Centar Informacijske Sigurnosti

Protokoli za podršku sjednice

lipanj 2011.

CIS-DOC-2011-05-014

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Sjednice su jedan od vrlo važnih segmenata u komunikaciji Internetom. One se uspostavljaju između dvoje ili više sudionika prije početka razmjene informacija. Sjednice mogu biti vrlo raznolike. Od jednostavnih sjednica između klijenta i poslužitelja u kojima se razmjenjuju jednostavni upiti i odgovori, do složenijih višemedijskih sjednica koje koriste različite izvore medijskih tokova podataka poput videa, zvuka i sintetičkih sadržaja. Protokoli koji pružaju podršku za sjednice moraju podržavati različite oblike sjednica, što predstavlja izazov u njihovom dizajnu. Veliku pažnju je potrebno posvetiti sigurnosti sjednice kako bi se zaštitili podaci koje sudionici izmjenjuju. U nekim sjednicama se otkrivaju osjetljivi podaci koji se mogu iskoristiti za daljnje napade.

Ovaj dokument se sastoji od tri dijela. Na početku će biti objašnjen pojam sjednice i za što se ona koristi. Objasnit će se koje je to probleme potrebno riješiti prije pokretanja sjednice i na koji način se oni rješavaju. Zatim će biti detaljno objašnjena tri protokola koja se koriste za uspostavljanje sjednice. Za svaki protokol će biti objašnjeno u kojim slučajevima se koriste, koje su njihove prednosti i nedostaci te način na koji se koriste. Objašnjenja će biti popraćena primjerima radi lakšeg shvaćanja. Zadnji dio dokumenta će se osvrnuti na sigurnosne probleme koji se javljaju pri korištenju sjednica. Objasnit će se najčešći napadi na sjednice te neki od sigurnosnih mehanizama kojima je napade moguće spriječiti.

2. Sjednica

Sjednica se definira kao polutrajna interaktivna razmjena informacija između dva ili više komunikacijskih uređaja ili između korisnika i računala. Za svaku sjednicu mora biti poznato kada je uspostavljena i kada je raskinuta, a najmanje jedan od sudionika sjednice mora čuvati informacije o povijesti sjednice, odnosno mora čuvati stanje u kojem se sjednica nalazi. Sjednice se mogu definirati na nekoliko slojeva OSI referentnog modela:

- Aplikacijski sloj – npr. HTTP sjednice;
- Sloj sjednice – npr. SIP sjednice;
- Transportni sloj – npr. TCP sjednice.

Jedan od najčešćih oblika arhitekture u Internetu je tzv. klijent-poslužitelj arhitektura koja se temelji na razmjeni informacija između dvije strane (klijenta i poslužitelja) pomoću mehanizma zahtjeva i odgovora. Prije nego razmjena informacija započne, između klijenta i poslužitelja se uspostavlja sjednica. Nakon toga, klijent može slati poslužitelju zahtjeve, a poslužitelj može na njih odgovarati. Sjednice u klijent-poslužitelj arhitekturi se razlikuju po mjestu na kojem se pohranjuje stanje sjednice. Razlikuju se:

- *server-side* sjednice i
- *client-side* sjednice.

U *server-side* obliku sjednice, podaci o stanju sjednice se pohranjuju na poslužitelju. Ovakav oblik sjednice je jednostavan i učinkovit ako poslužitelj mora komunicirati s malim brojem klijenata, jer inače memorija poslužitelja postaje nedostatna za pohranu podataka o svim tekućim sjednicama.

U *client-side* obliku sjednice, stanje sjednice se zapisuje na klijentskoj strani pomoću datoteka koje se zovu kolačići (eng. *cookies*). Na taj način se ne zahtjeva pohrana velike količine podataka na poslužiteljima. Kada korisnik otvori *web* stranicu, poslužitelj korisničkom Internet pregledniku šalje podatke o stanju u obliku kolačića. Klijent pohranjuje kolačić u memoriju ili na tvrdi disk. U zahtjevima koje potom šalje poslužitelju, šalje i dobiveni kolačić kako bi poslužitelj znao koje podatke mora poslati klijentu kao odgovor na njegov zahtjev. Problem koji se javlja je mogućnost izmjene podataka na klijentu. Kako bi se izbjegla moguća zloupotreba, potrebno je osigurati:

- **Povjerljivost** (eng. *confidentiality*): samo poslužitelj smije pregledavati podatke o sjednici.
- **Integritet** (eng. *integrity*): samo poslužitelj smije mijenjati podatke o sjednici.
- **Vjerodostojnost** (eng. *authenticity*): samo poslužitelj smije pokretati sjednice.

Opisani zahtjevi se ostvaruju šifriranjem podataka o sjednici na poslužitelju prije njihovog slanja klijentu. Dodatni problem je veličina kolačića. Razmjena kolačića između klijenta i poslužitelja pri svakom zahtjevu odnosno odgovoru može biti prihvatljiva samo ukoliko je kolačić male veličine. Veliki kolačić može značajno utjecati na brzinu prijenosa „korisnih“ podataka. Problem se rješava kompresijom kolačića na poslužitelju prije njegovog slanja klijentu.

Moguća je i kombinacija prethodna dva oblika sjednice, a primjer je značka HTTP sjednice. HTTP je protokol aplikacijskog sloja koji koristi sjednicu između klijenta i poslužitelja za razmjenu informacija. Značka HTTP sjednice je jedinstveni identifikator kojeg poslužitelj šalje klijentu kako bi označio trenutnu sjednicu. U pravilu se značka HTTP sjednice pohranjuje kao kolačić na klijentskom računalu. Kada poslužitelj to zatraži, značka se šalje kao parametar u GET ili POST upitima. Razlika u odnosu na *client-side* oblik sjednice je da korisnik nema sve podatke o sjednici, nego samo identifikator sjednice. Svi podaci o sjednici se nalaze na poslužitelju u internoj bazi podataka kojoj klijent ne može pristupiti. Kolačić se koristi samo za povezivanje klijenta s odgovarajućim podacima o sjednici.

3. Protokoli za podršku sjednice

U prethodnom poglavlju je spomenuto da se sjednica može definirati na tri sloja OSI modela. Ovisno o sloju na kojem se definira sjednice, koriste se različiti protokoli za opis i uspostavljanje sjednice. U ovom dokumentu će biti opisani sljedeći protokoli:

- SDP (eng. *Session Description Protocol*) – protokol za opis sjednice.
- SAP (eng. *Session Announcement Protocol*) – protokol za objavu sjednice.
- SIP (eng. *Session Initiation Protocol*) – protokol za pokretanje sjednice.

Najčešće sjednice u kojima se koriste spomenuti protokoli su višemedijske sjednice poput VoIP (eng. *Voice over IP*) telefonije. Ostale upotrebe uključuju videokonferencijske pozive, IM (eng. *Instant messaging*), prijenos datoteka i mrežne igre. Svima je zajedničko da koriste više medijskih tokova podataka (npr. u videokonferenciji se prenose zvuk i video), a svaki tok podataka se kodira na drugačiji način. Zbog toga se sudionici moraju dogovoriti o načinu na koji će kodirati medijske podatke kako bi ih svi znali dekodirati. U tu svrhu se koristi prvi protokol koji će biti objašnjen u ovom dokumentu, a radi se protokolu SDP.

3.1. Protokol za opis sjednice

Prije uspostavljanja sjednice između dva ili više sudionika, potrebno se je dogovoriti o parametrima sjednice. Najvažniji parametri su naziv i svrha sjednice te vrijeme održavanja. Dodatno se mogu razmijeniti i ostali parametri koji detaljnije opisuju način razmjene podataka, protokole koje se koriste, medijske tokove podataka kod višemedijskih sjednica itd.

SDP protokol definira format za opis sjednice. Najnovija specifikacija protokola nosi oznaku RFC 4566 [3]. Važno je naglasiti da se ovim protokolom ne uspostavlja sjednica, nego se samo opisuju parametri sjednice, a omogućeno je i pregovaranje. Zbog toga se SDP protokol koristi zajedno s nekim drugim protokolom poput protokola SAP i SIP (koji će biti objašnjeni kasnije).

Opis sjednice mora pružiti sve potrebne podatke kako bi svi sudionici sjednice mogli primati sve podatke u sjednici. U višemedijskim sjednicama može se prenositi nekoliko tokova medija, primjerice zvuk i video. U opisu sjednice pomoću SDP protokola potrebno je navesti sve potrebne informacije za dva medija: zvuk i video. To uključuje podatke o koderu i korištenom transportnom protokolu za svaki od medija.

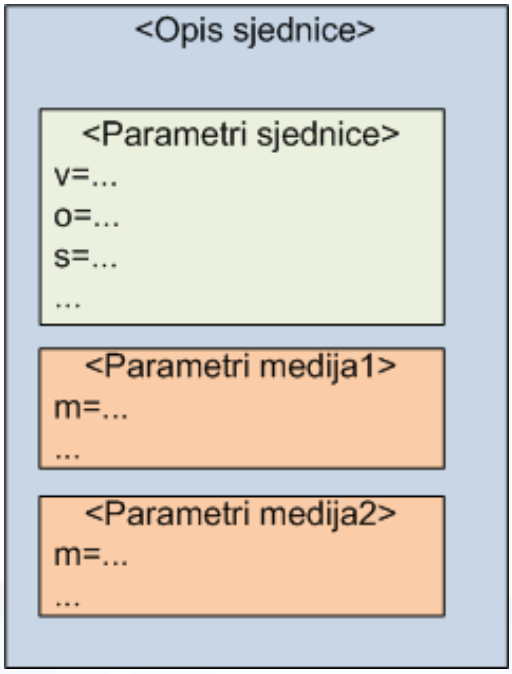
Opis sjednice SDP protokolom izgleda kao obični tekst koji se sastoji od niza redaka oblika:

```
<vrsta>=<vrijednost>
```

gdje je <vrsta> jedan znak koji označava neki od atributa, a <vrijednost> niz znakova čiji format ovisi o atributu kojeg opisuje.

Atributi se mogu podijeliti u dvije skupine (Slika 1):

1. **Parametri sjednice** – vrijede za cijelu sjednicu i za sve tokove medija (ukoliko nisu izričito nadjačanim nekim atributom medija).
2. **Parametri medija** – po jedna skupina za svaki tok medija.



Slika 1. Opis sjednice u SDP formatu

Parametri sjednice uvijek započinju atributom oznake „*v*", a završavaju prvom oznakom „*m*" koja označava atribut medija. Neki od parametara sjednice su obavezni i moraju biti navedeni u svakom opisu sjednice. To su parametri:

- „*v*" – inačica protokola,
- „*o*" – vlasnik/pokretač sjednice i identifikator sjednice i
- „*s*" – naziv sjednice.

Atributi s oznakama „*v*", „*o*" i „*s*" se mogu naći na početku svakog opisa sjednice, točno u tom poretku. Ostali (neobavezni) parametri sjednice su objašnjeni u tablici 1.

Oznaka atributa	Opis
i	dodatni podaci o sjednici
u	URI (eng. *Uniform Resource Identifier*) s opisom sjednice
e	adresa elektroničke pošte osobe za kontakt
p	telefonski broj osobe za kontakt
c	podaci o vezi
b	širina pojasa za prijenos podataka [kbit/s]
t	vrijeme održavanja sjednice
r	vrijeme ponavljanja (dolazi zajedno s atributom „*t*", moguće je postojanje nekoliko blokova „*t-r*" atributa)
z	podaci o vremenskoj zoni
k	ključ šifriranja
a	dodatni atributi sjednice (niti jedan, jedan ili više atributa)

Tablica 1. Neobavezni parametri sjednice

Drugu skupinu atributa čine parametri medija koji se zapisuju u blokove. Svaki blok parametara medija opisuje jedan tok medija koja se koristi u sjednici, a moguće je koristiti niti jedan, jedan ili više blokova. Blok započinje s obaveznim atributom oznake „*m*" i završava retkom ispred sljedeće oznake „*m*" ili zadnjim retkom u opisu sjednice (ukoliko je to zadnji blok medija).

Parametri medija navedeni su u tablici 2.

Oznaka atributa	Opis
m	naziv medija i transportna adresa, obavezni atribut
i	naslov medija
c	podaci o vezi
b	širina pojasa za prijenos podataka [kbit/s], odnosi se na jedan medij
k	ključ šifriranja
a	dodatni atributi za opis medija

Tablica 2. Parametri medija

Potrebno je primijetiti da se neki atributi za opis medija koriste i kao atributi parametara sjednice. Razlika je u tome što ovi atributi opisuju isključivo medij definiran u atributu s oznakom *m* i nadjačavaju parametre sjednice. Ukoliko nisu navedeni, koriste se parametri sjednice.

Primjer opisa sjednice nalazi se u nastavku (primjer je preuzet iz RFC specifikacije [3]):

```
v=0
o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.example.com/seminars/sdp.pdf
e=j.doe@example.com (Jane Doe)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 99
a=rtpmap:99 h263-1998/90000
```

Kao što je već spomenuto, opis sjednice započinje s tri obavezne oznake atributa („*v*", „*o*" i „*s*"). Vrijednost oznake „*v*" je 0, a ona označava inačicu SDP protokola. U sljedećem redu se nalaze osnovni podaci o sjednici. Iz tog retka se može očitati da je vlasnik sjednice korisnik *jdoe*. Kada vlasnik nije poznat ili nije važan, upisuje se znak crtice „-". Ostale vrijednosti u tom retku su identifikator sjednice, inačica sjednice, tip mreže (Internet), tip adrese (IPv4 adresa) i adresa izvora. Atribut oznake „*s*" ima vrijednost „SDP seminar" i to je ujedno naziv sjednice. Dodatni podaci o sjednici su navedeni u atributima „*i*" (opis sjednice) te „*u*" (URI s opisom sjednice). Kontakt podaci vlasnika sjednice su navedeni u atributu oznake „*e*". Kao vrijednost atributa oznake „*c*" je navedena *multicast* IP adresa sjednice (224.2.17.12/127). Vrijednost atributa „*t*" ima dva podatka: prvi broj označava vrijeme početka sjednice, dok drugi označava kraj sjednice. Obje vremenske oznake su zapisane prema NTP (eng. *Network Time Protocol*) protokolu. Vrijednost atributa oznake „*a*" je *recvonly* što znači da sudionici mogu samo primati podatke, ali ne i mijenjati ih. S ovim atributom je završen blok parametara sjednice, a slijede dva (kratka) bloka parametara medija. Vrijednost atributa „*m*" se sastoji od četiri dijela:

- Tip medija – u ovom slučaju audio i video.
- Priključnica – u ovom slučaju 49170, odnosno 51372.
- Transportni protokol – u primjeru se koristi RTP (eng. *Real-time Transport Protocol*) za prijenos medijskog sadržaja.
- Oznaka formata medija – svakom koderu medija je dodijeljena jedinstvena oznaka definirana u RTP protokolu.

Ostale informacije o vrijednostima pojedinih atributa se mogu naći u dokumentu RFC 4566 [3].

SDP podržava pregovaranje o parametrima sjednice po modelu *ponuda – odgovor*: jedna strana pošalje svoj prijedlog opisa sjednice, s mogućim alternativama, a druga strana odgovara na ponudu. U izvornoj specifikaciji ponuda se stvarala nizanjem oznaka formata medija u vrijednosti atributa oznake „*m*". Odgovor na ponudu se sastojao od samo jedne oznake. Na primjer:

Ponuda:

```
   ...
m=audio 49170 RTP/AVP 0 4
   ...
```

Odgovor:

```
   ...
m=audio 49170 RTP/AVP 0
   ...
```

RFC 5939 predstavlja proširene mogućnosti pregovaranja. Krajnje točke specificiraju podržane mogućnosti, potencijalne konfiguracije i aktualne konfiguracije sjednice, a pregovarati se može oko aktualnih i/ili potencijalnih konfiguracija. Dodatno poboljšanje SDP-a uvedeno je specifikacijom RFC 5888, i uvodi mogućnost grupiranja različitih medija i njihovog zajedničkog opisa. Moguće je specificiranje odnosa između raznih medija.

Osim ograničenja u pregovaranju o sadržaju koji su ispravljeni novim specifikacijama, SDP ima još jedan problem koji je posljedica korištenja NTP protokola za zapis vremenskih oznaka. Vremenska oznaka je zapisana kao 64-bitni broj bez predznaka u prikazu s fiksnim zarezom, a mjeri vrijeme u sekundama, od početka dana dogovorenog datuma 1.1.1900. Tih 64 bita sastoji se od 32-bitnog broja cijelih sekundi i 32-bitnog broja ostatka koji odgovara djelićima sekunde. Rezultat je točnost prikaza vremena od 200 pikosekundi. Pretvorba prva 32 bita u sekunde ne predstavlja problem, ali računanje milisekundi iz zadnja 32 bita je vrlo složeno. Dodatno, NTP vremenske oznake nisu kompatibilne s drugim vrstama vremenskih oznaka što može predstavljati problem u sinkronizaciji.

3.2. Protokol za objavu sjednice

Kako bi potencijalni sudionici saznali za sjednicu, potrebno je sjednicu na neki način objaviti. Kada sudionici sjednice nisu unaprijed poznati, koristi se SAP protokol za objavu sjednice definiran u RFC 2974 [4]. Ovaj protokol koristi periodičko razašiljanje objave sjednice na dobro poznatu višeodredišnu adresu i priključnicu koju osluškuju potencijalni sudionici. To može biti na primjer:

- UDP priključnica 9875,
- višeodredišna IP adresa 224.2.127.254 (*sap.mcast.net*) ili
- administrativno određena višeodredišna IP adresa.

Korisnici osluškuju spomenute adrese i priključnicu te ukoliko prime objavu neke sjednice za koju su zainteresirani, po želji joj se priključuju. Pri objavi sjednice potrebno je poslati SDP opis sjednice kako bi potencijalni sudionici odmah saznali sve potrebne informacije o sjednici (npr. vrijeme početka i adresu sjednice).

Posebna pažnja je posvećena definiranju vremenskog razmaka između dvije objave sjednice. Vremenski razmak između objava se određuje dinamički kako bi u svakom trenutku ukupna širina pojasa za SAP objave bila najviše 4 kbps (osim ako to nije drugačije definirano u lokalnoj mreži). Kako bi to bilo moguće, svaki pošiljatelj objave sjednice mora osluškivati sve objave sjednica ostalih pošiljatelja. Na taj način saznaje broj sjednica koje se objavljuju i koliku širinu pojasa zauzimaju. Na temelju tih informacija određuje kojim vremenskim razmakom mora objavljivati svoje sjednice. Način računanja je sljedeći:

1. Pošiljatelj objave sjednice postavlja varijablu *tp* na vrijeme posljednje slanje objave (ili na trenutno vrijeme ako se radi o prvom slanju objave).
2. Na temelju definirane širine pojasa za SAP (*limit*), broja objava sjednica u mreži (*no_of_ads*) te veličine objave sjednice koju pošiljatelj želi objaviti (*ad_size*), računa se vremenski razmak između objave (*interval*) prema izrazu:

   interval = max(300; (8 * *no_of_ads* * *ad_size*) / *limit*)

3. Dodatno, računa se vremenski odmak (*offset*) prema
   offset = rand(*interval* * 2/3) – (*interval* / 3)
4. Nakon toga moguće je izračunati vrijeme sljedećeg slanja objave (*tn*):
   tn =*tp*+ *interval*+ *offset*

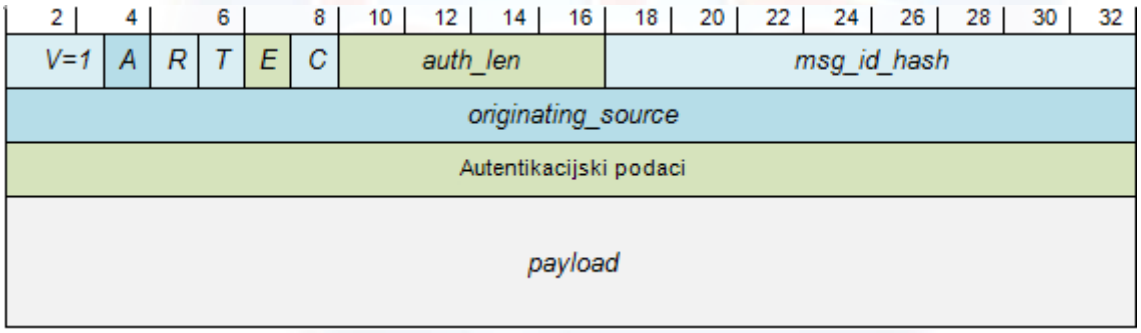
Pošiljatelj objave sjednice postavlja brojač i nakon što istekne *tn* ponovo računa vrijeme kada treba poslati sljedeću objavu.

U specifikaciji protokola SAP, definirani su i načini izmjene te odjave sjednice. Već objavljena sjednica se može izmijeniti vrlo jednostavno: dovoljno je objaviti izmijenjeni opis sjednice (podsjetnik: opis sjednice je definiran protokolom SDP). Kako bi se primateljima objave dalo do znanja da je opis sjednice izmijenjen, potrebno je promijeniti polje *msg_id_hash* u SAP paketu (objašnjeno kasnije). Na taj način primatelji uočavaju da je došlo do promjene i mogu ažurirati postojeći opis sjednice.

Odjava sjednice se može izvesti na tri načina:

1. **Eksplicitni istek vremena sjednice** (eng. *Explicit Timeout*) – u opisu sjednice mogu postojati vremenske oznake koje definiraju vrijeme početka i kraja sjednice (atribut oznake *t* u SDP opisu sjednice). Kada trenutno vrijeme bude veće od vremena kraja sjednice, tada bi se sjednica trebala odjaviti brisanjem na primateljevoj strani.
2. **Implicitni istek vremena sjednice** (eng. *Implicit Timeout*) – primatelj bi trebao periodički dobivati objave sjednice čak i za sjednicu koja trenutno traje. Na isti način kako pošiljatelj objave sjednice računa vrijeme slanja ponovne objave, primatelj može izračunati kada bi trebao primiti objavu sjednice. Ukoliko primatelj ne primi objavu sjednice unutar deset vremenskih perioda objave sjednice (odnosno za redom ne primi 10 objava za dotičnu sjednicu) ili unutar jednog sata, sjednica se odjavljuje brisanjem na primateljevoj strani.
3. **Eksplicitna odjava sjednice** (eng. *Explicit Deletion*) – obavlja se primanjem paketa za odjavu sjednice.

Na slici 2 prikazan je format SAP paketa. U RFC-u 2947 preporuča se da veličina SAP paketa ne prelazi 1kB kako ne bi došlo do fragmentacije paketa pri njegovom prijenosu.



Slika 2. SAP paket

Polja SAP paketa su sljedeća:

- *V*: inačica. Uvijek se postavlja na 1
- *A*: tip adrese. Ako je vrijednost 0, u polju *originating_source* će se nalaziti IPv4 adresa i polje će biti dugačko 32 bita. Ako se u polju *A* nalazi vrijednost 1, u polju *originating_source* će biti korištenja IPv6 adresa i polje će biti dugačko 128 bitova.
- *R*: rezervirano polje. Pošiljatelji objava postavljaju ovo polje na 0, a primatelji ignoriraju sadržaj ovog polja.
- *T*: tip poruke. Vrijednost 0 upućuje da se radi o paketu za objavu sjednice, a ako je vrijednost 1, radi se o paketu za odjavu sjednice
- *E*: zastavica za šifriranje. Ukoliko je vrijednost polja 1, polje *payload* će biti šifrirano.
- *C*: zastavica za sažimanje. Ukoliko je vrijednost polja 1, polje *payload* će biti sažeto korištenjem *zlib* kompresijskog algoritma.
- *auth_len*: veličina polja autentikacijskih podataka.

- *msg_id_hash*: ovo polje, zajedno s poljem *originating_source*, čini jedinstveni identifikator objave sjednice. Svaka SAP objava koja potiče od istog pošiljatelja i opisuje istu sjednicu ima isto *msg_id_hash* polje. Izmjenom opisa sjednice, polje se mijenja kako bi primatelji saznali da se opis tekuće sjednice promijenio.
- *originating_source*: IP adresa pošiljatelja objave sjednice, tj. izvora SAP paketa. Vrsta IP adrese (IPv4 ili IPv6) ovisi o vrijednosti u polju *A.*
- Autentikacijski podaci: ovo neobavezno polje sadrži digitalni potpis SAP paketa.
- *payload*: opis sjednice u SDP formatu. Polje započinje s „*application/sdp*“.

Iako postoji mogućnost šifriranja SAP paketa, ne preporuča se njegovo korištenje. Razlog je što se mreža nepotrebno opterećuje razašiljanjem paketa koje veliki broj primatelja ne može pročitati budući da nemaju odgovarajući ključ. Ukoliko za to zaista postoji potreba, preporuča se koristiti šifriranje SAP poruka u manjim mrežama, ali treba imati u vidu da način na koji se obavlja šifriranje podataka nije definiran u RFC-u 2974.

3.3. Protokol za pokretanje sjednice

Kako je već rečeno, SAP protokol se koristi kada sudionici sjednice nisu unaprijed poznati. Ukoliko sudionici jesu poznati, bolje je koristiti SIP protokol jer na taj način poruke o objavi sjednice dobivaju samo zainteresirani sudionici i ne dolazi do nepotrebnog zagušivanja mreže. Razvoj SIP-a je započeo 1996, a od tada je izdano nekoliko RFC dokumenata koji ga opisuju. Najnovija specifikacija nosi naziv RFC 3261 [6].

SIP se koristi za pokretanje, promjenu i odjavu sjednice između dva ili više sudionika, a sjednice mogu sadržavati nekoliko medijskih tokova podataka. Podržane su sljedeće izmjene sjednice:

- promjena adrese ili priključnice sjednice,
- poziv novih sudionika i
- dodavanje/uklanjanje medijskih tokova podataka.

SIP koristi SDP protokol za opis sjednice na isti način kako je objašnjeno u SAP protokolu. Na taj način sudionici dobivaju sve potrebne parametre za prijavu i sudjelovanje u sjednici. SIP je neovisan o transportnom protokolu koji se koristi za prijenos paketa pa tako može raditi zajedno s TCP ili UDP protokolom. Priključnice koje koristi SIP su 5060 i 5061. Prva priključnica se koristi kada promet nije potrebno šifrirati, dok se priključnica 5061 uobičajeno koristi za promet šifriran pomoću TLS-a (eng. *Transport Layer Security*).

3.3.1. Mrežni elementi

Protokol SIP je po svom dizajnu vrlo sličan HTTP-u (eng. *Hypertext Transfer Protocol*) jer koristi isti mehanizam zahtjeva i odgovora: klijent šalje zahtjev prema poslužitelju gdje se aktivira određena metoda ili funkcija, koja pak rezultira slanjem barem jednog odgovora klijentu. Ideja pri dizajnu protokola je bila da SIP pruža sličnu uslugu kao javna telefonska mreža (PSTN), ali preko IP-a. Zbog toga su uvedene neke značajke fiksne telefonije kao što su: pozivanje broja, čekanje da se druga strana javi, poziv na čekanju, prebacivanje poziva i sl. Kako bi to bilo moguće, uvedeni su sljedeći mrežni elementi (Slika 3):

- korisnički agent (eng. *user agent*) ili UA,
- poslužitelj za registraciju (eng. *registar*),
- posrednički poslužitelj (eng. *proxy server*) ili SIP usmjeritelj i
- poslužitelj za preusmjeravanje (eng. *redirect server*).

Korisnički agenti su krajnje točke u sjednici koje primaju ili šalje SIP poruke. Zapravo se radi o samim sudionicima sjednice. UA može biti UAC (eng. *User Agent Client*) koji šalje SIP zahtjeve ili UAS (eng. *User Agent Server*) koji prima zahtjeve i šalje odgovore. Ovom logičkom podjelom omogućuje se mehanizam zahtjeva i odgovora kao u HTTP-u. UAS ili UAC uloge traju samo dok traje sjednica, ali podjela tko je UAC, a tko UAS nije stroga jer u svakom trenutku bilo koja strana može poslati zahtjev te tako postati UAC. U fiksnoj telefoniji korisnike se poziva u sjednicu pomoću njihovog telefonskog broja. U SIP

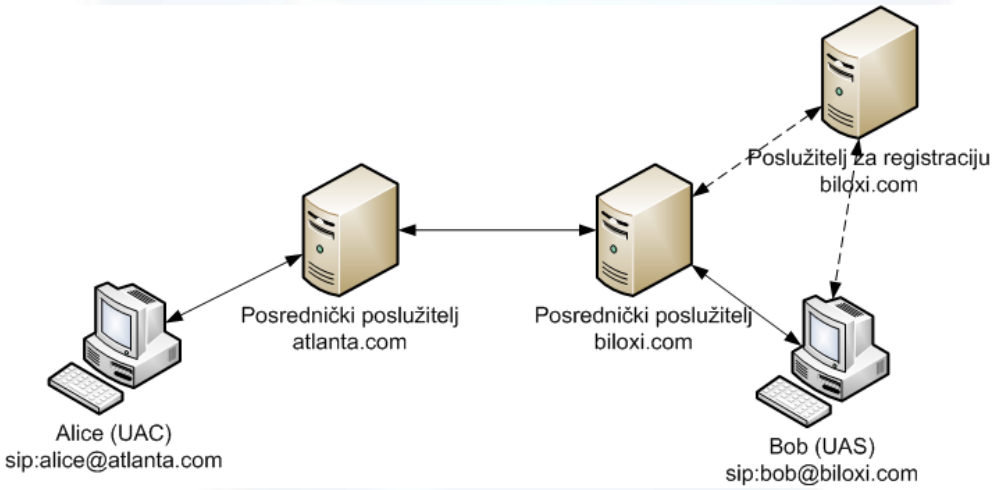
sjednicama se svakom UA dodjeljuje jedinstveni identifikator koji je u URI (eng. *Uniform Resource Identifier*) obliku. Karakterističan SIP URI je oblika:

```
sip:[korisničko ime]:[lozinka]@[domena]:[priključnica]
```

Ako se SIP poruke šifriraju, umjesto prefiksa „*sip:*", koristi se prefiks „*sips:*". Za pozivanje korisnika u sjednicu, nužno je poznavati njihov URI. Korisnici dobivaju svoj jedinstveni SIP URI registracijom. U tu svrhu se koriste poslužitelji za registraciju koji registriraju korisnike unutar domene za koju su zaduženi. Također, oni održavaju podatke o korisnicima i njihovim trenutnim adresama unutar domene u bazi koja se zove lokacijski poslužitelj.

Posredničke poslužitelje se može shvatiti kao SIP usmjeritelje. Oni primaju zahtjeve od korisničkih agenata ili drugih posredničkih poslužitelja i usmjeravaju zahtjeve prema njihovom odredištu. Posrednički poslužitelji su potrebni zato što UAC ne zna IP adresu UAS-a, nego samo njegov SIP URI. Zbog toga je potreban dodatni mrežni element koji će SIP URI povezati s pravom IP adresom (kako bi se SIP poruka poslala pravom primatelju). Posrednički poslužitelj na temelju domene u SIP URI adresi traži posrednički poslužitelj zadužen za tu domenu. To je moguće ostvariti, primjerice, DNS upitom. Kada poslužitelj sazna njegovu adresu, prosljeđuje primljeni zahtjev do sljedećeg posredničkog poslužitelja. Ako se u SIP URI adresi nalazi domena samog poslužitelja, onda poslužitelj mora potražiti odredišnu adresu u bazi koja se naziva lokacijski poslužitelj. U toj bazi su zapisane trenutne IP adrese za svakog SIP korisnika koji se nalazi u poslužiteljevoj domeni.

Zadnji mrežni element je poslužitelj za preusmjeravanje. Ovaj poslužitelj prihvaća zahtjeve za pokretanje sjednice, ali zahtjeve ne prosljeđuje dalje nego vraća adresu odgovarajućeg poslužitelja koji je zadužen za traženu domenu.



Slika 3. Neki mrežni elementi SIP protokola

3.3.2. SIP poruke

Budući da je SIP po dizajnu sličan HTTP-u, SIP poruke se mogu podijeliti u dvije skupine: zahtjevi i odgovori. Zahtjeve šalje klijent (UAC), a odgovore poslužitelj (UAS). Svi SIP zahtjevi započinju sljedećom sintaksom:

```
Method SP Request-URI SP SIP-Version CRLF
```

Zahtjevi započinju metodom koja opisuje vrstu zahtjeva, a metode mogu biti:

- REGISTER – služi za povezivanje trenutne IP adrese korisničkog agenta sa SIP URI adresom.
- INVITE – zahtjev za pokretanjem SIP sjednice.
- ACK – potvrda uspostave sjednice. Dolazi u paru sa zahtjevom INVITE.

- CANCEL – zahtjev koji prekida obradu prethodnog zahtjeva.
- BYE – koristi se za raskid sjednice, a zbog sigurnosnih razloga mogu ga poslati samo korisnički agenti koji sudjeluju u sjednici (ne posrednički poslužitelj ili korisnički agent koji nije sudionik sjednice).
- OPTIONS – provjera mogućnost primatelja.

Nakon navođenja metode slijedi razmak (SP) nakon kojeg dolazi SIP URI primatelja zahtjeva. Ostatak zahtjeva čini još jedan razmak, inačica SIP-a i kraj retka (CRLF). U retcima ispod mogu se nalaziti dodani podaci o zahtjevu što će biti objašnjeno na primjeru INVITE zahtjeva (primjer preuzet iz RFC 3261 [6]). Na ovom primjeru će biti objašnjen najčešći način pokretanja sjednice pomoću SIP protokola.

Promatrat će se uspostavljanje sjednice između dva korisnika: Alice i Bob. Mrežni elementi koji se koriste su prikazani na slici 3. SIP URI kojeg posjeduje Alice je *sip:alice@atlanta.com*, a registriran je na poslužitelju za registraciju zaduženom za domenu *atlanta.com* korištenjem SIP poruke REGISTER. Na isti način je Bob registrirao svoj SIP URI sip:bob@biloxi.com, ali na poslužitelju za registraciju zaduženom za domenu biloxi.com (poslužitelj za registraciju u domeni *atlanta.com* nije prikazan na slici). U ovom scenariju Alice poziva Boba u sjednicu, što znači da će Alice biti UAC, a Bob UAS iako je to zapravo samo logička podjela, jer i Bob u nekom trenutku može početi slati zahtjeve. Pozivanje sudionika sjednice se obavlja slanjem zahtjeva INVITE na odgovarajući SIP URI. Zahtjev koji šalje Alice je prikazan u nastavku:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

v=0
...
```

Svaki SIP zahtjev sastoji se od zaglavlja i tijela. Zaglavlje započinje oznakom metode (INVITE) te SIP URI adresom korisnika kojeg se poziva u sjednicu (*sip:bob@biloxi.com*). U sljedećim retcima se nalazi još nekoliko polja zaglavlja koja daju dodatne informacije o metodi INVITE:

- *Via* – adresa poslužitelja od kojeg Alice očekuje odgovore na svoje zahtjeve. To je adresa posredničkog poslužitelja zaduženog za domenu *atlanta.com*. Svaki posrednički poslužitelj na putu kojim prolazi zahtjev dodaje novo polje *Via* kako bi se odgovor vratio putem kojim je došao zahtjev.
- *Max-Forwards* – dozvoljeni broj skokova zahtjeva prije nego dođe do odredišta.
- *To* – ime primatelja (Bob) i njegov SIP URI.
- *From* – ime pošiljatelja (Alice) i njegov SIP URI.
- *Call-ID* – globalno jedinstveni identifikator sjednice nastao kombinacijom nasumično odabranog niza znakova i domene pošiljatelja.
- *CSeq* – brojač koji se povećava svakim slanjem zahtjeva s istim *Call-ID.*
- *Contact* – SIP URI s kojim ostali mrežni elementi znaju gdje slati svoje zahtjeve (za razliku od polja *Via* koje definira gdje se šalju odgovori).
- *Content-Type* – opis tijela zahtjeva (u ovom slučaju se nagoviješta korištenje SDP protokola za opis sjednice, ali dopuštene su i druge vrijednosti).
- *Content-Length* – veličina tijela zahtjeva u oktetima.

Nakon njih, dolazi tijelo zahtjeva u kojem je opis sjednice zapisan u SDP formatu. Poruka INVITE se osim za pokretanje sjednice može koristiti i za njenu izmjenu. Takva se poruka

naziva re-INVITE, ali polja u zaglavlju poruke se ne mijenjaju u odnosu na izvorni INVITE zahtjev. Izmjene se događaju samo u tijelu poruke (SDP opisu). Detaljan opis ostalih polja u SIP zahtjevima te koja polja je moguće koristiti u pojedinim zahtjevima moguće je pronaći u specifikaciji RFC 3261 [6].

INVITE zahtjev Alice šalje posredničkom poslužitelju zaduženom za domenu *atlanta.com* koji će se pobrinuti da zahtjev stigne do Boba. Nakon slanja zahtjeva, Alice očekuje odgovor koji ima sintaksu sličnu odgovorima kod HTTP protokola:

```
SIP-Version SP Status-Code SP Reason-Phrase CRLF
```

SIP odgovori se mogu svrstati u šest skupina, ovisno o prvoj znamenci u polju *Status-Code*:

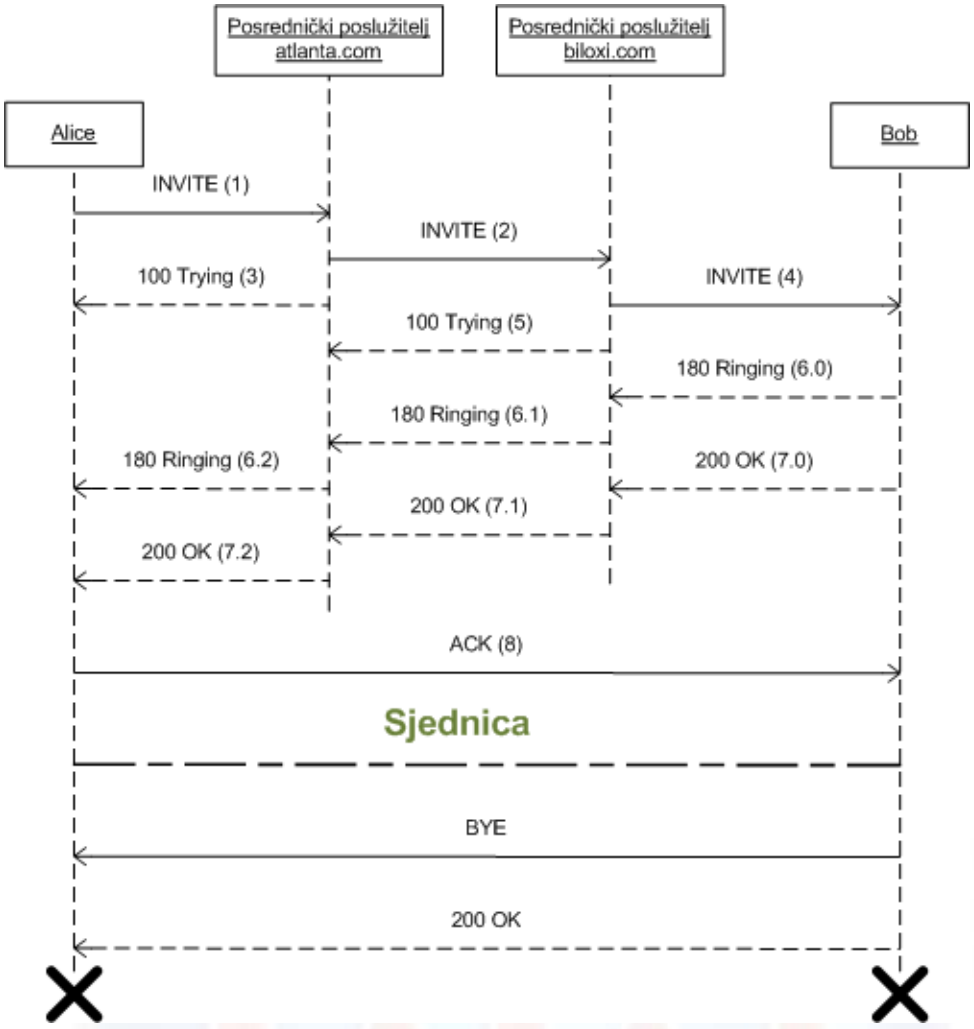
- 1xx – informativni odgovor. Označava da je zahtjev zaprimljen i da se obrađuje.
  - Npr: 100 *Trying*, 180 *Ringing*, 181 *Call Is Being Forwarded*
- 2xx – uspješno izvršen zahtjev.
  - Npr. 200 OK
- 3xx – dodatne akcije su potrebne (najčešće se radi o preusmjeravanju).
  - Npr. 301 *Moved Permanently*, 302 *Moved Temporarily*
- 4xx – greška na klijentu (sintaksna pogreška ili sl.).
  - Npr. 400 *Bad Request*, 401 *Unauthorized*, 404 *Not Found*, 407 *Proxy Authentication Required*
- 5xx – greška na poslužitelju (poslužitelj ne može izvršiti zahtjev).
  - Npr. 500 *Internal server error*
- 6xx – globalna pogreška.

  Npr. 600 *Busy Everywhere*, 603 *Decline*

Nakon što su objašnjeni zahtjevi i odgovori, može se dovršiti primjer uspostavljanja sjednice pomoću SIP-a. Radi lakšeg praćenja, Slika 4 prikazuje slijedni dijagram koji prikazuje razmjenu SIP poruka između svih mrežnih elemenata u primjeru.

Pokretanje sjednice:

1. Prva poruka INVITE koju Alice šalje svom nadležnom posredničkom poslužitelju je detaljno objašnjena u prethodnim odlomcima. U fiksnoj telefoniji je ovaj korak ekvivalentan postupku biranju broja.
2. Nakon toga posrednički poslužitelj domene *atlanta.com* prosljeđuje INVITE poruku do posredničkog poslužitelja domene *biloxi.com*. Njegovu adresu je saznao pomoću posebnog DNS upita ili na neki drugi način. Prije prosljeđivanja zahtjeva, dodaje još jedno polje *Via* u koje upisuje svoju adresu.
3. Kao odgovor na zahtjev INVITE kojeg je poslala Alice, posrednički poslužitelj šalje informativni odgovor 100 *Trying* kojim obavještava Alice da je zaprimio njen zahtjev i trenutno ga obrađuje.
4. Posrednički poslužitelj iz *biloxi.com* domene zaprima INVITE zahtjev i kreće u njegovu obradu. Na temelju polja *To* zaključuje da je korisnik kojem je namijenjen poziv u njegovoj domeni, ali poslužitelj ne zna korisnikovu IP adresu. Kako bi ju saznao, konzultira se s poslužiteljem za registraciju koji u sebi sadrži lokacijski poslužitelj. Prije nego proslijedi INVITE zahtjev do Boba, dodaje još jedno polje *Via* u koje upisuje svoju adresu.
5. Kao i u koraku 3, posrednički poslužitelj *biloxi.com* domene šalje poruku 100 *Trying* posredničkom poslužitelju *atlanta.com* domene.
6. U ovom koraku zahtjev INVITE je došao do Bobovog korisničkog agenta i čeka se na Bobovo javljanje. U fiksnoj telefoniji je ovaj slučaj ekvivalentan zvonjenju telefona prije nego se druga strana javi. Zbog toga se prosljeđuju informativni odgovori 180 *Ringing* do Alice kako bi se simulirala zvonjava telefona. Odgovori putuju istim putem kojeg je prolazio zahtjev INVITE, a put je moguće rekonstruirati zbog toga što su svi čvorovi na putu dodavali polje *Via*.



Slika 4. Slijedni dijagram uspostavljanja sjednice između Alice i Boba

7. Ako se Bob javi na poziv, do Alice se prosljeđuju poruke 200 OK. Na taj način Alice zna da je Bob odgovorio na njen poziv. U protivnom bi do Alice došla neka od poruka greške i sjednica ne bi bila pokrenuta. U tijelu poruke 200 OK nalazi se opis sjednice u SDP formatu. Na taj način se ostvaruje pregovaranje o parametrima sjednice. Sadržaj poruke 200 OK koju šalje Bob je prikazan u nastavku. Potrebno je obratiti pozornost na broj i sadržaj polja *Via*.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP server10.biloxi.com
     ;branch=z9hG4bKnashds8;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com
     ;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com
     ;branch=z9hG4bK776asdhds ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131

v=0
...
```

8. Zadnji korak prije uspostavljanja sjednice je slanje poruke ACK. Tu poruku šalje Alice Bobu potvrđujući parametre sjednice koje je on poslao u „200 OK“ poruci. Ova poruka se više ne šalje preko posredničkih poslužitelja, nego izravno na Bobovu adresu. Zbog polja *Contact*, korisnički agenti su saznali međusobne adrese i nema više potrebe za posredničkim poslužiteljima (oni se koriste na početku zato što Alice nije znala Bobovu adresu nego samo SIP URI). Nakon što Bob primi ACK poruku, sjednica je uspostavljena i može započeti razmjena paketa na način kako je to dogovoreno u SDP opisu sjednice. Važno je naglasiti da u razmjeni paketa sjednice ne sudjeluju posrednički poslužitelji.

Prekid sjednice:

1. Sjednicu može prekinuti isključivo neki od korisničkih agenata zbog sigurnosnih razloga. Neka u ovom slučaju sjednicu prekida Bob. Sjednica se prekida slanjem zahtjeva BYE s kraja na kraj sjednice (u ovom slučaju od Boba do Alice). Zahtjev BYE i dalje zaobilazi posredničke poslužitelje i dolazi izravno do Alice.
2. Alice potvrđuje primitak zahtjeva slanjem odgovora „200 OK“ Bobu. Nakon što Bob primi odgovor, sjednica se prekida.

4. Sigurnosni problemi

Budući da se opisane sjednice temelje na prijenosu paketa IP mrežama, sigurnosni problemi koji se javljaju su uobičajeni sigurnosni problemi u Internetu poput DoS (eng. *Denial of Service*) napada, *spoofinga* i *sniffinga*. Ostali sigurnosni problemi su:

- **Preuzimanje identiteta** – napadač se može lažno predstavljati ili kao sudionik sjednice ili kao neki od ključnih mrežnih elemenata sjednice. Primjer ovakvog napada u SIP-u je lažno predstavljanje napadača kao poslužitelja za preusmjeravanje. Primjerice, korisnički agent A šalje zahtjev za uspostavljanje sjednice korisničkom agentu B. Zahtjev dolazi do poslužitelja za preusmjeravanje koji bi trebao biti 'pošten' i dati točnu adresu poslužitelja koji je odgovoran za domenu korisničkog agenta B. Ukoliko je poslužitelj za preusmjeravanje napadnut ili su zahtjevi namijenjeni njemu preusmjereni na neki drugi poslužitelj, napadač može dati lažni odgovor o nadležnom poslužitelju za primateljevu domenu. Korisnički agent A ne zna da je odgovor lažan i poslat će svoje zahtjeve na lažni posrednički poslužitelj. Napadač to može iskoristiti za prikupljanje podataka o sjednici i njenim sudionicima ili za sljedeći korak napada.
- **Izmjena paketa sjednice** – napadač na neki način presreće pakete i proizvoljno ih mijenja. Presretanje paketa se može izvesti na način koji je opisan u prethodnoj točki. Izmjenom paketa sjednice moguće je utjecati na sjednicu kako bi se prikupili dodatni podaci o sudionicima sjednice.
- **Krađa sjednica** – napadač se predstavlja kao neki od sudionika sjednice i sudjeluje u sjednici umjesto pravog sudionika.
- **Prekid sjednica** – napadač može raskinuti sjednicu ako ima dovoljno podataka da pošalje poruku o raskidu sjednice tako da izgleda kao da je poruku poslao pravi sudionik sjednice. Napadi preuzimanja identiteta ili izmjene paketa sjednice također mogu rezultirati prijevremenim prekidom sjednice.
- **Prisluškivanje** – presretanje paketa sjednice jednom kada ona počne i sudionici počnu razmjenjivati pakete s, primjerice, audio i video sadržajem.
- **SPIT** (eng. *Spam over Internet Telephony*) – iako nije toliko raširen danas, predviđa se da će u budućnosti biti puno izraženiji kako VoIP bude sve popularniji. Uspostavljanje SIP poziva se može vrlo jednostavno automatizirati, a to olakšava slanje *spam* poruka. *Spam* u VoIP pozivima može korisnike jako smetati, čak i više od *spam* poruka elektroničke pošte, budući da VoIP *spam* uzrokuje zvonjenje virtualnog telefona. Zbog toga se već sada istražuju načini kako spriječiti *spam* u sjednicama.

Moguća rješenja nekih sigurnosnih problema će biti objašnjena na primjeru SIP protokola. SAP protokol ima mogućnost autentikacije, ali se njeno korištenje ne preporučuje zbog mogućeg zagušivanja mreže šifriranim SAP paketima koje primatelji ne mogu pročitati. SDP opis se koristi unutar SIP protokola, te svi sigurnosni mehanizmi koji štite SIP pakete ujedno štite i SDP opis.

Pri dizajnu SIP protokola više je pažnje posvećeno njegovoj jednostavnosti nego sigurnosti. Kako je protokol postajao raširenij, dodavana su nova pravila koja su uvodila podršku za različite vrste sjednica. To je rezultiralo brojnim izmjenama u RFC specifikacijama što otežava implementaciju SIP protokola. Ako se još k tome želi SIP sjednice osigurati od mogućih napada, implementiranje SIP protokola može biti veliki izazov.

Jedna od ranjivosti SIP protokola leži u korištenju običnog teksta u paketima koje izmjenjuju sudionici sjednice. Pakete je moguće vrlo jednostavno pročitati i izmijeniti podatke u njima te tako izvesti napad. SIP ima podršku za šifriranje teksta, ali ona nije obavezna i većina sjednica ne šifrira podatke. Čak i ako se koristi neka od podržanih zaštita poput IPsec, SSL/TLS ili S/MIME (objašnjeni kasnije), polja poput *To* i *Via* moraju ostati nešifrirana kako bi se SIP zahtjevi ispravno usmjeravali do odredišta. Napadači to mogu iskoristiti za slanje lažnih INVITE ili BYE zahtjeva kako bi započeli lažne SIP sjednice ili prekinuli postojeće.

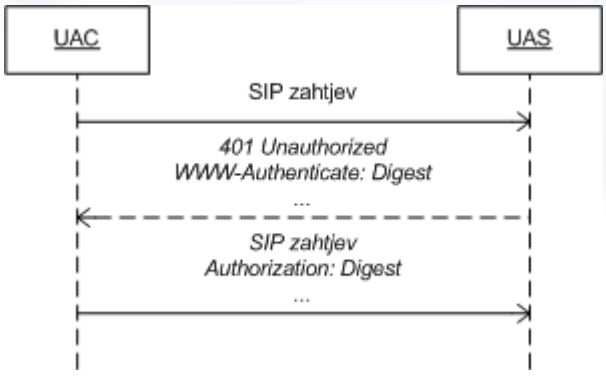
Nekoliko DoS (eng. *Denial of Service*) ranjivosti otkriveno je u načinu obrade INVITE zahtjeva kod nekoliko SIP aplikacija. Napadači ih mogu iskoristiti za rušenje aplikacije, a u nekim slučajevima i neovlašteni pristup napadnutom uređaju. Ranjivosti su bile posljedica neispravne implementacije SIP protokola u aplikaciji. Jedan od uzroka loše implementacije je velika složenost SIP protokola koji mora osigurati podršku za raznolike sjednice, a opet osigurati ograničenja kako ne bi došlo do zloupotrebe.

Nisu svi sigurnosni nedostaci SIP protokola posljedica lošeg dizajna protokola. Mnogi nedostaci su posljedica korištenja nesigurne arhitekture na kojoj se temelji Internet, korištenju UDP/IP protokola s kojim nije moguće osigurati ispravnu dostavu svih paketa, ali i programski izvedenih korisničkih agenata koji nemaju postavljena dovoljna ograničenja kao fiksni telefoni.

RFC 3261 definira nekoliko sigurnosnih mehanizama poput Digest autentikacija, S/MIME te korištenje TLS i IPsec.

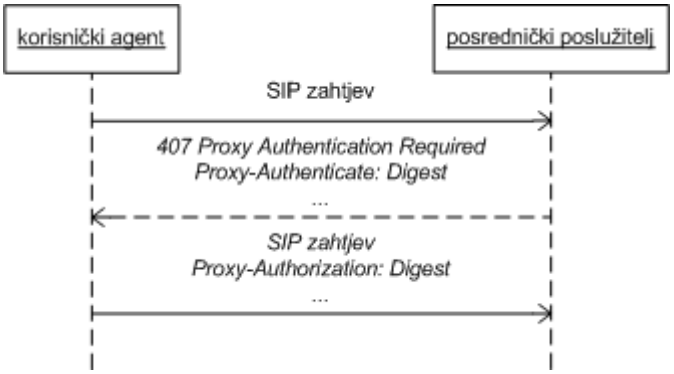
Digest autentikacijski mehanizam koriste HTTP poslužitelji kako bi s vremena na vrijeme provjerili autentičnost korisnika s kojim razmjenjuju pakete. Budući da SIP ima nekoliko zajedničkih značajki s HTTP-om, razumljivo je zašto je odabran ovaj način autentikacije i u SIP protokolu. Potrebno je naglasiti da Digest autentikacijski mehanizam ne osigurava integritet i povjerljivost SIP paketa, ali može onemogućiti lažno predstavljanje napadača kao jednog od mrežnih entiteta SIP protokola. Prema specifikaciji SIP protokola, dvije su vrste autentikacije u SIP protokolu:

1. **UAS traži autentikaciju UAC-a** (Slika 5): po primitku SIP zahtjeva UAS može provjeriti autentičnost drugog korisničkog agenta (svi zahtjevi osim ACK i CANCEL). Zahtjev za autentikaciju šalje pomoću odgovora 401 *Unauthorized* u kojeg uključuje polje *WWW-Authenticate*. Po primitku poruke 401, UAC šalje novi zahtjev s poljem *Authorization* u kojeg upisuje sve potrebne podatke za autentikaciju.



Slika 5. Postupak autentikacije između korisničkih agenata

2. **Posrednički poslužitelj traži autentikaciju korisničkog agenta** (Slika 6): slično kao u prethodnom slučaju, poslužitelj može provjeriti autentičnost korisničkog agenta koji je zahtjev poslao (također, bilo koji SIP zahtjev osim ACK i CANCEL). Poslužitelj šalje odgovor 407 *Proxy Authentication Required* s poljem *Proxy-Authenticate*. Po primitku poruke 407, korisnički agent šalje novi zahtjev s popunjenim poljem *Proxy-Authorization*.



Slika 6. Autentikacija između korisničkog agenta i posredničkog poslužitelja

Način provjere podataka u dobivenim porukama je identičan HTTP Digest sigurnosnom mehanizmu i detaljno je opisan u dokumentu RFC 2617.

S/MIME (eng. *Secure/Multipurpose Internet Mail Extensions*) je metoda šifriranja javnim ključem i digitalnim potpisom MIME podataka. SIP poruke su u obliku čistog teksta, zbog čega su ranjive na napade čitanja i izmjene podataka u paketima. S/MIME se može upotrijebiti za šifriranje poruke kako bi se očuvao njihov integritet i povjerljivost. Ovaj sigurnosni mehanizam koristi privatne i javne ključeve za šifriranje SIP poruka. Tijelo (ali ne i zaglavlje) SIP poruka se digitalno potpisuje privatnim ključem pošiljatelja poruke, a njegov javni ključ se može poslati zajedno s porukom. Ključna stvar je da se tijelo SIP poruke šifrira javnim ključem primatelja. Očito, pošiljatelji moraju poznavati ispravni javni ključ primatelja. Pažljivim odabirom korisnika kojima će se poslati javne ključeve sudionika sjednice moguće je spriječiti napade. Novi problem koji se javlja je sigurna distribucija javnih ključeva do krajnjih korisnika. U RFC 3261 se predlaže korištenje SIP poruka za razmjenu ključeva, a autentičnost poruka se treba provjeriti ispitivanjem dobivenih certifikata pomoći VA identiteta (eng. *Validation Authority*) kojem se vjeruje. U nastavku je primjer SIP poruke čije je tijelo šifrirano pomoću S/MIME standarda. Potrebno je primijetiti vrijednost u prvom polju *Content-Type* i šifrirani opis sjednice koji je ovdje napisan u obliku običnog teksta (kako bi čitatelj znao što piše), ali u stvarnosti je on šifriran i nečitljiv:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
      name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
      handling=required

*******************************************************
* Content-Type: application/sdp                       *
*                                                     *
* v=0                                                 *
* o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com *
* s=-                                                 *
* t=0 0                                               *
* c=IN IP4 pc33.atlanta.com                           *
* m=audio 3456 RTP/AVP 0 1 3 99                       *
* a=rtpmap:0 PCMU/8000                                *
*******************************************************
```

Prethodni opis korištenja S/MIME standarda je štitio samo tijelo SIP poruke, ali ne i njeno zaglavlje. Ako se S/MIME koristi za šifriranje cijele SIP poruke, uključujući i njeno zaglavlje, govori se o tuneliranom SIP-u. Pomoću S/MIME postupka digitalno se potpiše ili šifrira cijela SIP poruka, a onda

se rezultat umeće u novu SIP poruku kao njeno tijelo. Zaglavlje nove SIP poruke se popunjava s istim vrijednostima kao u staroj SIP poruci. Na taj način primatelj može otkriti je li došlo do neželjenih izmjena u zaglavlju SIP poruke. Povjerljivost podataka se može osigurati do neke mjere, jer polja poput *To* i *From* moraju ostati nešifrirana (kako bi se paketi mogli usmjeravati kroz mrežu).

Na početku ovog potpoglavlja spomenuto je kako dio sigurnosnih ranjivosti SIP protokola leži u korištenju nesigurne TCP-UDP/IP Internet arhitekture. Za rješavanje tog problema predlaže se korištenje sigurnosnih mehanizama TLS i IPsec na transportnom i mrežnom sloju.

5. Zaključak

Sjednice su vrlo važne u komunikaciji putem Interneta. Zbog toga je posebna pažnja posvećena razvoju protokola za podršku sjednice. Protokoli moraju pružati podršku za vrlo raznovrsne sjednice, a ujedno pružati dovoljnu razinu sigurnosti od mogućih napada na sjednice što može predstavljati veliki izazov pri dizajnu i implementaciji takvih protokola. Kako bi se omogućila raznovrsnost u podržanim sjednicama, dizajniran je poseban protokol za opis sjednice nazvan SDP. On propisuje format za opis sjednice, a moguće ga je koristiti unutar drugih protokola za podršku sjednice poput SAP i SIP protokola. Ova dva protokola se koriste za objavljivanje i pokretanje sjednice, s tim da se SAP protokol koristi kada sudionici sjednice nisu unaprijed poznati, a SIP kada su poznate adrese sudionika sjednice. Protokoli ujedno podržavaju i izmjene sjednice poput izmjene parametara te pozivanja novih sudionika u sjednicu, a definiraju i način raskida sjednice.

Sigurnost sjednice je vrlo važna budući da napadači mogu doći do osjetljivih informacija ukoliko, primjerice, prisluškuju sjednicu, a informacije mogu iskoristiti za daljnje napade na računala sudionika sjednice. Najčešći sigurnosni mehanizmi su autentikacija korisnika mehanizmima tajnih i javnih ključeva te šifriranjem sadržaja paketa. Ovim sigurnosnim mehanizmima sprječavaju se napadi krađe identiteta, prisluškivanja i izmjene paketa. Ipak, sigurnost sjednica je i dalje veliki problem te je potrebno dodatno istraživanje na tom području.

6. Leksikon pojmova

Kolačić (Kolačić datoteka)

Datoteka koja sadrži podatke o posjeti web stranici. Na taj način vlasnici *web* stranice rade statistiku posjeta. Kolačić također pamti neke postavke koje ste namjestili i podatke koje ste upisali na posjećenoj stranici (npr. lozinku).

http://www.httpwatch.com/httpgallery/cookies/

DOS napad (Napad uskraćivanjem usluge)

Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad.

http://searchsoftwarequality.techtarget.com/definition/denial-of-service

TCP (Transmission Control Protocol)

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela.

http://www.webopedia.com/TERM/T/TCP.html

IP (IP protokol - Internet Protocol)

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

IPsec (IPsec protokol - Internet Protocol Security)

IPsec je standard i skup protokola (opcionalan za IPv4, a obavezan za IPv6) koji obuhvaća mehanizme za zaštitu prometa na razini trećeg sloja OSI modela - kriptiranjem i/ili autentifikacijom IP paketa. IPsec osigurava tajnost, autentičnost, raspoloživost i besprijekornost.

http://technet.microsoft.com/en-us/network/bb531150

IETF (Internet Engineering Task Force)

IETF je skupina koja razvija i promiče standarde u Internetu, a surađuje s W3C i ISO/IEC standardizacijskim tijelima. Svi članovi su volonteri i ne postoji službeno članstvo.

http://www.webopedia.com/TERM/I/IETF.html

HTTP (HTTP protokol)

HyperText Transfer Protocol - Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. *web* stranica). HTTP je *request/response* protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je *web* preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim *web* poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju.

http://hr.wikipedia.org/wiki/HTTP http://www.w3.org/Protocols/

RTP (Real-time Transport Protocol)

RTP definira standardizirani format paketa za dostavu audio i video sadržaja preko IP mreža. Koristi se u komunikacijskim sustavima i sustavima za zabavu koji uključuju dohvati različitih vrsta medija (zvuk, video, sintetički sadržaj...).

http://searchnetworking.techtarget.com/definition/Real-Time-Transport-Protocol

URI (Uniform Resource Identifier)

URI je niz znakova koji se koristi za identifikaciju imena ili nekog drugog resursa na Internetu. URI sintaksa započinje URI shemom (npr. http, ftp, mailto, sip), nakon čega slijedi dvotočka i niz znakova koji ovisi o odabranoj shemi.

http://searchsoa.techtarget.com/definition/URI

SAP (Session Announcement Protocol)

Protokol za objavu sjednice i njenog opisa. Pokretač sjednice periodički šalje objavu sjednice, a potencijali sudionici sjednice osluškuju unaprijed poznatu priključnicu i IP adresu. Ukoliko su zainteresirani, mogu se pridružiti sjednici.

http://tools.ietf.org/html/rfc2974

SDP (Session Description Protocol)

Protokol koji definira format za opis sjednice. Ne koristi se za pokretanje sjednice i dostavu medijskih paketa nego za pregovaranje o tipovima medijskih podataka, formatima i ostalim parametrima.

http://searchunifiedcommunications.techtarget.com/definition/SDP

SIP (Session Initiation Protocol)

SIP protokol se koristi za uspostavu, izmjenu i raskid sjednice između dva ili više sudionika koje koriste jedan ili više medijskih struja podataka. SIP koristi mehanizam zahtjeva i odgovora slično kao HTTP, a može raditi zajedno s nekoliko drugih protokola poput SDP protokola.

http://searchunifiedcommunications.techtarget.com/definition/Session-Initiation-Protocol

TLS (Transport Layer Security)

TLS je kriptografski protokol koji pruža sigurnu komunikaciju Internetom. TLS šifrira dijelove iznad transportnog sloja koristeći simetrične kriptografske ključeve i autentikacijski kod poruka. TLS je nasljednik SSL protokola.

http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS

VoIP (Voice over IP)

VoIP je skup internetskih tehnologija, komunikacijskih protokola i tehnologija prijenosa kako bi se ostvario prijenos govora preko IP mreže. VoIP koristi protokole za podršku sjednice poput SIP-a i SAP-a za uspostavljanje i raskid sjednica, tj. poziva.

http://voip.about.com/od/voipbasics/a/whatisvoip.htm

DNS (Domain Name System)

Domain Name System (DNS) je hijerarhijski sustav imenovanja izgrađen na distribuiranim bazama podataka za računala, usluge ili bilo koji resurs spojen na Internet ili privatnu mrežu.

http://www.kb.iu.edu/data/adns.html

7. Reference

[1] Wikipedia: Session (computer science), http://en.wikipedia.org/wiki/Session_(computer_science), svibanj 2011.

[2] Wikipedia: Session Description Protocol, http://en.wikipedia.org/wiki/Session_Description_Protocol, svibanj 2011.

[3] RFC 4566: SDP: Session Description Protocol, http://tools.ietf.org/html/rfc4566, srpanj 2006.

[4] RFC 2974: Session Announcement Protocol, http://www.ietf.org/rfc/rfc2974.txt, listopad 2000.

[5] Wikipedia: Session Initiation Protocol, http://en.wikipedia.org/wiki/Session_Initiation_Protocol, svibanj 2011.

[6] RFC 3261: SIP: Session Initiation Protocol, http://tools.ietf.org/html/rfc3261, lipanj 2002.

[7] RFC 3329: Security Mechanism Agreement for the Session Initiation Protocol (SIP), http://www.rfc-editor.org/rfc/rfc3329.txt, siječanj 2003.