Jedno rješenje posrednika u sistemu uslovnog pristupa digitalne televizije

Radenko Banović, Ilija Bašičević i Nemanja Lazukić

***Apstrakt*— Postoje dvije vrste TV (televizijske) usluge u domenu pretplate: javna (svima dostupan sadržaj za koji nije potrebna pretplata) i pretplatnička TV usluga (TV sadržaj je dostupan samo pretplaćenim korisnicima). Da bi pretplatnička TV usluga imala smisla potrebno je zaštititi TV sadržaj cijelim prenosnim putem. Postoji nekoliko modela zaštite pretplatničkog TV sadržaja, a jedan od njih je CAS (eng. Conditional Access System). Kompanija Widevine je kreirala rješenje sistema uslovnog pristupa (CAS) takvo da je besplatno za sve operatere. Da bi operateri mogli upravljati korisnicima i sadržajem, potrebno je implementirati korisničku upravljačku logiku sistema. U ovom radu je predstavljeno jedno rješenje softverskog posrednika (eng. Proxy) u kome je realizovana korisnička upravljačka logika sistema uslovnog pristupa u Widevine CAS sistemu.**

***Ključne reči*—Conditional Access System; Proxy; Digital Television;**

I. Uvod

Pretplatnička televizija je usluga koju nude satelitski, kablovski i drugi distributeri televizijskih kanala. Ključna tačka preduzetničkog modela u pretplatničkoj televiziji jeste zaštita televizijskog sadržaja cijelim prenosnim putem, od emitera do krajnjeg korisnika, čime se otklanja mogućnost pristupa sadržaju nepretplaćenim korisnicima[1]. Postoji nekoliko tehnologija zaštite televizijskog sadržaja, a najpoznatije su upravljanje digitalnim pravima (eng. Digital Rights Management) i sistem uslovnog pristupa (eng. Conditional Access System).

Sistem uslovnog pristupa predstavlja zaštitu prenosnog puta[2] (i on se najčešće koristi za televiziju uživo), dok je upravljanje digitalnim pravima zamišljeno kao mehanizam zaštite sadržaja (te se najčešće koristi za televiziju na zahtjev (eng. On Demand)). Za razliku od upravljanja digitalnim pravima, u sistemima uslovnog pristupa uobičajno je da se nakon određenog vremenskog intervala mijenjaju ključevi kojima je skremblovan sadržaj koji se dostavlja korisniku[3]. Kompanija Widevine je kreirala sopstveno rješenje CAS sistema za Android TV i Android STB (Set-Top Box) uređaje koje je napravilo veliki pomak u industriji digitalne televizije.

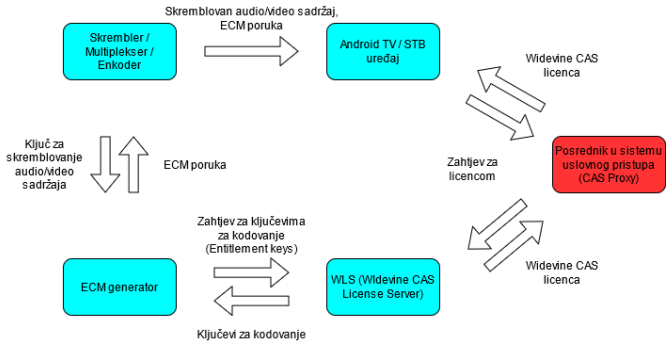
Radenko Banović – Fakultet Tehničkih Nauka, Univerzitet u Novom Sadu, Trg Dositeja Obradovića 6, 21000 Novi Sad, Srbija (e-mail: Radenko.Banovic@rt-rk.com).

Ilija Bašičević – Fakultet Tehničkih Nauka, Univerzitet u Novom Sadu, Trg Dositeja Obradovića 6, 21000 Novi Sad, Srbija (e-mail: ilibas@uns.ac.rs).

Nemanja Lazukić – Istraživačko-razvojni Institut RT-RK, Novi Sad, Srbija, (e-mail: Nemanja.Lazukic@rt-rk.com).

II. Widevine CAS sistem

Ključna prednost Widevine CAS rješenja u odnosu na konkurenciju jeste to što je kompletan CAS ekosistem dat operatorima na besplatno korištenje, pod uslovom da se izvršava na Android TV operativnom sistemu[5]. Komponente Widevine CAS sistema su : licencni poslužioc (eng. License Server), OEMCrypto (modul koji se integriše u Android TV), ECM (eng. Entitlement Control Message) generator, skrembler i posrednik u sistemu uslovnog pristupa. Sl. 1. prikazuje komponente Widevine CAS sistema na visokom nivou apstrakcije.



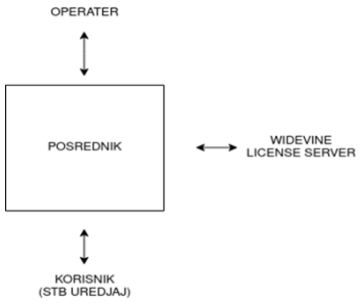
Sl. 1. Widevine CAS sistem

Neke komponente sistema su date tako da se ne mogu prilagođavati (OEMCrypto, licencni poslužioc), dok ECM generator i posrednik u sistemu uslovnog pristupa moraju da se implementiraju za svakog provajdera posebno, ali tako da se oslanjaju na Widevine SDK (eng. Software Development Kit). Licencni poslužioc je ključna tačka sistema u kojoj se sastaju predajna i prijemna strana. Korištenje licencnog poslužioca je moguće nakon što Widevine odobri zahtjev za korištenjem, i kreira posebne URL putanje prema zahtjevu provajdera.

Sa predajne strane se licencnom poslužiocu šalje zahtjev za dostavljanjem ključa (eng. Entitlement Key) kojim se enkriptuje ECM poruka u kojoj se nalaze ključevi kojima je skremblovan televizijski sadržaj. Sa prijemne strane se licencnom poslužiocu šalje zahtjev za dostavljanjem licence iz koje se izvlače ključevi kojima je moguće dekriptovati ECM poruku, te sa ključevima izvučenim iz ECM poruke deskremblovati televizijski sadržaj i prikazati ga korisniku.

III. Posrednik u sistemu uslovnog pristupa sa korisničkom upravljačkom logikom

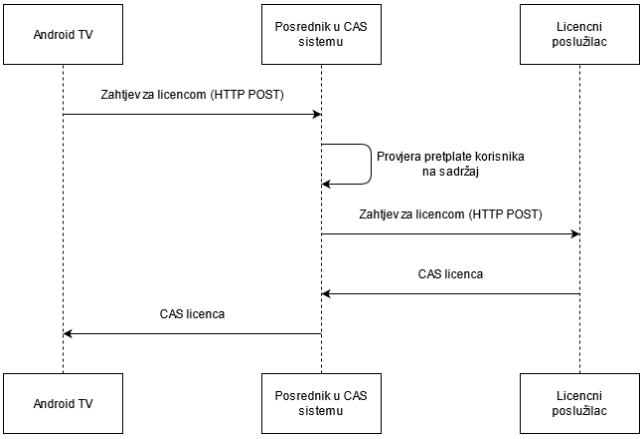
Posrednik kao jedan od elemenata CAS sistema komunicira sa Android TV / STB uređajem, kao i sa licencnim poslužiocem. Takođe, potrebno je kreirati korisnički interfejs preko kog je moguće unositi podatke vezane za korisnike, kanale, pakete na koje su korisnici pretplaćeni, što je ilustrovano u Sl. 2.



Sl 2. Interakcija posrednika sa okolinom

Posrednik je zamišljen kao mrežno orijentisan servis koji koristi REST (eng. Representational State Transfer) API (eng. Application Programming Interface) arhitekturu softvera[4]. Korištenje REST API arhitekture je omogućilo identifikovanje različitih resursa uz pomoć definisanja posebnih URI (eng. Uniform Resource Identifier) putanja, tako da i operater i korisnik (STB uređaj) mogu koristiti posrednik šaljući različite zahtjeve ka njemu. URI putanje namijenjene komunikaciji sa operaterom se odnose na upravljanje sadržajem baze podataka (dodavanje i brisanje korisnika, uređaja, paketa kanala, ažuriranje informacija o pretplatama korisnika).

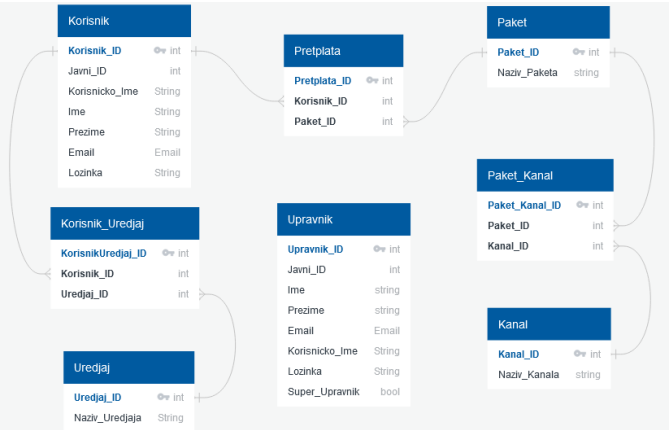
STB uređaj korisniku šalje zahtjev za licencom, zatim se nakon obrade zahtjeva provjerava da li je korisnik koji zahtjeva licencu za svoj STB uređaj pretplaćen na željeni sadržaj. Ukoliko jeste pretplaćen, zahtjev se proslijeđuje licencnom serveru, te se licenca dobijena od strane licencnog servera proslijeđuje korisniku koji je uputio zahtjev za licencom. Komunikacija između STB uređaja i posrednika, te posrednika i licencnog poslužioca je prikazana u Sl. 3



Sl. 4. Dijagram poziva posrednika

IV. Opis realizacije

Posrednik je ralizovan kao HTTP poslužilac u C++ programskom jeziku, jer je SDK na koji se on oslanja takođe realizovan u C++ programskom jeziku. Jezgro posrednika predstavlja baza podataka u kojoj se nalaze sve relevantne informacije na osnovu kojih je moguće odrediti da li je korisnik pretplaćen na odgovarajuće pakete kanala. Šema baze podataka je prikazana na Sl. 4.



Sl. 4. Šema baze podataka

A. *Alati korišteni za realizaciju*

Pošto je C++ izabran kao programski jezik, a posrednik treba da bude HTTP poslužilac izabrali smo Mongoose biblioteku[6] u kojoj je implementiran na događaj pobuđeni (eng. Event-driven) neblokirajući API za HTTP i uz koji je moguće kreirati REST API servise koji su neophodni za komunikaciju sa okolinom. Za upravljanje bazom podataka korištena je SQlite biblioteka[7].

B. *Implementacija obrade zahtjeva za licencom*

Nakon što posrednik zaprimi zahtjev na URI putanji *dobavi_licencu* u funkciji *handle_lic_req()* se uz pomoć poziva SDK funkcije *getDeviceInfo()* iz zahtjeva za licencu dobijaju informacije o uređaju i to : proizvođač, model, identifikacioni broj uređaja i serijski broj sertifikata uređaja. Iz zahtjeva za licencu se uz pomoć poziva SDK funkcije *getContentId()* dobavlja informacija o paketu kanala za koji se šalje zahtjev za licencu.

Na osnovu dobijenih informacija o uređaju iz baze podataka se dobavlja informacija o korisniku. Zatim se na osnovu informacije o korisniku i paketu kanala provjerava da li je korisnik pretplaćen na željeni paket kanala. Ukoliko je korisnik pretplaćen na paket kanala pozivom SDK funkcije *GenerateLicenseRequestAsJSON()* se na osnovu zahtjeva za licencu generiše zahtjev koji se preko HTTP Post metode korištenjem Curl biblioteke šalje licencnom serveru.

HTTP odgovor dobijen on licencnog poslužioca se proslijeđuje STB uređaju koji je poslao zahtjev pozivom funkcije mg_printf() biblioteke mongoose. Ukoliko korisnik nije pretplaćen na željeni sadržaj na STB uređaj se odmah šalje HTTP odgovor sa statusnim kodom 405 koji se odnosi na to da takav zahtjev nije dozvoljen.

Svaka akcija za popunjavanje baze podataka je kreirana sa posebnom uri putanjom i funkcijom koja obrađuje zahtjev. Akcije koje su obrađene su : dodaj korisnika, obriši korisnika, pretplati korisnika, ukini pretplatu korisnika, dodaj uređaj, obriši uređaj, dodaj kanal, obriši kanal, dodaj pretplatu, obriši pretplatu, dodaj kanal u paket i izbaci kanal iz paketa. U ovoj fazi razvoja nije predviđena realizacija prednjeg dijela (eng. Front-end) zbog čega su implementirane samo funkcije za popunjavanje baze podataka, i čitanja iz baze podataka neophodna za dobavljanje licence.

V. TESTIRANJE

Predloženo rješenje je testirano na Synaptics BG5CT STB (Sl. 8.) uređajima sa operativnim sistemom Android Q. Korištena je Live Channels korisnička aplikacija koja se oslanja na Comedia DTV (eng. Digital Television) srednji sloj kompanije iWedia, u kom je integrisam OEMCrypto koji kreira zahtjev za licencom i koji služi za deskremblovanje televizijskog sadržaja.

Sl. 8. Synaptics BG5CT platforma

Sa predajne strane je korišten TSDuck set alata [8] koji se u ovom slucaju koristio za skremblovanje TS (eng. Transport Stream) toka podataka koji se nalazio u izvorišnoj datoteci, kao i za slanje skremblovanog toka podataka ka odrednišnom STB uređaju korištenjem računarske mrežne infrastrukture i IPv6 (eng. Internet Protocol version 6) protokola. Takođe, sa predajne strane je korišten ECM generator koji je razvijan u paraleli sa posrednikom u sistemu uslovnog pristupa.

Funkcionalnost je testirana korištenjem više prijemnih uređaja pri čemu su mijenjane informacije o pretplaćenim korisnicima u bazi podataka. Kreirano je nekoliko testnih slučajeva u kojima su različiti korisnici u različitim testnim slučajevima bili pretplaćeni na željeni sadržaj. Jedan primjer testnog slučaja: korisnik A je pretplaćen na željeni sadržaj, korisnik B nije pretplaćen na željeni sadržaj, testiranjem je utvrđeno da korisnik A ima pristup sadržaju, dok korisnik B nema pristpu sadržaju.

Po završetku testiranja utvrđeno je da su STB uređaji pretplaćenih korisnika uspješno deskremblovali i reprodukovali sadržaj iz izvorišne datoteke koja je emitovana ka njima. U slučajevima nepretplaćenih korisnika STB uređaji su dobijali odgovor od posrednika da nisu pretplaćeni na željeni sadržaj, te nisu dobili licencu iz koje bi mogli izvuću ključeve kojima bi uspješno deskremblovali sadržaj.
Testiranjem je utvrđena funkcionalnost rješenja.

VI. ZAKLJUČAK

U ovom radu je prikazano jedno rješenje posrednika u sistemu uslovnog pristupa sa korisničkom upravljačkom logikom. Opisan je Widevine CAS sistem u cjelini kao i uloga posrednika u njemu. Navedeni su svi alati korišteni u realizaciji rješenja, te je dat detaljan opis rješenja. Rješenje je testirano korištenjem nekoliko prijemnih uređaja i nakon uspješno završenih testova potvrđena je funkcionalnost rješenja. Doprinos ovog rada u odnosu na postojeća rješenja je u tome što je kompatibilan sa Widevine CAS ekosistemom. U budućnosti ovo rješenje može biti unaprijeđeno kreiranjem prednjeg dijela poslužioca čime bi se omogućio jednostavan vizuelni prikaz i lakše upravljanje pretplatom korisnika, te proširenjem zadnjeg dijela poslužioca.

LITERATURA

[1] I. Kaštelan, V. Peković, V. Zlokolica, J. Zloh, D. Trifunović, “Simultaneous automated verification of conditional access system on multiple TV sets,” Proc. IEEE International Conference on Consumer Electronics, Berlin, Germany, pp. 269-270, Sept. 2012.

[2] Fu-Kuan Tu, Chi-Sung Laih and Hsu-Hung Tung, "On key distribution management for conditional access system on pay-TV system," in *IEEE Transactions on Consumer Electronics*, vol. 45, no. 1, pp. 151-158, Feb. 1999, doi: 10.1109/30.754430.

[3] Milan Bjelica, Nikola Teslić, Velibor Mihić, “Softver u digitalnoj televiziji 1”, 2017.

[4] Fielding, Roy Thomas (2000). "Chapter 5: Representational State Transfer (REST)". Architectural Styles and the Design of Network-based Software Architectures (Ph.D.). University of California, Irvine

[5] Widevine CAS, Jun 2021. [online]. https://www.widevine.com/solutions/widevine-cas

[6] Mongoose - Embedded Web Server, Jun 2021. [online]. https://github.com/cesanta/mongoose

[7] SQLite, Jun 2021. [online]. https://www.sqlite.org

[8] TSDuck, Jun 2021. [online]. https://tsduck.io/

ABSTRACT

There are two types of TV (television) services in the domain of subscription: public (content available to all for which no subscription is required) and subscriber TV service (TV content is available only to subscribed users). In order for the subscriber TV service to make sense, it is necessary to protect the TV content throughout the transmission. There are several models of protection of subscriber TV content, and one of them is CAS (Conditional Access System). Widevine has created a conditional access system (CAS) solution that is free for all operators. In order for operators to be able to manage users and content, it is necessary to implement the user management logic of the system. This paper presents a solution of a proxy server in which the user control logic of the conditional access system in the Widevine CAS system is realized.

One solution of proxy server in the digital television conditional access system

Radenko Banović, Ilija Bašičević, Nemanja Lazukić