Jedno rješenje ECM generatora

Radenko Banović, Ilija Bašičević, Ksenija Popov i Milenko Maksić

***Apstrakt*—Zaštita televizijskog sadržaja predstavlja jedan od najvećih izazova u industriji digitalne televizije usljed sve manjeg broja televizijskih kanala čije se gledanje ne naplaćuje. Da bi omogućili naplaćivanje televizijskog sadržaja korisnicima, potrebno je zaštiti televizijski sadržaj cijelim prenosnim putem. Najkorišteniji model zaštite živog televizijskog sadržaja je CAS (eng. Conditional Access System). CAS model podrazumijeva postupak zaštite video i audio sadržaja skremblovanjem koje ima za cilj sprječavanje neovlaštene reporodukcije audio i video sadržaja. Kontrolne riječi kojima je izvršeno skremblovanje se prenose istim prenosnim kanalom kao i skremblovani sadržaj u okviru ECM (eng. Entitlement Control Message) poruke ali u enkriptovanom obliku. Kompanija Widevine je realizovala sopstveni CAS ekosistem potpuno besplatan za sve korisnike. U ovom radu je predstavljeno jedno rješenje ECM generatora u Widevine CAS sistemu.**

***Ključne reči*—ECM generator, Conditional Access System, Digital Television**

I. Uvod

U junu 2014. godine je prvi put prikazan Andoid TV operativni sistem, koji je prilagođena verzija Android operativnog sistema za televizore i STB (set-top box) uređaje[4]. Do danas je veliki broj proizvođača televizora i STB uređaja, kao i operatera televizijskih kanala integrisalo Android TV kao operativni sistem koji se izvršava na njihovim uređajima[5].

Kako bi privoljeli i preostale operatere televizijskih kanala i proizvođače televizora i STB uređaja da integrišu Android TV na svoje uređaje kreiran je Widevine CAS sistem uslovnog pristupa koji je na korištenje dat potpuno besplatno, ali može da se koristi samo uz Android TV operativni sistem. Da bi sistem postao funkcionalan, potrebno je implementirati ECM generator i posrednik u sistemu uslovnog pristupa, za šta je dat SDK (eng. Software Development Kit).

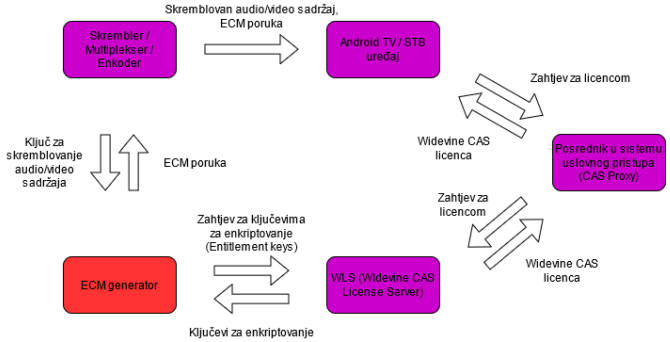
Komponente sistema koje je potrebno implementirati nisu implementirane da bi svaki operater televizijskih kanala prilagodio sistem svojim potrebama. Postoji nekoliko primjera implementacije ECM generatora [1, 2], ali oni nisu prilagođeni Widevine CAS ekosistemu. Widevine CAS sistem je prikazan u Sl. 1.

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).

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

Milenko Maksić – Istraživačko-razvojni Institut RT-RK, Novi Sad, Srbija, (e-mail: Milenko.Maksic@rt-rk.com).



Sl. 1. Widevine CAS sistem

II. ECM generator

Da bi audio i video sadržaj bio zaštićen tokom kompletnog prenosnog toka vrši se postupak skremblovanja. Inverzni postupak u odnosu na skremblovanje se naziva deskremblovanje, njime se zaštićeni sadržaj prevodi u osnovni format razumljiv audio i video dekoderima[3].

Skremblovanje se vrši korištenjem kontrolne riječi (ključa za skremblovanje). Korištenje kontrolne riječi u procesu skremblovanja omogućuje promjenu kontrolne riječi u vremenu, a period između dve promjene se naziva periodom kriptovanja. Što je češća izmjena kontrolne riječi, to je proces skremblovanja bezbjedniji.

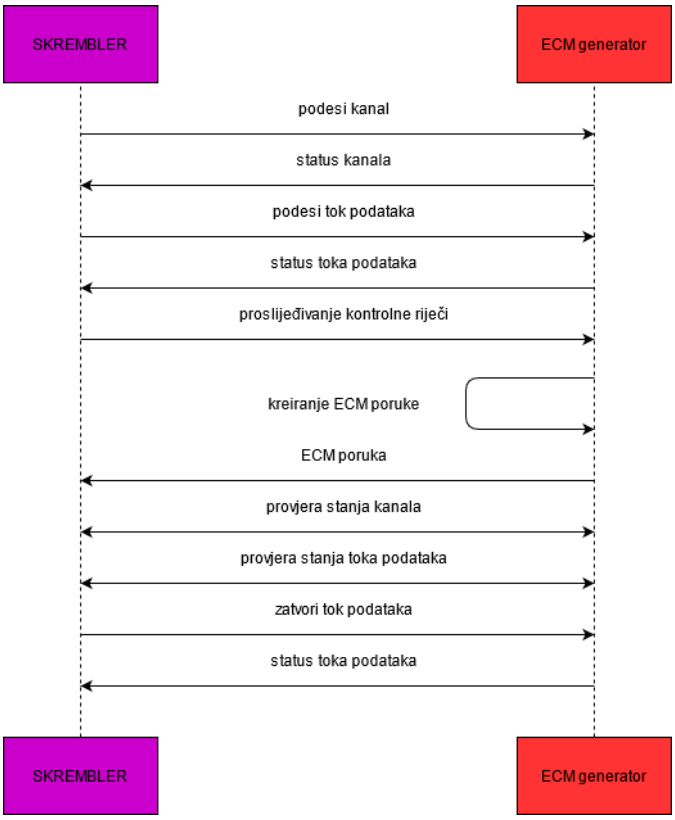
Trenutno korištena kontrolna riječ prenosi se u okviru ECM poruke koja se generiše u ECM generatoru. PID (eng. Packet Identifier) vrijednost TS (eng. Transport Stream) paketa u kom se nalazi ECM poruka se nalazi u CA deskriptoru PMT tabele. ECM generator u Widevine CAS sistemu komunicira sa licencnim poslužiocem (eng. License Server) i skremblerom. Pozicija ECM generatora u Widevine CAS sistem je prikazan na Sl. 2.

Sl. 2. Pozicija ECM generatora u widevine sistemu

U ovom radu je korišten skrembler implementiran u TS Duck programskoj podršci. TS Duck je set alata koji se koristi za manipulaciju MPEG prenosnim tokovima, a jedan od alata je i skrembler koji može da koristi i eksterni ECM generator za generisanje ECM poruka[6]. ECM generator i TS Duck komuniciraju po ECMG/SCS (eng. Simulcrypt Synchroniser) protokolu[7].

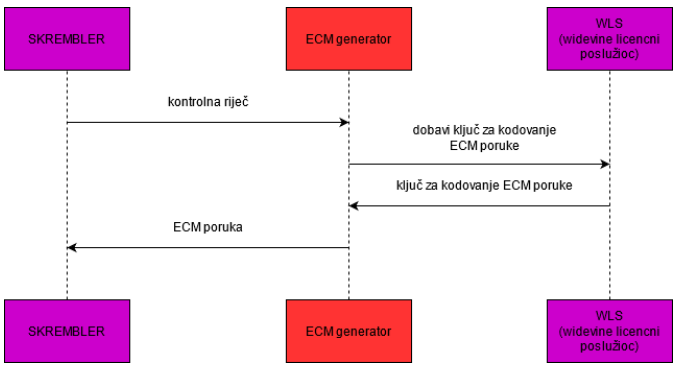
U komunikaciji između generatora i skremblera, skrembler je implementiran kao klijent, dok generator treba da bude implementiran kao poslužioc, te je ECM generator je u smislu komunikacije sa skremblerom implementiran kao TCP/IP poslužioc koja čeka zahtjeve od skremblera.

Po uspostavljanju veze generatora i skremblera kreira se sesija koja je zadužena za razmjenu poruka u okviru ECMG/SCS protokola. ECMG/SCS protokol je prikazan na Sl. 3.



Sl 3. Dijagram ECMG/SCS protokola

WLS (eng. Widevine License Server) je već gotovo rješenje sa kojim ECM generator komunicira putem HTTP protokola. ECM generator treba od WLS da dobavi (eng. Entitlement) ključeve kojima će enkriptovati ECM poruku u kojoj se nalaze ključevi kojima je skremblovan sadržaj, tako da u slučaju presretanja ECM poruke presretač ne može da dobije informaciju o ključevima kojima je sadržaj skremblovan. Dijagram komunikacije skremblera, ECM generatora i WLS je prikazan na Sl. 4.



Sl. 4. Dijagram komunikacije ECM generatora

III. Opis realizacije

ECM generator je realizovan kao C++ CLI (eng. Command Line Interface) aplikacija. Prilikom pokretanja aplikacije potrebno je proslijediti broj porta na kom aplikacija osluškuje zahtjev klijenta (skrembler) za uspostavljanjem veze. Kompletno rješenje se oslanja na Widevine SDK (eng. Software Development Kit). Rješenje možemo podijeliti u tri logičke cjeline, i to: TCP/IP poslužilac, ECMG/SCS protokol, i ECM generator.

A. TCP/IP poslužilac

Ovaj modul sadrži dvije funkcije*: void TCPstart(int port, void (*onSessionEstablished)())* i *void TCPstop(int port)*. Funkcija *TCPstart* kreira TCP/IP utičnice sa podrškom za IPv4 i IPv6 protokole, stavlja poslužioca u stanje čekanja zahtjeva za konekcijom klijenta, te uspostavlja vezu i kreira sesiju za korisnik / poslužilac komunikaciju. Funkcijom *TCPstop* se zatvara otvorena sesija.

B. ECMG/SCS protokol

U ovom modulu je implementiran ECMG/SCS protokol. Implementiran je tako da se izvršava u *while* petlji, poziva se funkcija *read()* koja je blokirajuća, i koja zaustavlja izvršavanje petlje dok se memorija za smještanje dolaznih podataka ne popuni. Iz pristiglih podataka se pozivom funkcije *int32_t msg_pars(const uint8_t* buff, uint32_t size, struct ecmgp_msg* msg)* popunjava sktruktura *ecmgp_msg*.

Jedno od polja strukture koja predstavlja poruku je tip poruke, na osnovu kog se korištenjem *swich* grananja bira grana u kojoj se priprema odgovor na poslatu poruku. Tip poruke može biti : *CHANNEL_SETUP, STREAM_SETUP, CW_PROVISION, STREAM_CLOSE_REQUEST*. Svaka od grana popunjava strukturu koja predstavlja poruku, te se poziva funkcija *int32_t msg_generator(uint8_t* buff, struct ecmgp_msg* msg)* koja od podataka iz strukture kreira poruku koja se šalje ka klijentu.

Poruka tipa *CW_PROVISION* nosi i vrijednost ključa za skremblovanje audio/video sadržaja koja kriptovana treba da se nađe u ECM poruci. U funkciji *int32_t gen_ecm_datagram(uint8_t* ecm_datagram, struct ecmgp_msg* msg)* je implementirano kreiranje ECM poruke, te se ona poziva u grani obrade poruke tipa *CW_PROVISION*. Nakon poziva ove funkcije ECM poruka se dodaje kao polje strukture *ecmgp_msg*, poziva se funkcija *msg_generator* nakon koje se kreirana ECM poruka šalje skrembleru.

C. ECM generator (u užem smislu)

Za generisanje ECM poruke i kreiranje TS paketa, te kreiranje zahtjeva za ključevima za enkriptovanje ECM poruke i parsiranjem odgovora dobijenog od WLS korištene su funkcije dobijene iz Widevine SDK paketa. Funkcija u kojoj se kreira ECM poruka *gen_ecm_datagram()* kroz parametar dobija poruku dobijenu od skremblera u kojoj se nalaze ključevi za skremblovanje audio/video podataka. Pored ključeva za skremblovanje, potrebno je dobaviti ključeve za enkriptovanje ECM poruke koji se dobijaju slanjem ispravnog HTTP zahtjeva ka WLS.

Pozivom funkcije *CreateEntitlementRequest()* koja je dio Widevine SDK kreira se zahtjev za ključevima za enkriptovanje ECM poruke. Da bi se kreirao ispravan zahtjev potrebno je funkciji proslijediti sledeće podatke: identifikator sadržaja za skremblovanje, naziv operatera, broj ključeva za skremblovanje (jedan, ili dva), rezolucija sadržaja, ime operatera koji potpisuje zahtjev za licencom, ključ za potpisivanje enkriptovanog zahtjeva i vektor za potpisivanje zahtjeva. Nakon što je zahtjev ispravno kreiran korištena je CURL biblioteka[8] kako bi se poslao HTTP zahtjev ka WLS, nakon čega se odgovor upisuje u željeni dio memorije.

Nakon dobijenog odgovora, poziva se funkcija *ParseEntitlementResponse()* koja iz sirovog odgovora izvlači dva ključa za enkriptovanje ECM poruke. Pozivom funkcije *GenerateEcm()* kojoj se kao parametri proslijeđuju ključevi za enkriptovanje ECM poruke kreira se ECM poruka, da bi se na kraju pozivom *GenerateTsPacket()* kreirao paket koji se šalje ka skrembleru.

IV. TESTIRANJE

U paraleli sa izradom ECM generatora, kreirano je i rješenje posrednika u sistemu uslovnog pristupa (CAS Proxy), te je integrisana Widevine OEMCrypto biblioteka u Android STB uređaj. Nakon što na Android STB uređaj pristigne skremblovan audio/video sadržaj, on posredniku u sistemu uslovnog pristupa šalje zahtjev za licencom, sa informacijom o kom sadržaju je riječ. Ukoliko dobije odgovor od posrednika, licenca se proslijeđuje OEMCrypto biblioteci koja iz licence izvlači ključeve za dekriptovanje ECM poruke. Ukoliko se poruka uspješno dekriptuje, ključevima dobijenim iz ECM poruke se deskrembluje audio/video sadržaj, te je na ekranu moguće vidjeti audio/video sadržaj koji je poslat na STB uređaj. Predloženo rješenje je testnirano na Synaptics BG5CT STB (Sl. 5.) 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.

Sl. 5. Synaptics BG5CT platforma

Pošto su STB uređaji uspješno deskremblovali i reprodukovali audio/video sadržaj skremblovan ključevima generisanim u TS Duck alatu, te ECM porukama enkriptovanim ključevima dobijenim od WLS, konstatovali smo da je testiranjem utvrđena funkcionalnost rješenja.

V. ZAKLJUČAK

U ovom radu je prikazano jedno rješene ECM generatora u Widevine CAS sistemu. U uvodu je objašnjena uloga i značaj CAS sistema, kao i njegova komercijalna primjena. Bliže je opisan način zaštite televizijskog sadržaja u CAS sistemima, Prikazan je opis rješenja. Rješenje je testirano na nekoliko prijemnih uređaja, sa nekoliko ulaznih tokova podataka te je potvrđena funkcionalnost sistema. U budućnosti se ovo rješenje može unaprijediti podrškom za kreiranje ECM poruke za više različitih tokova podataka u paraleli.

LITERATURA

[1] Li Xi and Chen Xin, "Design of Digital Video Broadcasting Conditional Access System Headend Communication Interface," in *Computer and Modernization*, vol. 1, no. 3, pp. 118-121, 2012.

[2] In-Hee Jo and Byoung-Soo Koh, " Building a common encryption scrambler to protect paid broadcast services," in *International Journal of Internet Technology and Secured Transactions*, vol. 6, no. 3, Nov. 2016, doi: 10.1504/IJITST.2016.080391.

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

[4] Google Unveils First Android TV Device, Jun 2021. [online]. https://www.nexttv.com/news/google-unveils-first-android-tv-device-384772

[5] Android TV OS reaches 80M monthly active devices, Jun 2021. [online]. https://techcrunch.com/2021/05/18/android-tv-os-reaches-80m-monthly-active-devices-adds-new-features/

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

[7] ECMG/SCS protokol, Oktobar 2008. [online]. https://www.etsi.org/deliver/etsi_ts/103100_103199/103197/01.05.01_60/ts_103197v010501p.pdf

[8] Curl library, Jun 2021. [online]. https://curl.se/

ABSTRACT

The protection of television content is one of the biggest challenges in the digital television industry due to the declining number of free-to-air television channels. In order to enable the charging of television content to operators, it is necessary to protect television content throughout the transmission. The most widely used model for the protection of live television content is the CAS (Conditional Access System). The CAS model involves a process of protecting video and audio content by scrambling that aims to prevent unauthorized reproduction of audio and video content. The scrambled control words are transmitted via the same transmission channel as the scrambled content within the ECM (Entitlement Control Message) message but in encrypted form. Widevine has implemented its own CAS model completely free for all users. In this paper, one solution of ECM generator in Widevine CAS system is presented.

One solution of ECM generator

Radenko Banovic, Ilija Basicevic, Ksenija Popov, Milenko Maksic