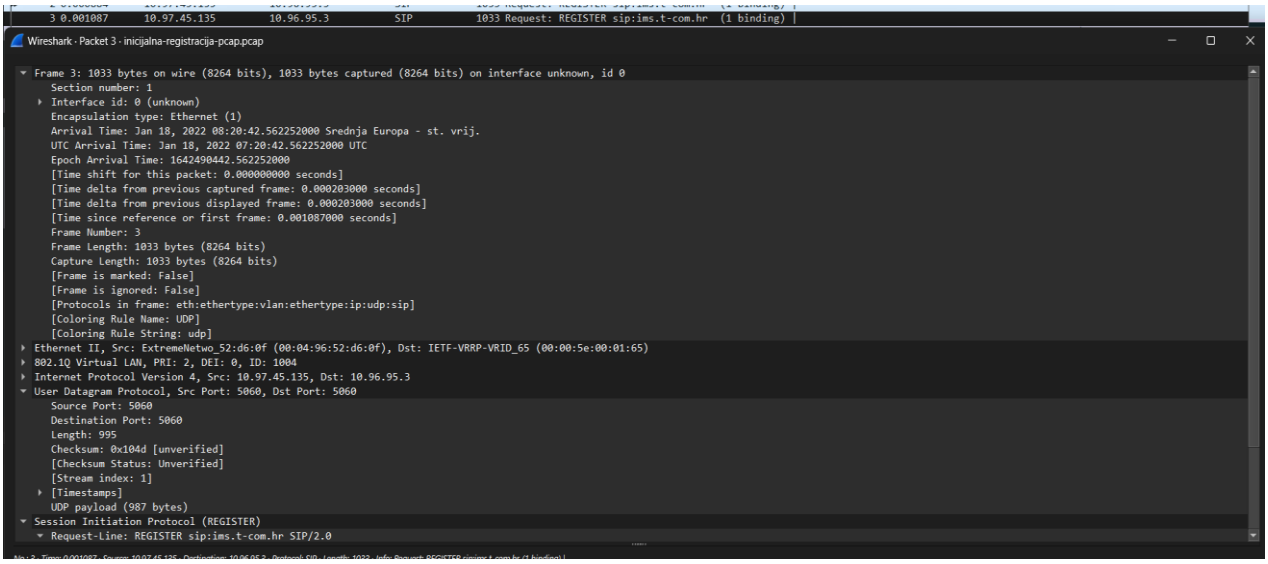
13. S-CSCF prosljeđuje autentifikacijske podatke HSS-u.

14. HSS provjerava “nonce” i “response” te vraća potvrdu i novu “nonce” vrijednost. S-CSCF obavještava HSS (Home Subscriber Server) da je korisnik registriran. S-CSCF dohvaća korisnički profil od HSS-a. S-CSCF šalje 200 OK odgovor P-CSCF-u s “nextnonce” i Service Route headerom.

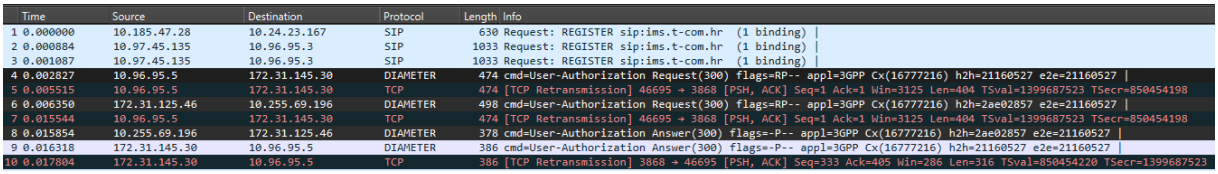
15. P-CSCF pohranjuje Service-Route header i P-Associated-Id te prosljeđuje 200 OK odgovor UE-A.

16. Treća strana registracija se pokreće prema preuzetom korisničkom profilu usluge. MTAS (*Multimedia Telephony Application Server)* - aplikacijski poslužitelj za multimedijsku telefoniju preuzima podatke iz HSS-a. MTAS povlači potrebne podatke koristeći Diameter protokol preko Sh sučelja i šalje 200 OK odgovor na REGISTER zahtjev.

Na slikama 7.2 i 7.3. prikazani su dio stvarno snimljene signalizacije vezane uz registraciju korisnika na sustav i tok registracije snimljeni Wireshark programom.



7. 2. Inicijalni register zahtjev.



7. 3. Tok registracije.

U četvrtom zapisu (*User Authorization Request*) koji je prikazan na slici 7.3. nalaze se parametri:

- User-Authorization Request (UAR) koji označava vrstu zahtjeva. U ovom slučaju, to je zahtjev za autorizaciju korisnika.

- RP--: Flagovi određuju svojstva poruke. RP- označava da je poruka zahtjev (Request).

- 3GPP Cx (16777216) - Oznaka aplikacije je specifična za 3GPP Cx aplikacijski protokol, koji se koristi za IMS (*IP Multimedia Subsystem*).

- Hop-by-Hop Identifier (h2h): 21160527 - Ovaj identifikator koristi se za povezivanje zahtjeva i odgovora koji prolaze kroz više čvorova.

- End-to-End Identifier (e2e): 21160527 - Ovaj identifikator je jedinstven za cijelu sesiju i koristi se za praćenje poruke od početka do kraja.

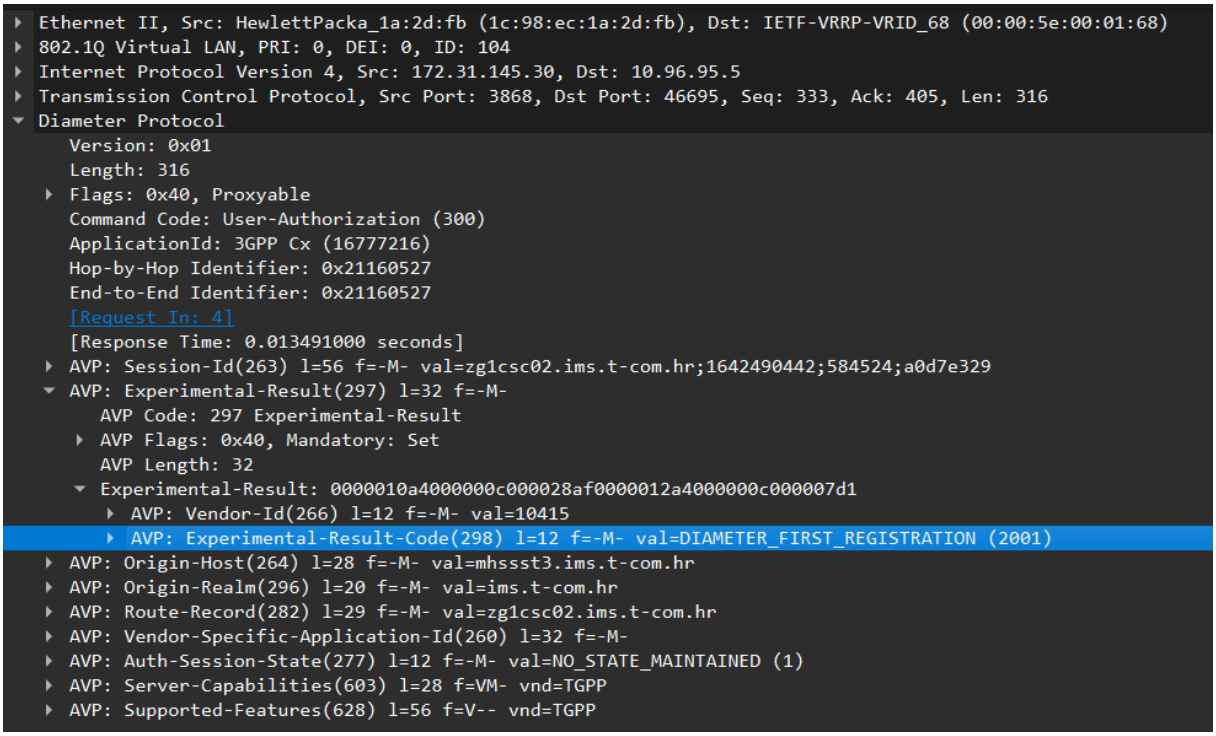
U šestom zapisu na istoj slici pod nazivom *User-Authorization Answer* (UAA) nalaze se bitne informacije poput:

- Vrsta poruke (cmd): cmd=User-Authorization Answer (300) - označava da je poruka odgovor na prethodni zahtjev za autorizaciju korisnika (*User-Authorization Request*).

- -P--: Flagovi određuju svojstva poruke. U ovom slučaju, bit P označava da je ovo odgovor (Answer).

- Application ID (appl): 3GPP Cx (16777216) - Oznaka aplikacije je specifična za 3GPP Cx aplikacijski protokol, koji se koristi za IMS.

Daljom analizom retka 6 sa slike 7.3. mogu se očitati detaljni podaci o DIAMETAR protokolu što je prikazana na Slici 7.4.



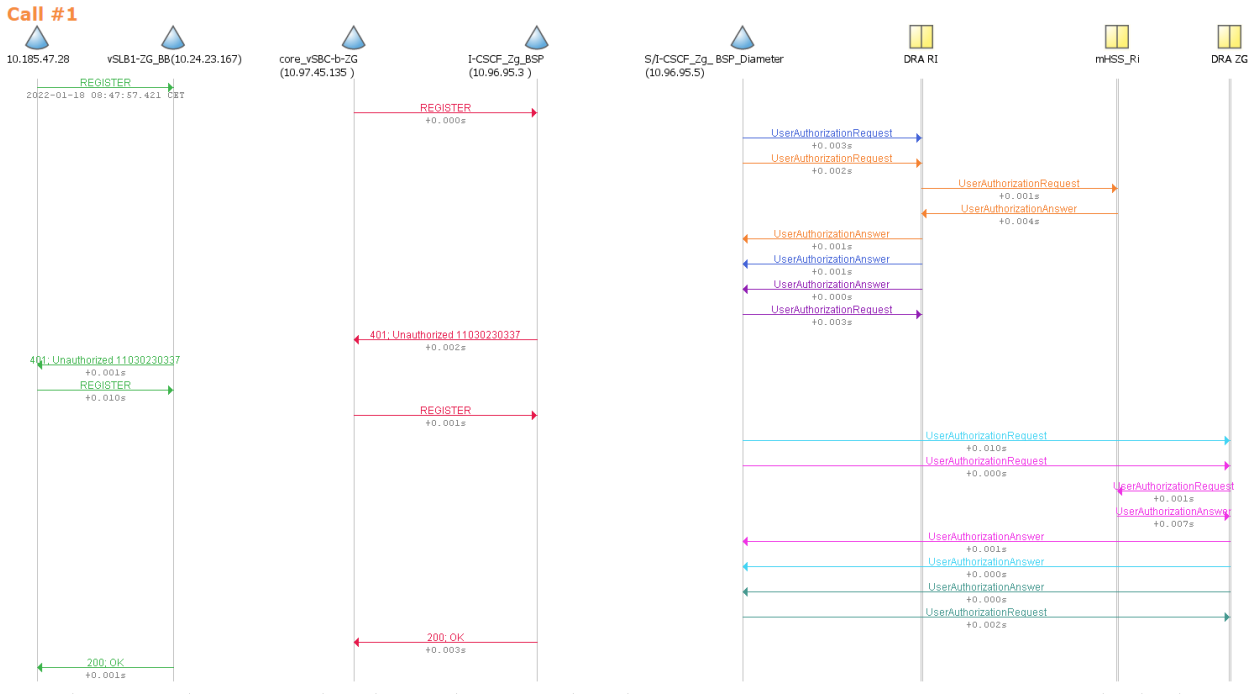
7. 4. Dimaeter protokol za redak 6. UAA.

Result-Code označava rezultat autorizacije. Njegove tipične vrijednosti su:

- 2001 (DIAMETER_SUCCESS): Autorizacija je uspješna.
- 4001 (DIAMETER_ERROR): Dogodila se greška u autorizaciji.

Ako pogledamo Result code na slici 7.4 možemo vidjeti da je inicijalna registracija bila uspješna.

Korisnik se u određenim vremenski intervalima mora reregistrirati u sustav kako bi ostao ažuran. Na slici 7.5. je prikazana signalizacija za proces reregistracije. Obično vrijeme reregistracije za protokole kao što su DIAMETER i SIP iznosi 3600 sekundi (1 sat). Bitno je odrediti odgovarajuću granicu za vrijeme reregistracije kako bi se održala ravnoteža između sigurnosti i stabilnosti mreže.



7. 5. SIP reregistracija

Koraci SIP reregistracije prikazani na slici 7.5 su:

1. Korisnik A pokreće ponovnu registraciju s UE-A, gdje UE-A šalje REGISTER poruku prema matičnoj mreži. REGISTER uključuje korisničku javnu adresu, privatnu adresu, IP adresu registriranog UE-a, vrijednost "nonce" i izračunatu "response" vrijednost za autentifikacijski zahtjev prethodno primljen od S-CSCF-a te novu vrijednost trajanja registracije. REGISTER se šalje na P-CSCF koristeći unaprijed konfiguriranu proxy adresu u UE-u.

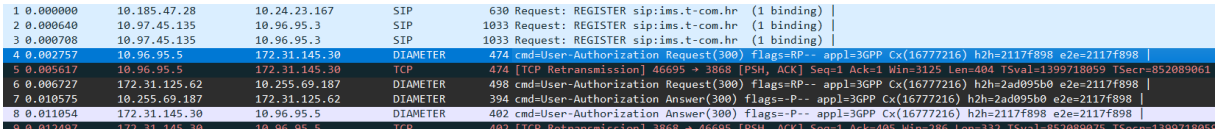
2. P-CSCF prosljeđuje REGISTER na S-CSCF-A dodavanjem SCSCF-URI iz Route-Headera (pohranjenog tijekom inicijalne registracije).

3. S-CSCF umeće primljene autentifikacijske parametre u novi Cx MULTIMEDIA AUTHENTICATION REQUEST (Diameter protokol) prema HSS-u.

4. HSS provjerava primljene "nonce" i "response" vrijednosti i vraća pozitivnu potvrdu te novu "nonce" vrijednost (= "nextnonce").

5. Budući da je autentifikacija bila uspješna, S-CSCF ažurira vrijednost trajanja registracije na onu uključenu u primljeni REGISTER prije nego što pošalje 200 OK odgovor UE-u ukazujući da je ponovna registracija bila uspješna.

Na slici 7.6. prikazan je tok reregistracije.



7. 6. Tok reregistracije.

Analizom zapisa u četvrtom (4.) retku možemo izvuci bitne informacije za *Diameter User-Authorization Request* (UAR) za SIP re-registraciju:

- Vrsta poruke (cmd):

    - cmd=User-Authorization Request (300) - označava da je poruka zahtjev za autorizaciju korisnika. U kontekstu SIP re-registracije, ovo je početni korak gdje se potvrđuje identitet korisnika.

- RP--: Flagovi označavaju svojstva poruke. R označava da je poruka zahtjev (Request), a P označava da koristi Proxy bit.

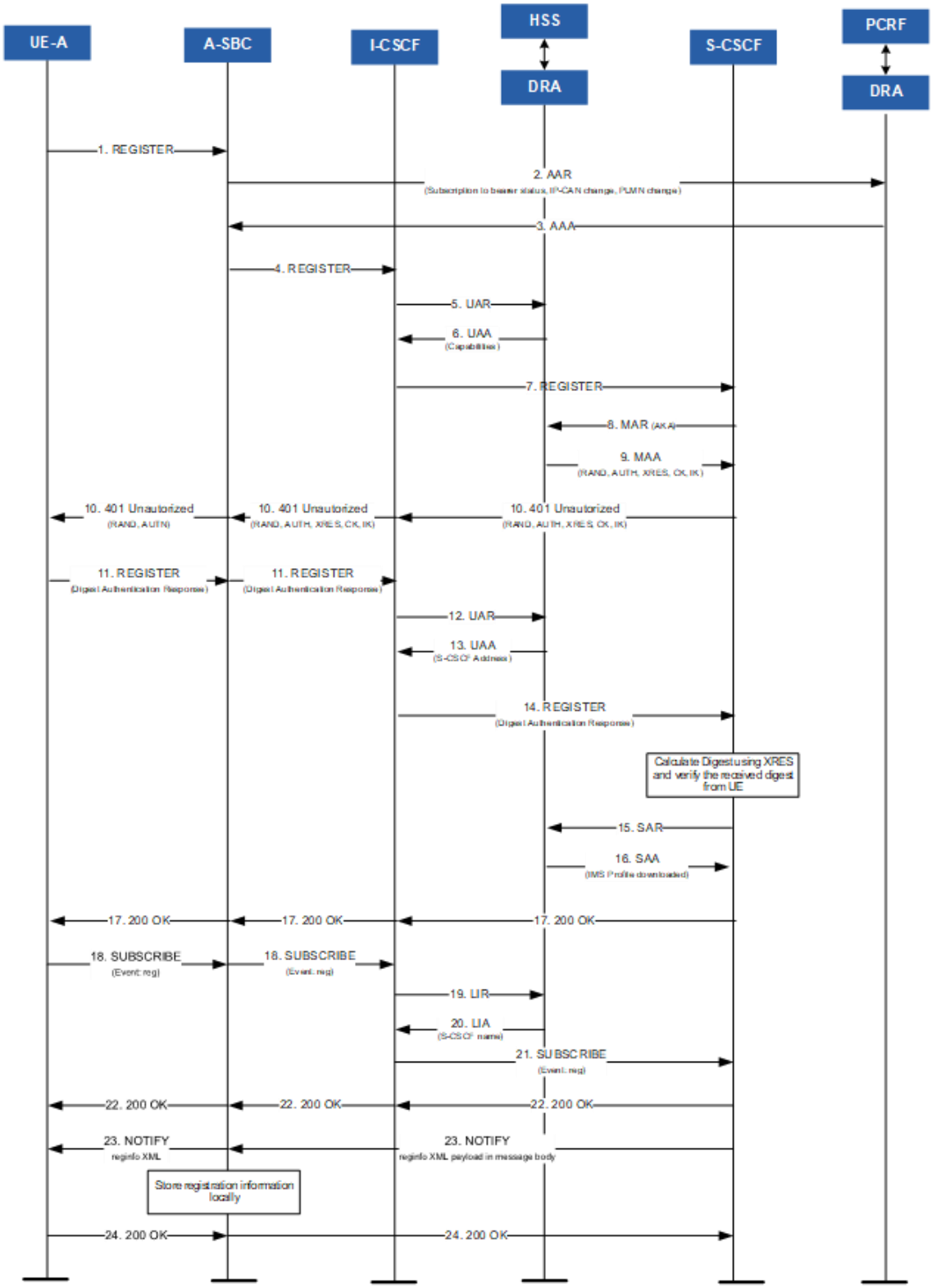
- Application ID (appl):
    - 3GPP Cx (16777216) - ovaj ID označava da poruka pripada 3GPP Cx aplikacijskom protokolu, koji se koristi za IP Multimedia Subsystem (IMS).

- Hop-by-Hop Identifier (h2h):
    - 2117f898 - ovaj identifikator koristi se za povezivanje zahtjeva i odgovora kroz više čvorova. Ovaj broj je jedinstven za svaku transakciju između dva susjedna Diameter čvora.

- End-to-End Identifier (e2e):
    - 2117f898 - ovaj identifikator je jedinstven za cijelu sesiju i koristi se za praćenje poruke od početka do kraja kroz cijelu mrežu.

VoLTE inicijalna registracija je proces u kojem se uređaj autenticira na LTE mrežu radi uspostavljanja osnovne veze za glasovne i podatkovne usluge putem IP-a. U ovom procesu, uređaj šalje zahtjev za registraciju, a mreža provjerava i potvrđuje identitet uređaja. Nakon uspješne registracije uređaj može započeti komunikaciju preko VoLTE mreže.

Na slici 7.7. nalazi se prikaz VoLTE inicijalne registracije.



7. 7. Volte inicijalna registracija.

Proces registracije je sljedeći:

- Početni SIP REGISTER zahtjev:
  - UE šalje početni SIP REGISTER zahtjev za registraciju na mreži.

- 2-3. Rx sesija:
  - Aktivira se Rx sesija koja se povezuje s default signalizacijskim nosačem. Koristi se za:
    - Pretplatu na obavijesti o statusu signalizacijskog nosača.
    - Pretplatu na IP-CAN_Change događaje dok je UE u stanju mirovanja (nije u pozivu).
    - Pretplatu na promjene PLMN (Public Land Mobile Network), npr. kad roamer na S8HR izvrši IMS.

- 4-6. I-CSCF upit prema HSS-u:
  - Kada REGISTER zahtjev dođe do I-CSCF, I-CSCF šalje upit HSS-u kako bi dobio informacije o serverima (S-CSCF) koje će se koristiti za korisnika.

- Prosljeđivanje REGISTER zahtjeva:
  - Početni REGISTER zahtjev I-CSCF prosljeđuje prema S-CSCF-u koji je odredio HSS.

- 8-9. Autentifikacija:
  - S-CSCF šalje Cx Multimedia Authentication Request (MAR) prema HSS-u kako bi dobio autentifikacijski vektor. HSS vraća autentifikacijski vektor S-CSCF-u.

- 10. SIP 401 Unauthorized:
  - S-CSCF sprema XRES parametar i uključuje RAND, AUTN, CK, i IK parametre u SIP 401 Unauthorized poruku koja se šalje prema A-SBC/P-CSCF radi autorizacije.

- 11. Autorizacijski odgovor:
  - UE šalje REGISTER zahtjev s autorizacijskim odgovorom.

- 12-13. Ponovni upit I-CSCF-a prema HSS-u:
    - I-CSCF ponovno šalje UAR (User-Authorization Request) prema HSS-u kako bi potvrdio odabir S-CSCF-a za korisnika.

- 14. Prosljeđivanje UAR REGISTER zahtjeva:
    - Nakon odgovora HSS-a, I-CSCF prosljeđuje UAR REGISTER zahtjev prema S-CSCF-u.

- 15-16. Dobivanje korisničkog profila:
    - S-CSCF šalje upit HSS-u kako bi dobio korisnički profil putem Cx protokola.

- 200 OK odgovor:
    - S-CSCF šalje 200 OK odgovor natrag prema UE, potvrđujući uspješnu registraciju.

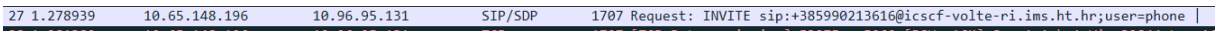
- 18-19. Pretplata na događaje registracije:
    - P-CSCF se pretplaćuje na paket događaja registracije.

- 20-21. Obavijesti o registraciji:
    - S-CSCF sprema pretplatu P-CSCF-a na događaje registracije i šalje NOTIFY poruku s informacijama o početnoj registraciji. Kad god se promijeni registracijska informacija, S-CSCF šalje dodatne NOTIFY poruke prema P-CSCF-u, koji lokalno sprema stanje registracije.

Ovaj proces opisuje korake kroz koje uređaj (UE) prolazi kako bi se registrirao na IMS mreži. Glavni koraci uključuju slanje početnog REGISTER zahtjeva, autentifikaciju korisnika putem S-CSCF-a i HSS-a, te potvrdu uspješne registracije. Osim toga, P-CSCF se pretplaćuje na događaje vezane uz registraciju kako bi mogao pratiti status korisnika.

U Wiresahrk programu mogu se izvojiti bitne informacije za analizu kao što su:

- SIP INVITE zahtjev



7. 8. SIP invite zahtjev.

Informacije prikazane na slici 7.8.:

- Vrijeme:
  - Vrijeme zapisa: 1.278939 sekundi od početka snimanja.
  - Ovaj podatak je važan za vremensku analizu komunikacijskog toka.

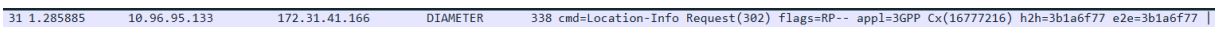
- IP adrese:
  - Izvorna IP adresa: 10.65.148.196 (IP adresa korisničkog uređaja ili mrežnog elementa koji šalje INVITE zahtjev).
  - Odredišna IP adresa: 10.96.95.131 (IP adresa mrežnog elementa, npr. I-CSCF).

- SIP metoda:
  - Metoda: INVITE
  - Ovaj zahtjev inicira novu sesiju ili poziv u VoLTE mreži.

- Request URI:
  - URI: sip:+385990213616@icscf-volte-ri.ims.ht.hr;user=phone
  - Ciljani korisnik je označen s sip:+385990213616, a domena mreže je icscf-volte-ri.ims.ht.hr.

- SDP (*Session Description Protocol*):
  - SDP dio poruke sadrži informacije o multimedijskim parametrima sesije, kao što su kodeci, IP adrese i portovi za RTP (Real-time Transport Protocol).

- Zahtjev za informacijama o lokaciji:



7. 9. Zahtjev za informacijama o lokaciji.

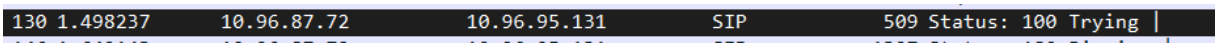
- Komanda Location-Info Request(302):
  - Ovo je zahtjev za informacijama o lokaciji korisnika u mreži.

- Zastavice RP-- (Request, Proxyable):
  - Označavaju da je ovo zahtjev (Request) i da se može poslati preko proxyja (Proxyable).

- Aplikacija 3GPP Cx (16777216):
  - Ukazuje da se koristi aplikacija Cx specifična za 3GPP (3rd Generation Partnership Project) za ovu komunikaciju.

- Identifikatori H2H i E2E:
  - Identifikatori koji prate poruke kroz mrežu, korisni za dijagnostiku i praćenje komunikacijskog toka.

- Odgovor "100 Trying" na Invite zahtjev



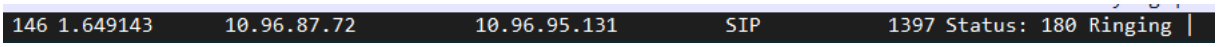
7. 10. Odgovor "100 Trying" na Invite zahtjev

- Ova poruka se šalje kao odgovor na SIP INVITE zahtjev.

- Indikacija je da je INVITE zahtjev primljen i da se trenutno obrađuje, ali još nema konačnog odgovora (npr. 180 Ringing, 200 OK).

- Pomaže u obavještavanju pošiljatelja INVITE zahtjeva da je zahtjev u tijeku, sprečavajući timeout ili ponavljanje zahtjeva.

U VoLTE mrežama, kada korisnički uređaj (UE) šalje INVITE zahtjev za uspostavu poziva, mrežni elementi (kao što su P-CSCF, I-CSCF, S-CSCF) mogu poslati "100 Trying" odgovor kako bi naznačili da se zahtjev obrađuje. Ovaj odgovor je ključan za održavanje fluidne komunikacije i osiguranje da korisnički uređaj ne ponavlja zahtjeve nepotrebno.



7. 11. "180 Ringing" poruke

Na slici 7.11. prikazan je redak 180 Ringing poruke. Ova poruka se šalje kao odgovor na SIP INVITE zahtjev. Omogućava pozivatelju da zna da je poziv stigao do pozvanog korisnika i da je u tijeku zvonjenje. Odgovor je ključan za davanje povratne informacije pozivatelju da je poziv stigao do destinacije.

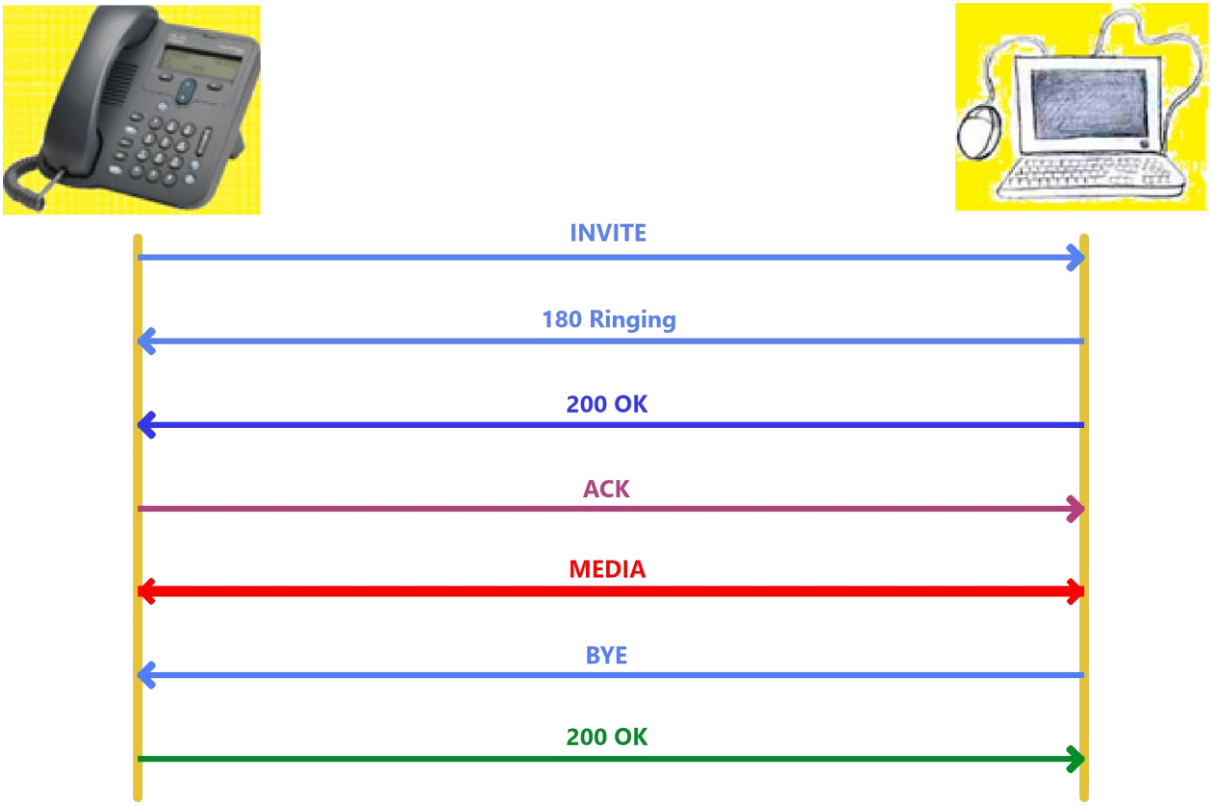
7. 12. 487 Request Terminated poruke

Na slici 7.12. prikazan je zahtjev Terminated poruke. Ova poruka se šalje kao odgovor na SIP zahtjev koji je prekinut prije nego što je završen. Tipično, to znači da je pozivatelj prekinuo poziv (npr. poslao BYE) prije nego što je pozvani korisnik mogao odgovoriti. Indikacija je da je obrada zahtjeva prekinuta, te da se poziv neće uspostaviti. Ova poruka je ključna za obavještavanje svih strana uključenih u poziv da je zahtjev prekinut i da se ne treba nastaviti s obradom.

ACK (*Acknowledgment*) je SIP poruka koja potvrđuje prijem 200 OK odgovora ili odgovora koji završava INVITE transakciju. U ovom slučaju, ACK poruka potvrđuje prijem "487 Request Terminated" odgovora.

Kada korisnički uređaj (UE) šalje INVITE zahtjev za uspostavu poziva, mrežni elementi poput P-CSCF, I-CSCF i S-CSCF mogu poslati različite odgovore, uključujući "487 Request Terminated" ako je poziv prekinut. Nakon što se pošalje takav odgovor, uređaj koji je poslao INVITE mora potvrditi prijem tog odgovora slanjem ACK poruke. Ovo zatvara SIP transakciju i osigurava da su obje strane svjesne trenutnog statusa poziva.

Cijeli tok uspostave opisanog poziva prikazan je na slici 7.13.



7. 13. Prikaz SIP poziva

Osnovni opis jednog SIP poziva:

- REGISTRACIJA: prije nego se poziv može obaviti oba krajnja korisnika moraju biti registrirani na SIP server.
- INICIJALIZACIJA POZIVA (INVITE): Korisnik A (UA-A) šalje INVITE poruku korisniku B (UA-B) preko SIP servera. INVITE poruka sadrži informacije o pozivatelju, pozvanom broju, i medijskim parametrima (SDP - Session Description Protocol).
- POZIV NA ČEKANJU :
    - 100 Trying: SIP server odgovara sa "100 Trying" na INVITE poruku, što znači da pokušava da pronađe korisnika B.
    - 180 Ringing: Kada SIP server pronađe korisnika B i pošalje mu INVITE poruku, korisnik B odgovara sa "180 Ringing", što znači da njegov uređaj zvoni.
- PRIHVAĆANJE POZIVA:
    - 200 OK: Kada korisnik B prihvati poziv, njegov uređaj šalje "200 OK" poruku korisniku A preko SIP servera. Ova poruka potvrđuje prihvaćanje poziva i može sadržavati dodatne medijske parametre.
- USPOSTAVLJANJE MEDIJSKOG TOKA:
    - ACK: Nakon što korisnik A primi "200 OK" poruku, šalje "ACK" poruku korisniku B da potvrdi uspostavljanje sesije. Medijski tok (RTP - Real-time Transport Protocol) se zatim uspostavlja direktno između korisnika A i B, omogućavajući prijenos glasa ili videa.
- ZATVARANJE POZIVA:
    - BYE: Kada jedan od korisnika želi da završi poziv, šalje "BYE" poruku drugom korisniku.

- 200 OK: Drugi korisnik odgovara sa "200 OK" porukom na BYE poruku, čime se završava SIP sesija i medijski tok se prekida.

8. ZAKLJUČAK

AAA poslužitelji (autentikacija, autorizacija i administracija) ključni su u telekomunikacijskim sustavima, osiguravajući kontrolu pristupa i sigurnosne mjere. Sastoje se od tri glavne komponente: autentikacija (provjera identiteta korisnika putem lozinki, certifikata ili biometrije), autorizacija (dodjeljivanje pristupnih prava na temelju uloga korisnika) i administracija (prikupljanje i analiza računovodstvenih podataka za nadzor mreže i naplatu). Korišteni protokoli uključuju RADIUS i Diameter. AAA poslužitelji centraliziraju kontrolu mrežnog pristupa, poboljšavaju sigurnost i pomažu u održavanju točnih evidencija i optimizaciji mreže.

AAA poslužitelji koriste autorizacijske protokole poput RADIUS-a i Diameter-a za kontrolu pristupa mrežnim resursima. RADIUS centralizira autentikaciju i autorizaciju mrežnog pristupa, dok Diameter poboljšava sigurnost i fleksibilnost u usporedbi s RADIUS-om. Sigurnosna razmatranja u autorizaciji uključuju definiranje jasnih politika kontrole pristupa i primjenu načela najmanjih privilegija.

Mehanizmi kontrole pristupa uključuju DAC, MAC i RBAC, s RBAC-om kao popularnim modelom za AAA poslužitelje zbog jednostavnije administracije. Sigurnosne mjere za poboljšanje autorizacije uključuju višefaktorsku autentikaciju, redovito praćenje i reviziju politika pristupa. Administrativni protokoli poput RADIUS-a i TACACS+ upravljaju autentikacijom i autorizacijom korisnika, s TACACS+ pružajući veću fleksibilnost u kontroli pristupa. Diameter se koristi u modernim mrežama, uključujući 5G, zbog svoje skalabilnosti i sigurnosti.

Sigurnosni problemi AAA poslužitelja uključuju neovlašteni pristup, DoS napade, slabe mehanizme provjere autentičnosti i krađu vjerodajnica. Rješavanje sigurnosnih problema zahtijeva jake kontrole pristupa, enkripciju i redovitu sigurnosnu procjenu. Implementacija višefaktorske autentikacije i segmentacija mreže ključni su za zaštitu AAA poslužitelja.

Osiguranje komunikacije između AAA klijenata i poslužitelja putem TLS-a pomaže u zaštiti osjetljivih informacija. Sveobuhvatno bilježenje i praćenje aktivnosti ključni su za otkrivanje i reagiranje na sigurnosne incidente. Regularno ažuriranje softvera AAA poslužitelja pomaže u sprječavanju iskorištavanja poznatih sigurnosnih propusta. Organizacije trebaju biti svjesne novih prijetnji i najboljih praksi za osiguranje AAA poslužitelja.

U praktičnom dijelu rada prikazana je analiza AAA pokusa uključujući korake SIP registracije te prikaz toka registracije i reregistracije u IP multimedijskom sustavu (IMS-u) čija je signalizacija snimljena programom Wireshark. Analizom signalizacije detaljno su pojašnjene i obrađene funkcije registracije i reregistracije te njihova važnost u komunikacijskom procesu.

LITERATURA

[1] Nakhjiri, M., & Nakhjiri, M. (2005). AAA and network security for mobile access: radius, diameter, EAP, PKI and IP mobility. John Wiley & Sons.

[2] Burnett, M. (2006). Perfect password: Selection, protection, authentication. Elsevier.

[3] Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. Int. J. Sci. Technol. Res, 5(11), 246-249

[4] Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.

[5] Uzunov, A. V., Fernandez, E. B., & Falkner, K. (2015). Security solution frames and security patterns for authorization in distributed, collaborative systems. Computers & Security, 55, 193-234.

[6] Metz, C. (1999). AAA protocols: authentication, authorization, and accounting for the Internet. IEEE Internet Computing, 3(6), 75-79.

[7] Bertino, E. (2003). RBAC models—concepts and trends. Computers & Security, 22(6), 511-514.

[8] Housley, R., & Aboba, B. (2007). Guidance for authentication, authorization, and accounting (AAA) key management (No. rfc4962).

[9] Ravi, V., Sunitha, N. R., Pradeep, R., & Verma, S. (2017, December). Formal methods to verify authentication in TACACS+ protocol. In 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT) (pp. 1-4). IEEE.

[10] Tschofenig, H., Decugis, S., Mahoney, J., & Korhonen, J. (2019). Diameter: New Generation AAA Protocol-Design, Practice, and Applications. John Wiley & Sons.

[11] Stallings, W. (2016). Network security essentials: applications and standards. Pearson.

[12] Materijali s predavanja

SAŽETAK

Cilj ovog završnog rada bio je detaljnije razumjeti kako AAA poslužitelji, kroz autentikaciju, autorizaciju i administraciju igraju ključnu ulogu u osiguravanju sigurnosti i upravljanju pristupom u telekomunikacijskim sustavima. Fokus je bio na analizi kako ovi poslužitelji omogućuju kontrolu pristupa mrežama, što je od vitalnog značaja za zaštitu osjetljivih korisničkih podataka od stalnih sigurnosnih prijetnji i ranjivosti.

U praktičnom dijelu istraživanja detaljno je prikazana analiza AAA sustava, što uključuje korake SIP registracije i prikaz toka registracije te reregistracije korištenjem programa Wireshark. Kroz analizu, istražene su komponente i važnost procesa registracije i reregistracije kako bi se bolje razumjela njihova funkcija.

Ključne riječi: SIP, RADIUS, DIAMETER, VoIP

SUMARRY

The aim of this bachelor thesis was to gain a deeper understanding of how AAA servers, through authentication, authorization, and administration, play a crucial role in ensuring security and managing access in telecommunications systems. The focus was on analyzing how these servers enable network access control, which is vital for protecting sensitive user data from ongoing security threats and vulnerabilities.

In the practical part of the study, a detailed analysis of AAA systems was presented, including the steps of SIP registration and the display of registration and re-registration flows using Wireshark. Through this analysis, the components and importance of the registration and re-registration processes were explored to better understand their functionality

Key words: SIP, RADIUS, DIAMETER, VoIP

POPIS SLIKA

ŽIVOTOPIS

Josip Pejić rođen je 13.05.1999. godine u Slavonskom Brodu. 2014. godine završava osnovnu školu Antun Matija Reljković Bebrina nakon čega upisuje Tehničku školu u Slavonskom Brodu smjer Tehničar za računalstvo. Nakon završene srednje škole 2019. godine upisuje stručni preddiplomski studij Računalstva na Fakultetu elektrotehnike, računalstva i informacijskih tehnologija u Osijeku.