Primena XML interfejsa u integraciji korisničkih naloga u okviru IP telefonije

Dragan Marković, Marko Džida

***Sadržaj* — Zbog raširene primene IP telefonije u poslovnim sistemima, koja po pravilu koristi infrastrukturu klasične računarske mreže, kao i gotovo neizbežne primene računara u skoro svakom poslovnom okruženju, razvijena je aplikacija koja integriše korisničke kredencijale računara i IP telefona u okviru jedinstvenog prijavljivanja na sistem i odjavljivanja sa njega. Uvođenjem aplikacije može se postići višestruka korist, u smislu smanjenja troškova, kontrole pristupa resursima i dr.**

***Ključne reči* — CDP, Extension Mobility, LDAP, LLDP, Unified Communications, XML.**

I. UVOD

U savremenim rešenjima iz oblasti IP telefonije, teži se što boljoj integraciji govora, podataka i multimedijalnih sadržaja, kroz upotrebu iste infrastrukture, najčešće i istim fizičkim putem do krajnjeg korisnika. Tako se u većini trenutnih komercijalnih VoIP rešenja IP telefonski aparat uvodi kao veza između računara i ostatka IP mreže (Sl. 1), kako bi se povezivanje praktično dva IP uređaja u mrežu izvršilo preko jednog kabla i jednog porta na odgovarajućem sviču. U ovakvim konfiguracijama, koje su uobičajene u poslovnim primenama, krajnji korisnik po pravilu ima zaštićen računarski nalog, dok je IP telefon često ili potpuno nezaštićen od neovlašćenog korišćenja ili ima posebne kredencijale za pristup, pa je potreban praktično dupli unos *username/password* podataka. Ovakav pristup oduzima vreme korisnika ili predstavlja mogući izvor neovlašćenog pristupa.

U ovom radu prikazano je jedno moguće rešenje uvođenjem aplikacije koja integriše računarske i telefonske kredencijale korisnika. Njenom primenom izbegavaju se dvostruka prijavljivanja i odjavljivanja sa računarskog i telefonskog sistema, bez kompromisa na račun bezbednosti nekog od njih. Zbog značaja i boljeg razumevanja najpre je opisana *Cisco Extension Mobility (EM)* funkcionalnost [1], koja je osnova za razvoj aplikacije opisane u radu, a zatim način rada same aplikacije, kroz algoritam i XML [2] poruke, koje predstavljaju glavne komunikacione interfejse EM-a.

Dragan Marković, dipl.el.inž, SAGA d.o.o., Milentija Popovića 9, Sava Centar, 11000 Beograd, Srbija (telefon: 381-64-860-6270; e-mail: dragan.markovic@saga.rs).

Marko Džida, dipl.el.inž. - master, SAGA d.o.o., Milentija Popovića 9, Sava Centar, 11000 Beograd, Srbija (telefon: 381-64-860-6206; e-mail: marko.dzida@saga.rs).

II. OSNOVA SISTEMA

Aplikacija je razvijena na *Cisco Unified Commucations Manager* (CUCM) platformi. CUCM je skalabilno, distributivno poslovno rešenje visoke pouzdanosti za procesiranje poziva u IP telefoniji [2]. Pored standardnih karakteristika zajedničkih za većinu IP rešenja ove vrste, podržava različite interfejse za masovno konfigurisanje (*provisioning*), pozivanje *feature*-a, nadgledanje i kontrolu IP telefonskih aparata u sistemu. Dostupni su sledeći interfejsi:

- *Administration XML*,
- *Extension Mobility* servis, koji je ovde od značaja.

Extension Mobility (u daljem tekstu EM) omogućava IP telefonskim aparatima da privremeno preuzmu kompletnu konfiguraciju, uključujući sopstvene linije (brojeve telefona), tastere za brzo biranje, servise i sl. Ova konfiguracija označava se kao profil uređaja (*device profile*) i predstavlja vrstu šablona za fizički uređaj, sa svim potrebnim atributima osim onih koji su su vezani za konkretni telefonski aparat, poput MAC adrese, informacije o lokaciji uređaja i sl. Na CUCM sistemu, analogno korisnicima računara u korporativnoj mreži, definišu se korisnički nalozi i povezuju sa određenim profilima uređaja.

Dve osnovne funkcije EM rešenja sastoje se od autentifikacije korisnika koji se prijavljuje i generisanja konfiguracionog fajla iz informacija o korisniku, koji se potom učitava na konkretnom telefonskom aparatu.

Podršku za *Extension Mobility* servis na *Cisco Unified Call Manager* sistemu čine aplikacioni i servisni modul, koji zajedno sa infrastrukturom CUCM-a, u okviru koje su DBL (*Database Layer*), korisnički direktorijum kao interni ili eksterni LDAP (*Lightweight Directory Access Protocol*) direktorijum, TFTP (*Trivial File Transfer Protocol*) server, obezbeđuju *Extension Mobility* funkcionalnost [2].

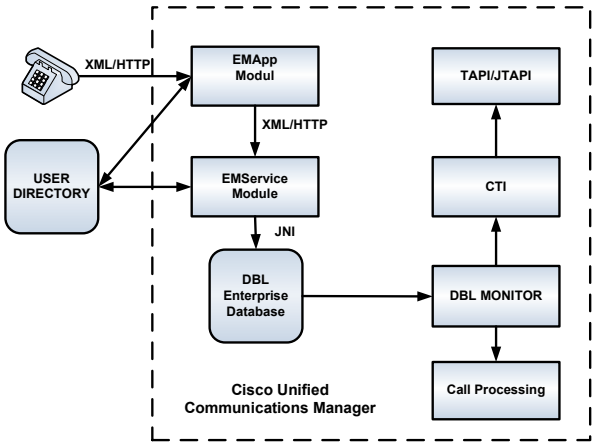
Arhitektura sistema može se grubo podeliti na tri komponente.

Aplikacioni modul prihvata XML zahteve preko HTTP (*Hyper Text Transfer Protocol*) POST poruka za prijavljivanje i odjavljivanje korisnika sa IP telefona i odgovara HTTP porukama ka IP telefonima. Modul proverava korisničko ime (*user ID*) i šifru, konsultujući lokalni korisnički direktorijum, lokalnu bazu podataka ili spoljni direktorijum, kao što je LDAP. Ukoliko su kredencijali validni, komunicira sa servisnim modulom u ime telefona. Nakon uspešne interakcije sa servisnim

modulom, obaveštava telefon o potrebi da se ponovo pokrene sa novom konfiguracijom.

Servisni modul prihvata XML/HTTP zahteve od aplikacionog u cilju formiranja novog konfiguracionog fajla. Servisni modul obezbeđuje informacije poput identiteta uređaja i profila uređaja za određenog korisnika koji se prijavljuje u sistem. U cilju slanja konfiguracionog fajla za IP telefon na TFTP server, obraća se sloju baze podataka (DBL) preko JNI (*Java Native Interface*).

Sloj baze podataka (*Database Layer*, *DBL*) prihvata zahteve od servisnog modula i generiše novi konfiguracioni fajl. Podaci o profilu uređaja, kao i o konkretnom telefonskom aparatu na kom će biti primenjen, predstavljaju osnovu za formiranje konfiguracionog fajla. Nakon generisanja, novi konfiguracioni fajl šalje se CUCM bazi podataka, a modul za procesiranje poziva obaveštava se o promeni. Ovo obaveštenje rezultuje slanjem novog konfiguracionog fajla na TFTP server, odakle ga preuzima fizički IP telefon [3].



Sl. 1. Arhitektura *Extension Mobility* funkcionalnosti.

A. *Postupak prijavljivanja/odjavljivanja*

Extension Mobility API (*Application Programming Interface*) predstavlja XML interfejs zasnovan na HTTP komunikaciji. Kao tačka pristupa ovom API-ju određuje se *web* stranica preko koje se šalju svi zahtevi i upiti kroz URI-je.

XML poruka šalje se kao HTTP POST. Polje "xml" sadrži XML string koji definiše upit ili zahtev. Odgovor IP centrale predstavlja čistu XML poruku sa indikatorom bilo uspeha bilo neuspeha u slučaju zahteva, odnosno odgovor u slučaju upita.

Aplikacija za prijavljivanje šalje XML poruku ka *EMService* servletu preko HTTP-a. *EMService* koristi LDAP direktorijum da proveri *userID* i PIN, poslate u okviru poruke. Ako su *userID* i PIN ispravni *EMService* izvršava zahtev komunikacijom sa DBL preko JNI.

Ukoliko DBL promeni profil uređaja na osnovu *login/logout* zahteva, obaveštava o tome DBL monitor, koji prosleđuje informaciju CTI (*Computer Telephony Interface*) modulu i modulu za procesiranje poziva, koji telefonu šalje signal da treba da se resetuje kako bi učitao novu konfiguraciju.

CTI sloj obraća se JTAPI ili TAPI aplikacijama koje prate uređaje i korisnike sa porukom da se kontrolna lista promenila.

Ukoliko DBL uspešno izvrši transakciju, obaveštava *EMService*, koji XML porukom odgovara lokalnoj aplikaciji da je operacija uspešno izvršena.

Lokalna aplikacija komunicira sa *Extension Mobility* servisom preko *EmService* komponente. Kada ova komponenta primi HTML poruku od aplikacije za prijavljivanje, koristi HTTP da pošanje XML odgovor o uspešnosti izvšenja operacije.

B. *Autentifikacija*

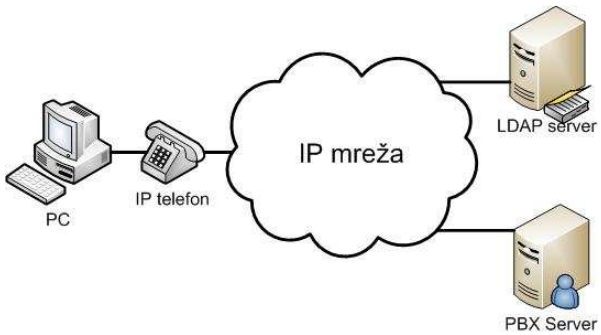
Extension Mobility servis dozvoljava autentifikaciju preko posrednika (*proxy*). Preciznije, korisnik sa posebnim (administrativnim) pravima može da uloguje bilo kog drugog korisnika na bilo koji uređaj, pod pretpostavkom da je EM servis ispravno konfigurisan. Ova funkcija pruža mogućnost da posebna aplikacija bude odgovorna za autentifikaciju na način na koji to najviše odgovara njenom dizajneru: korišćenjem šifre, PIN-a, hardverskog ključa, biometrijskih podataka i td.

Sama aplikacija mora da obezbedi kredencijale koje zahteva *Extension Mobility* servis. **Upravo ova funkcionalnost je iskorišćena u razvoju aplikacije opisane u nastavku.**

Potreban uslov je konfiguranje posebnog korisnika u direktorijumu, namenjenog za aplikaciju, koji ima standardne LDAP kredencijale – korisničko ime i PIN, i koji će svoje kredencijale koristiti da bi prijavio ili odjavio drugog korisnika sa fizičkog uređaja.

III. Opis aplikacije

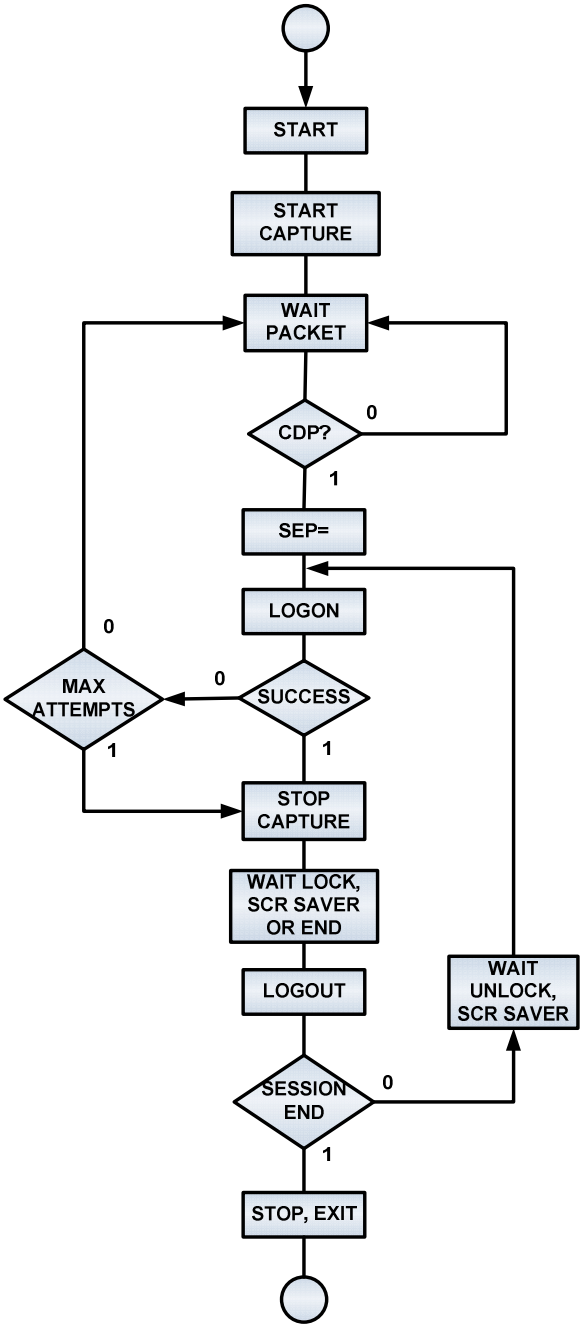
U konfiguraciji prikazanoj na Sl. 2., aplikacija na računaru (PC) sposobna je da, prateći saobraćaj na mrežnom interfejsu, prepozna upravo IP telefon na koji je PC direktno vezan, koristeći CDP (*Cisco Discovery Protocol*) [4] ili LLDP (*Link Layer Discovery Protocol*) [5]. Zbog opreme koja je poslužila u razvoju softvera, korišćen je CDP protokol.



Sl. 2. Standardni način povezivanja računara i IP telefona u mrežu.

Aplikacija se izvršava kao *Microsoft Windows* platformi kao servis - pokreće se sa podizanjem operativnog sistema računara, odnosno korisničkog naloga na sistemu, i nije vizuelna, tako da ne zahteva dodatnu pažnju krajnjeg korisnika. Na Sl. 3 prikazan je algoritam softvera, s

obzirom na ograničen prostor izlaganja, manju preglednost izvornog koda i činjenicu da ja aplikacija, iako razvijena u *Microsoft Visual C# .NET* okruženju [6], mogla biti napisana i u nekom drugom programskom jeziku/platformi. Za detektovanje CDP/LLDP paketa i uopšte pristup mrežnom intefejsu na drugom sloju OSI modela upotrebljeni su specijalizovana biblioteka *WinPcap* [6] i *SharpPcap* [8][9] API za pristup *WinPcap* funkcijama iz *Microsoft .NET* okruženja.



Sl. 3. Dijagram toka aplikacije.

Nakon startovanja, aplikacija je u stanju osluškivanja, čekajući na prijem CDP paketa. U slučaju prepoznavanja CDP-a, ispituje se polje *Devide ID* u okviru paketa. Polje se interpretira kao *string* (znakovni niz). Uslov za dalje procesiranje je da polje *Device ID* počinje sa "SEP", što je indikator da je uređaj koji je poslao CDP paket Cisco IP telefon. Ostatak ovog stringa predstavlja MAC adresu aparata, koja se u narednom koraku koristi za slanje XML *login* zahteva kroz HTTP POST ka IP centrali, tj. CUCM-u. Pored MAC adrese, ova poruka sadrži IP adresu centrale, korisničko ime naloga koji treba da se aktivira na aparatu, kao i korisničko ime i šifru posebnog korisnika koji je na centrali iskonfigurisan sa pravima da prijavljuje druge korisnike, što je objašnjeno u prethodnom delu teksta. Važan detalj predstavlja *username* korisnika koji treba da se aktivira na telefonu preko *Extension Mobility* interfejsa. Uslov da je *username Windows* naloga isti kao i na IP centrali, osim što pojednostavljuje održavanje oba sistema, važan je za rad aplikacije. Naime, *username* Windows naloga sama aplikacija automatski koristi za *username* naloga koji treba da se aktivira na telefonskom aparatu, kao i naziv *Device Profile*-a. Npr. *Windows* korisnik „petar" i na CUCM se registruje kao „petar".

Format XML zahteva za aktivaciju IP telefona sa nalogom "petar":

```
<request>
  <appInfo>
    <appID>posrednik</appID>
    <appCertificate>sifra_posrednika</appCertificate>
  </appInfo>
 <login>
   <deviceName>SEP003094C25B15</deviceName>
   <userID>petar</userID>
   <deviceProfile>petar</deviceProfile>
   <exclusiveDuration>
     <time>60</time>
     </exclusiveDuration>
 </login>
</request>
```

U XML zahtevu „posrednik" predstavlja pomenutog korisnika-administratora CUCM-a, koji ima prava da upravlja običnim korisnicima. Ovi kredencijali se ugrađuju šifrovani u sam kod aplikacije i isti su za sve instance aplikacije na ostalim računarima u sistemu.

Ukoliko je odgovor na *login* zahtev oblika:

```
<response>
  <success>
</response>
```

aplikacija prestaje sa osluškivanjem mreže i prelazi u stanje praćenja događaja na operativnom sistemu - odjavljivanje, zaključavanje, aktiviranje *screensaver*-a. Bilo koji od tih slučajeva je signal da treba odjaviti telefon, iz istog razloga iz kojih je i korisnik zaštitio svoj računar od neovlaščenog pristupa. Aktiviranje *screensaver*-a ukazuje na eventualnu odsutnost korisnika od računara, pa se iz predostrožnosti telefon odjavljuje. Treba napomenuti da se odjavljivanje telefonskog aparata ne izvršava dokle god postoji aktivan poziv, kako se otvorena veza ne bi prekinula. Zahtev za odjavljivanjem ima sledeću formu:

```
<request>
```

```
  <appInfo>
    <appID>posrednik</appID>
    <appCertificate>sifra_posrednika</appCertificate>
  </appInfo>
  <logout>
    <deviceName>SEP003094C25B15</deviceName>
  </logout>
</request>
```

U ovoj poruci nije potrebno slanje korisničkog imena i profila uređaja, već je dovoljna MAC adresa aparata koji se odjavljuje. Odgovor centrale ima isti format kao i kod *login* zahteva. U slučaju da je uzrok za odjavljivanje kraj sesije, aplikacija se zaustavlja, kako bi se korisnički nalog pravilno zatvorio. Ako je odjavljivanje telefona uzrokovano zaključavanjem naloga ili aktivavijom *screensaver*-a, aplikacija nastavlja da radi, čekajući ponovno otključavanje ili deaktivaciju *screensaver*-a, kada se postupak prijavljivanja na IP telefon ponavlja od „*login*“ bloka prikazanog na Sl. 3.

Slučaj zagušenja u mreži i drugi mogući problemi u komunikaciji sa IP centralom, obrađeni su višestrukim pokušajima prijavljivanja posle određenog vremenskog intervala. Ako ni tada prijavljivanje aparata preko *Extension Mobility* interfejsa ne uspe, aplikacija odustaje od daljih pokušaja i prestaje sa osluškivanjem paketa na mrežnom interfejsu, kako ne bi uticala na performanse rada računara.

IV. Zaključak

Prikazana aplikacija, razvijena na konkretnoj IP telefonskoj platformi, može se na sličnom konceptu i uz izvesna prilagođenja primeniti i na druge platforme, s obzirom na brojna napredna rešenja u ovoj oblasti. Iako potencijalno korisna, naročito u korporativnom okruženju, ovo je samo jedna od mogućih praktičnih primena programski dostupnih interfejsa modernih IP telefonskih sistema.

Literatura

[1] Extension Mobility API (EMAPI), Cisco Systems, http://developer.cisco.com/web/emapi/home (4.10.2010.)

[2] Extensible Markup Language (XML), World Wide Web Consortium (W3C), http://www.w3.org/XML/ (4.10.2010.)

[3] “Cisco Unified Communications Manager System Guide – Release 7.1(2)”, Cisco Systems, Inc. 2009.

[4] CDP Packet Format, Cisco Systems, http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/frames.htm#xtocid12, (4.10.2010.)

[5] 802.1AB, IEEE Standard for Local and metropolitan area networks, Station and Media Access Control Connectivity Discovery, Institute of Electrical and Electronics Engineers, 2005.

[6] Microsoft Visual Studio 2010 Express, http://www.microsoft.com/express/Windows/ (4.10.2010.)

[7] WinPCap, Windows Packet Capture Library, http://www.winpcap.org/ (4.10.2010.)

[8] http://sourceforge.net/projects/sharppcap/ (4.10.2010.)

[9] http://www.tamirgal.com/blog/page/SharpPcap.aspx (4.10.2010.)

Abstract

In widespread enterprise VoIP implementations, IP telephony systems typically rely on existing network infrastructure. In the manner of increasing integration of data, voice and multimedia traffic, an application was developed to unify PC and IP phone login credentials of a typical enterprise end user. The application based on Cisco Extension Mobility platform can bring multiple benefits in business implementations, reducing call costs, giving easier control of access, through additional level of VoIP integration. The concept can easily be adapted to other modern IP telephony solutions.

INTEGRATION OF END USER CREDENTIALS IN MODERN IP TELEPHONY SOLUTIONS USING XML INTERFACES

Dragan Marković, Marko Džida