Centar Informacijske Sigurnosti

AACS – sustav za zaštitu digitalnog sadržaja

CIS-DOC-2011-02-003

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

Kroz povijest, vlasnici autorskih prava, autori i druge financijski ili umjetnički zainteresirane strane protivile su se tehnologijama koje omogućuju umnažanje izvornih kreativnih sadržaja. Njihovi razlozi su jasni: neovlašteno umnažanje tako nastalih sadržaja dovodi do narušavanja autorskog integriteta [12] i smanjenih prihoda autora i izdavača. Digitalni formati zapisa sadržaja značajno olakšavaju njegovo umnažanje, zbog čega su uvišestručeni napori vlasnika autorskih prava uloženi u njihovu zaštitu.

Skup tehnologija za zaštitu i kontrolu korištenja digitalnog sadržaja zajednički se naziva upravljanje digitalnim pravima (eng. *Digital Rights Management - DRM*). Primjenjuju ih izdavači i drugi vlasnici autorskih prava kako bi ograničili pristup digitalnim uređajima i multimedijalnim sadržajima te spriječili njihovo neovlašteno umnažanje i pretvorbu u druge formate. Tehnologije upravljanja digitalnim pravima prvenstveno se susreću u zabavnoj industriji, primjerice glazbenoj i filmskoj, ali se pojavljuju i na drugim područjima. Tvrtke koje se bave prodajom glazbe na Internetu (npr. *iTunes*), pojedini izdavači elektroničkih knjiga (eng. *e-books*) i mnogi drugi također su razvili različite strategije upravljanja digitalnim sadržajima. Posljednjih godina brojni televizijski producenti isto tako zahtijevaju uporabu DRM tehnologija kako bi se kontrolirao pristup njihovim programima zbog porasta popularnosti DVR uređaja (eng. *Digital Video Recorder*).

S druge strane, DRM tehnologije poznate su i zbog brojnih kontroverzi vezanih uz njihovu uporabu. Velik broj krajnjih korisnika zajedno s nekim organizacijama poput FSF-a (eng. *Free Software Foundation*) ili EFF-a (eng. *Electronic Frontier Foundation*) smatraju da DRM tehnologije zapravo uvode ograničenja na legalno korištenje zaštićenih sadržaja te ograničavaju ravnopravnost tržišne utakmice onemogućavanjem konkurencije.

Jedna od nekolicine popularnih tehnologija upravljanja digitalnim pravima vezanih uz zaštitu video sadržaja je i tehnologija poznata pod akronimom AACS (eng. Advanced Access Content System). Riječ je o standardu za distribuciju digitalnih sadržaja i upravljanje pravima njihova korištenja namijenjenom ograničenju pristupa i onemogućavanju neovlaštenog umnažanja sadržaja pohranjenog na optičkim diskovima nove generacije. Specifikacija standarda objavljena je u travnju 2005. godine i prihvaćena od strane proizvođača kao osnova zaštite HD DVD i *Blu-ray* diskova.

U nastavku dokumenta bit će predstavljen AACS standard, opisan njegov razvoj i način na koji se njime štite digitalni sadržaji te analizirana sigurnost takve zaštite. Uz to, dan je pregled najvažnijih napada na ovaj standard i njihove posljedice.

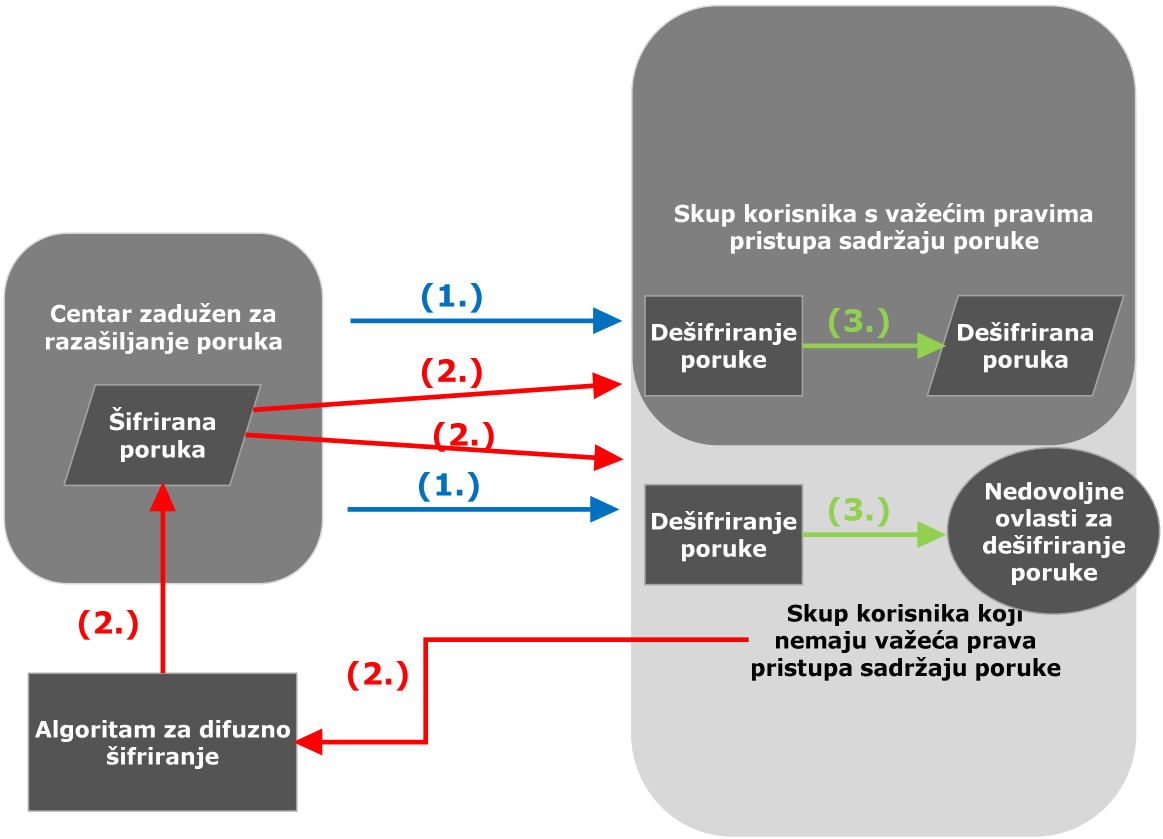
2. Razvoj

2.1. Osnovni koncept

Kao što je već navedeno, AACS spada u tehnologije upravljanja digitalnim pravima namijenjene prvenstveno zaštiti video sadržaja zapisanog na HD DVD i *Blu-ray* diskovima. Zaštita podrazumijeva ograničenja vezana uz distribuciju digitalnih sadržaja i upravljanje pravima njihova korištenja.

Rad AACS tehnologije temelji se na šifriranju sadržaja korištenjem principa tzv. difuznog šifriranja (eng. *broadcast encryption*). Difuzno šifriranje u osnovi rješava kriptografski problem šifriranja razašiljanog sadržaja (primjerice televizijski programi) na način da samo određeni korisnici (recimo pretplatnici koji su platili svoje pristojbe) mogu dešifrirati takav sadržaj. Teškoće se javljaju zbog zahtjeva da kraj pretplate kod nekih korisnika ne smije utjecati na preostale korisnike. Problematika se dodatno komplicira činjenicom da je često potrebno šifrirati više od jednog podatkovnog toka (više televizijskih kanala) od kojih svaki može imati zasebne pretplatnikev[2].

Danas je na tržištu dostupno nekoliko rješenja od kojih svako na svoj način rješava spomenuti problem, uz odgovarajuće prednosti i nedostatke. Svako od njih temelji se na zajedničkom principu: šifrirana poruka razašilje se prema nekom skupu korisnika koji se može podijeliti na skupinu korisnika s važećim pravima pristupa (pretplatnika) i skupinu onih koji ta prava nemaju. Ideja je da samo oni korisnici s važećim pravima pristupa mogu dešifrirati izvorni sadržaj poruke. Postupak difuznog šifriranja prikazuje Slika 1.



Slika 1. Osnovni koraci postupka difuznog šifriranja

Na slici se mogu vidjeti osnovni koraci postupka difuznog šifriranja:

1. Inicijalizacijski korak podrazumijeva dodjelu tajne informacije svakom od korisnika iz skupa korisnika kojima će biti razašiljana šifrirana poruka. Ta tajna informacija služit će za dešifriranje šifriranog sadržaja izvorne poruke.

2. Centar zadužen za razašiljanje poruka koristi algoritam za difuzno šifriranje. Takav algoritam kao ulaznu informaciju prima poruku koju se želi poslati te skup korisnika koji nemaju važeća prava pristupa sadržaju poruke. Izlaz algoritma je posebno šifrirana izvorna poruka koja se šalje svim korisnicima.
3. Kad korisnici prime takvu poruku, mogu iskoristiti dobivenu tajnu informaciju iz prvog koraka kako bi dešifrirali njen sadržaj samo pod uvjetom da se ne nalaze u listi korisnika koji nemaju važeća prava pristupa njenom sadržaju.

S obzirom na činjenicu da model difuznog šifriranja predstavlja funkciju koja kao ulaz prima skup korisnika koji nemaju važeća prava pristupa sadržaju, često se naziva i revokacijskom shemom (eng. *Revocation Scheme*). Valja naglasiti kako se korisnicima s kompromitiranim pravima u svakom trenutku mogu povući ovlasti dodjelom osvježenih informacija korisnicima [2].

Dalit Naor, Moni Naor i Jeff Lotspiech su 24. veljače 2001. godine objavili članak [13] u kojem su opisali shemu difuznog šifriranja korištenjem koncepta nazvanog Naor-Naor-Lotspiechova diferencijska stabla podskupova (eng. *Naor-Naor-Lotspiech subset-difference trees*). U tom članku postavili su teorijske osnove mehanizma na kojem se temelji rad AACS-a.

2.2. Razvoj specifikacije

2004. godine osnovan je AACS LA (eng. *AACS Licensing Administrator*) konzorcij kojeg čine poznate svjetske tvrtke kao što su Disney, Intel, Microsoft, Panasonic, Warner Brothers, IBM, Toshiba i Sony. Jedan od osnovnih ciljeva tog konzorcija bila je izrada naprednog standarda za zaštitu video sadržaja zapisanog na optičkim diskovima nove generacije.

U siječnju 2005. časopis IEEE Spectrum objavio je članak u kojem je razvijanu AACS tehnologiju svrstao u jednu od tehnologija najvjerojatnije osuđenih na propast prvenstveno imajući na umu objavu DeCSS-a, programa za dešifriranje digitalnog sadržaja pod zaštitom CSS (eng. *Content-Scrambling System*) standarda.

Objava konačnih specifikacija AACS standarda odgađana je stoga nekoliko puta, sve do trenutka kada je Toshiba predložila objavu privremenih specifikacija. Prijedlog je prihvaćen i privremene specifikacije objavljene su u travnju 2005. godine, a sama tehnologija počela se uvelike primjenjivati na HD DVD te Blu-ray diskovima od 2006. godine. Privremene specifikacije nisu sadržavale sve prvotno zamišljene funkcionalnosti (vođeno umnažanje, audio vodeni žigovi itd.) te je rad na standardu nastavljen.

Završne specifikacije AACS standarda objavljene su 2009. godine, no rad na samom standardu i dalje se nastavlja. Specifikacije cjelokupne tehnologije trenutno su dostupne na više od 550 stranica raspoređenih u preko 7 dokumenata i pružaju pregled cijelog sustava te specifične implementacije za prazne *Blu-ray* i HD DVD diskove te one s unaprijed pohranjenim sadržajem. Sve objavljene specifikacije mogu se pregledati u dokumentu „AACS LA: Advanced Access Content System Home Site“ [1].

2.3. Primjena standarda

Privremene i konačne specifikacije AACS standarda globalni su proizvođači prihvatili kao osnovu zaštite, kako na praznim HD DVD i *Blu-ray* diskovima, tako i na onima s unaprijed pohranjenim sadržajem.

Prije pojave spomenutih optičkih diskova nove generacije, osnovni i daleko najpopularniji optički diskovi korišteni za pohranu velike količine podataka na čelu s visokokvalitetnim video sadržajem bili su (i još uvijek jesu) tzv. DVD-ovi (eng. *Digital Versatile Disc*). Sustav za upravljanje digitalnim pravima koji se koristi kod većine komercijalnih *DVD-Video* diskova već je spomenut u ovom poglavlju i poznat je pod nazivom CSS. Na njega se može gledati kao na svojevrsnog prethodnika AACS-a s obzirom na činjenicu da se oba, uz razlike u implementaciji i stupnju sigurnosti, temelje upravo na kriptografiji i specifičnim metodama šifriranja digitalnog sadržaja. Ipak, zbog ograničenja kako samih DVD diskova, tako i CSS-a kao osnovnog sustava zaštite visokokvalitetnog digitalnog video sadržaja, predviđa se kako će ih HD DVD te pogotovo *Blu-ray* diskovi u kombinaciji s naprednijim AACS-om u potpunosti istisnuti s tržišta.

2.3.1. HD DVD diskovi

HD DVD (eng. *High Density DVD, High-Definition DVD ili High Definition Digital Video Disc*) je jedan od standarda za pohranu velike količine podataka na optičke diskove stvoren za

visokokvalitetne video zapise i podatke. Razvila ga je grupa proizvođača potrošne elektronike i poznatih ICT (eng. *Information and Communication Technology*) tvrtki predvođena Toshibom s namjerom da ga pretvori u nasljednika popularnog DVD formata. Međunarodna organizacija u koju se ubrajala i spomenuta grupacija osnovana je 1995. godine i poznata je pod nazivom DVD Consortium (kasnije DVD Forum). Prvenstveno je zaslužna za razvoj i promociju DVD formata, a HD DVD format je odlučila poduprijeti 2003. godine.

HD DVD format za zapisivanje sadržaja koristi ljubičastu lasersku zraku valne dužine od 405 nm na posebne HD DVD optičke diskove promjera 80 ili 120 mm. Gustoća zapisa HD DVD-a je preko tri puta veća od gustoće zapisa kod klasičnih DVD diskova, ali i preko 65% manja od gustoće zapisa *Blu-ray* diskova koji koriste lasersku zraku iste valne dužine. Na jednoslojni 120-milimetarski HD DVD stane 15 GB, a na dvoslojni (eng. *dual layer*) 30 GB podataka, što je dovoljno za pohranu cjelovečernjih filmova u visokoj 720p, 1080i i 1080p rezoluciji. Na sljedećoj slici (Slika 2) nalazi se HD DVD disk zajedno s poznatim logom HD DVD formata.

Slika 2. HD DVD logo i HD DVD disk
Izvor: Wikipedia

U veljači 2008. godine Toshiba je kao idejni začetnik HD DVD tehnologije javno objavila kako više neće razvijati, proizvoditi niti prodavati HD DVD snimače i rekordere. Tako je okončan rat optičkih formata visoke definicije u kojem je pobjedu odnijela konkurentska Sonyjeva *Blu-ray* tehnologija.

2.3.2. *Blu-ray* diskovi

Blu-ray (BD) je optički disk za pohranu velike količine podataka dizajniran da naslijedi popularne DVD diskove. Standardni fizički medij plastičan je optički disk jednake veličine kao i klasičan DVD ili CD, promjera 120 mm, i kapaciteta 25 GB po sloju zapisa. Poput HD DVD-a, i *Blu-ray* za zapisivanje sadržaja koristi plavo-ljubičast laser valne duljine od 405 nm s mogućnošću višestrukog zapisa podataka. Na sljedećoj slici (Slika 3) nalazi se *Blu-ray* disk zajedno s poznatim logom tehnologije.

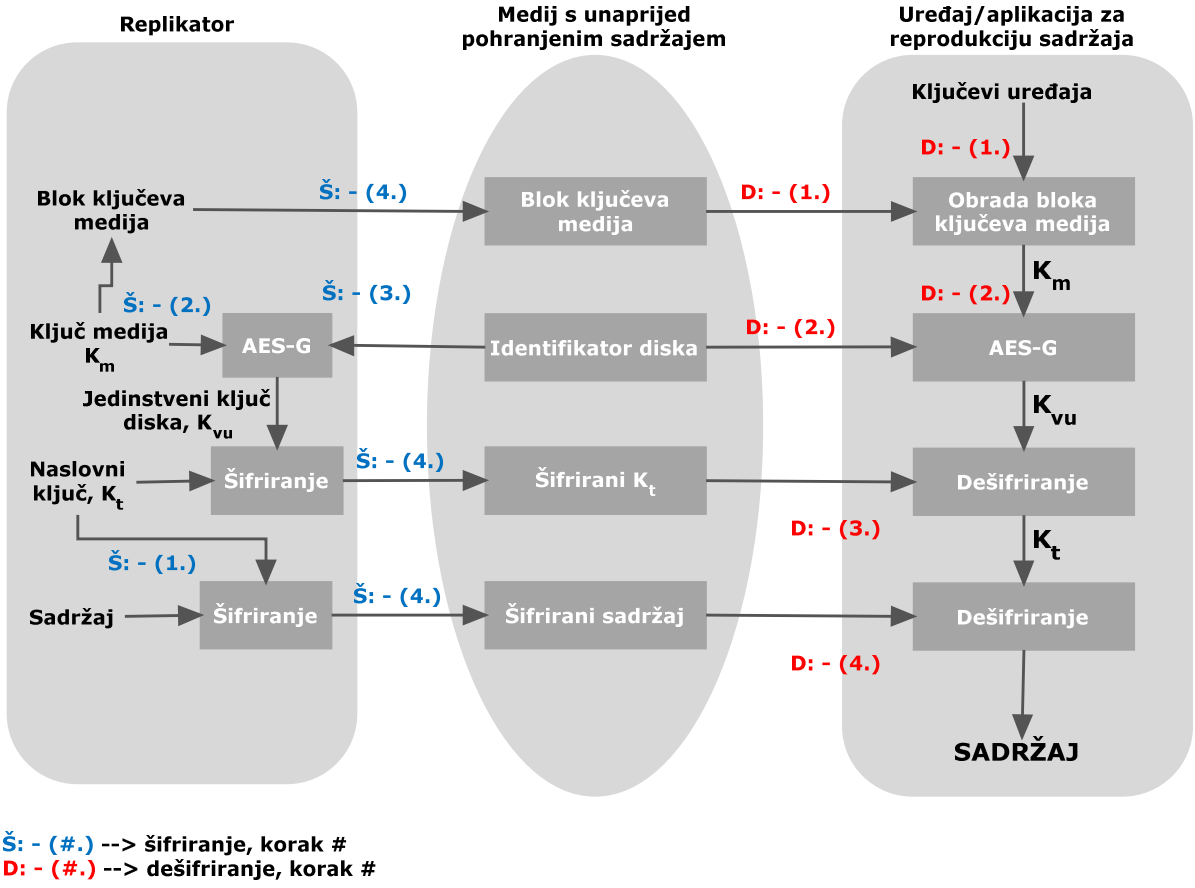
Slika 3. Blu-ray logo i Blu-ray disk

Blu-ray tehnologiju razvila je tzv. Blu-ray Association grupacija koju, između ostalih, čine i poznate tvrtke poput Matsushite, Philipsa, Sonyja, Thompsona, LG Electronicsa, Hitachija, Sharpa i Samsunga. Osnovne specifikacije određene su u veljači 2002. godine. Kao što je već navedeno, *Blu-ray* tehnologija je 2008. godine izašla kao pobjednik nad konkurentskom HD DVD tehnologijom čime je okončan rat optičkih formata visoke definicije, a *Blu-ray* je postao jedini pravi nasljednik popularnog DVD formata.

3. Princip rada

AACS se u svom radu koristi prvenstveno kriptografskim mehanizmima kako bi omogućio kontrolu pristupa sadržaju pohranjenom na digitalnim medijima. Pomoću AACS-a mogu se štititi i prazni optički mediji i oni s unaprijed pohranjenim podacima.

Kod diskova s unaprijed pohranjenim sadržajem podaci se prije zapisivanja na optički medij šifriraju posebnim tehnikama na način opisan u nastavku poglavlja. Za reprodukciju sadržaja potrebno je dešifrirati zaštićeni sadržaj, što, u principu, mogu samo ovlašteni korisnici. Postupak dešifriranja i reprodukcije zaštićenog sadržaja također je opisan u ovom poglavlju. Skica šifriranja i dešifriranja sadržaja AACS metodom kod diskova s unaprijed pohranjenim sadržajem nalazi se na slici u nastavku (Slika 4).

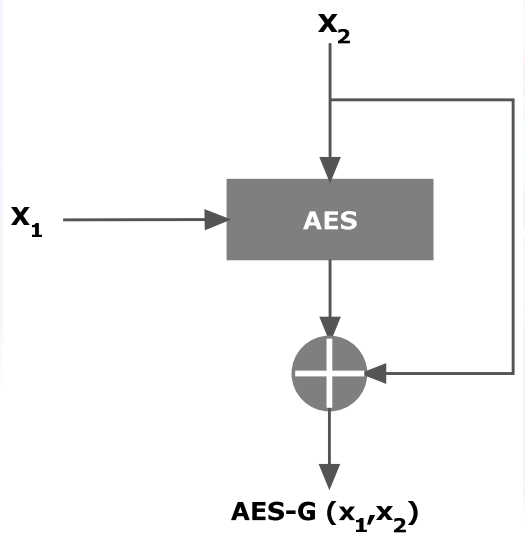


Slika 4. Pregled mehanizma šifriranja i dešifriranja sadržaja AACS metodom

Na gornjoj slici jasno se vidi kako je šifriranje sadržaja implementirano u uređajima koji se nazivaju replikatori, a dešifriranje u uređajima ili aplikacijama za reprodukciju (eng. *playback device*) koji se nalaze kod krajnjeg korisnika. Prije objašnjenja samih postupaka šifriranja i dešifriranja korisno je popisati i objasniti osnovne termine i kriptografske elemente označene na slici:

- **naslov** (eng. *Title*) – vlasnik sadržaja (primjerice produkcijski studio koji je izradio sadržaj) pruža sadržaj licenciranom replikatoru u obliku jednog ili više naslova. Primjerice, naziv filma „King Kong“ predstavlja jedan naslov.
- **naslovni ključ** (eng. *Title Key, K_t*) – replikator nasumično generira tajni, 128-bitni naslovni ključ za svaki naslov. Ovisno o replikatoru, jedan naslovni ključ može se koristiti za šifriranje svih instanci nekog naslova, ili se različiti naslovni ključevi mogu koristiti za različite instance. Kod postojećih implementacija AACS mehanizma sve se instance jednog naslova šifriraju jednim, zajedničkim naslovnim ključem.

- **identifikator diska** (eng. *Volume ID*) – replikator također nasumično generira 128-bitni identifikator za svaki naslov, koji se naziva identifikator diska. On se tada zapisuje na posebno područje optičkog diska, tzv. "*burst cut area*". To posebno područje, neovisno o tome radi li se o praznom disku ili onom s unaprijed upisanim sadržajem, je na korisničkim snimačima namijenjeno isključivo za čitanje. Uloga identifikatora diska je zaštita protiv umnažanja zaštićenog sadržaja metodom "bit po bit" (postupak replikacije sadržaja pohranjenog na digitalnom mediju na najnižoj mogućoj razini, razini svakog pojedinog bita). Kao i kod naslovnog ključa, i identifikator diska može se koristiti za sve instance nekog naslova ili se različiti identifikatori mogu koristiti za različite instance.
- **ključ medija** (eng. *Media Key, K_m*) – ključ medija pruža AACS Licensing Authority. Riječ je o organizaciji unutar spomenutog AACS LA-a koja se bavi distribucijom pojedinih ključeva potrebnih za uspješnu implementaciju AACS mehanizma. Sam ključ koristi se zajedno s identifikatorom diska za izračun tzv. jedinstvenog ključa diska (eng. *Volume Unique Key*). Kao i većina ključeva koji se koriste u AACS-u, ključ medija je duljine 128 bita.
- **jedinstveni ključ diska** (eng. *Volume Unique Key, K_{vu}*) – ključ koji se koristi za šifriranje naslovnog ključa. Dobije se uporabom jednosmjerne funkcije AES-G koja kao ulaz primi identifikator diska i ključ medija.
- **AES** (eng. *Advanced Encryption Standard*) – je osnovni mehanizam šifriranja i dešifriranja podataka u AACS-u. Sadržaj se šifrira uporabom AES algoritma u CBC (eng. *cipher-block chaining*) modu [10]. Svi ključevi šifriraju se i dešifriraju AES algoritmom u EBC (eng. *electronic codebook*) modu [10]. S obzirom na činjenicu da je većina ključeva duljine 128 bita, jedno AES šifriranje ili dešifriranje je dovoljno. Više o radu AES algoritma može se pronaći u Wikipedijinom članku „Advanced Encryption Standard"[9].
- **AES-G** – je jednosmjerna funkcija koja za ulaz prima dva 128-bitna ključa i iz njih stvara jedan izlazni 128-bitni ključ. Shema koja opisuje rad funkcije nalazi se na sljedećoj slici (Slika 5).



Slika 5. Shema koja opisuje rad funkcije AES-G

- **ključ uređaja** (eng. *Device Key*) – ključevi uređaja koriste se kao oznake kod implementacije revokacijske sheme (*subset difference revocation scheme, SDRS*).
- **ključ obrade** (eng. *Processing Key*) – ovi ključevi su ekvivalentni dugotrajnim ključevima kod implementacije revokacijske sheme (ključevi koji omogućuju prepoznavanje postojanja ovlasti za dešifriranjem sadržaja). Svaki je duljine 128 bita i može se dobiti iz ključeva uređaja. Ključevi obrade koriste se za šifriranje ključa medija.
- **blok ključeva medija** (eng. *Media Key Block*) – blok ključeva medija također se dobije od AACS LA i sadrži listu računala i čitača koji ne posjeduju odgovarajuća prava za pristup šifriranom sadržaju. Ključ medija šifriran s jednim ili više ključeva obrade zapisuje se u spomenuti blok zajedno s indeksima ključeva obrade korištenim kod šifriranja.

3.1. Šifriranje i zapis sadržaja

Šifriranje i zapis sadržaja provode se kroz sljedeće korake (Slika 4):

1. Vlasnik sadržaja isporučuje sadržaj licenciranom replikatoru koji nasumično generira tajni naslovni ključ sadržaja. Sadržaj se potom šifrira pomoću naslovnog ključa preko algoritma AES u CBC modu.
2. Za svaki naslov (ili skup naslova) AACS LA isporučuje blok medijskih ključeva i tajni ključ medija replikatoru. Šifrirani ključevi medija uključuju se u blok medijskih ključeva i samo ovlašteni korisnici imaju mogućnost dešifriranja jednog od tih blokova kako bi dobili izvorni ključ medija.
3. Replikator nasumično generira identifikator diska za dobiveni sadržaj. Taj identifikator koristi se zajedno s ključem medija za izračun jedinstvenog ključa diska preko algoritma AES-G. Naslovni ključ šifrira se potom jedinstvenim ključem diska korištenjem algoritma AES.
4. Napokon, replikator zapisuje blok medijskih ključeva, identifikator diska te šifriran naslovni ključ i sadržaj na disk, zajedno s dodatnim informacijama neizravno povezanim sa samim sadržajem. Identifikator diska pritom se zapisuje na zasebno mjesto u disku ("*burst cut area*"), korisničkim snimačima namijenjenom isključivo za čitanje.

3.2. Dešifriranje i reprodukcija sadržaja

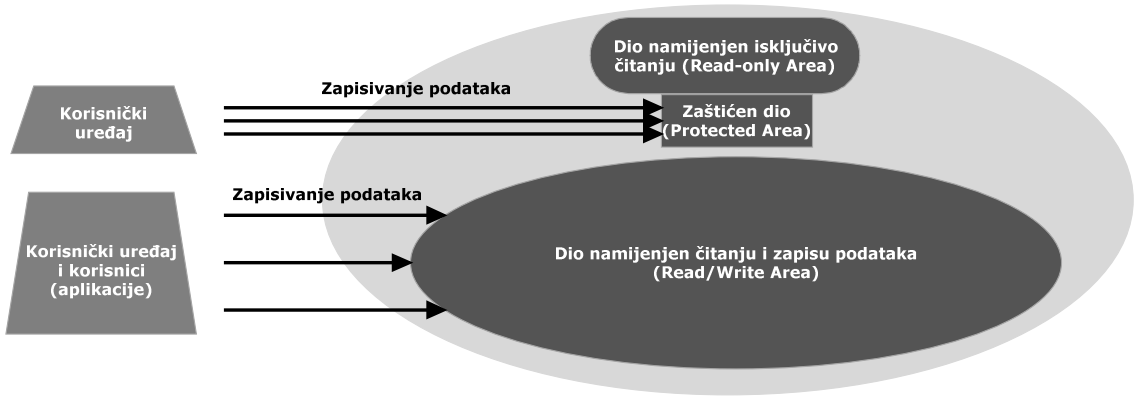
Dešifriranje sadržaja radi reprodukcije provodi se u sljedećim koracima (Slika 4):

1. Ako uređaj za reprodukciju sadržaja ima odgovarajuće ovlasti onda bi korištenjem mehanizma revokacijske sheme (objašnjen u poglavlju 2.1) preko vlastitih ključeva uređaja trebao izračunati ključ obrade. Pomoću ključa obrade može se dešifrirati jedan od ključeva medija zapisan u šifriranim blokovima medijskih ključeva.
2. Uređaj za reprodukciju sadržaja zatim čita identifikator diska i pomoću njega te izračunatog ključa medija dobiva jedinstveni ključ diska uporabom algoritma AES-G.
3. Nakon što se izračuna jedinstveni ključ diska, preko njega je moguće dešifrirati naslovni ključ.
4. Napokon, uređaj za reprodukciju sadržaja dešifrira sam sadržaj korištenjem naslovnog ključa dobivenog u prethodnom koraku. Nakon dešifriranja sadržaja slijedi njegova reprodukcija.

Kod praznih optičkih medija mehanizam zaštite temelji se na logičkoj podjeli medija na tri dijela (Slika 6):

1. **dio namijenjen isključivo čitanju (eng. *Read-only Area*) -** dio optičkog diska na koji se ne mogu zapisivati korisnički podaci. Ovaj dio koristi se za zapis identifikatora medija (eng. *Media Identifier*), 128-bitne vrijednosti koje je jedinstvena za svaki disk. Zapisivanjem takve, nepromjenjive vrijednosti na svaki disk gotovo je nemoguće stvoriti njegovu, u potpunosti identičnu kopiju. Identifikator medija koristi se za računanje autentikacijskog koda (eng. *Message Authentication Code*) zajedno s naslovnim ključem, čime se može odrediti je li naslovni ključ generiran baš za taj disk ili je neovlašteno kopiran s drugog diska. Ovaj dio može sadržavati i blok medijskih ključeva koji se koristi za distribuciju osvježenih medijskih ključeva dijelu namijenjenom čitanju i zapisu podataka (opisan u nastavku poglavlja) [2].
2. **zaštićen dio (eng. *Protected Area*)** - poseban dio diska kojem može pristupati isključivo korisnički uređaj. Aplikacije na korisničkom računalu ne mogu uređaju slati naredbe koje bi ga natjerale da podatke zapisuje ovdje. Umjesto toga, uređaj je sam sposoban za stvaranje i zapisivanje odgovarajućih informacija, ako je to potrebno. Jedini podaci koji se ovdje zapisuju poznati su pod nazivom „Binding Nonce" i predstavljaju posebne vrijednosti preko kojih se mogu izračunati naslovni ključevi diska [2].
3. **dio namijenjen čitanju i zapisu podataka (eng. *Read/Write Area*)** - dio optičkog diska na koji se zapisuje željeni sadržaj, zajedno s blokom medijskih ključeva, šifriranim naslovnim ključem (ili ključevima) i eventualnim pravilima korištenja (eng. Usage Rules). Svaki djelić šifriranih podataka zapisan na disku sadrži vlastiti blok medijskih ključeva, popis naslovnih ključeva (eng. *Title Key File*) koji sadrži naslovne ključeve povezane sa

sadržajem te vlastita pravila korištenja. Pravila korištenja za pojedini djelić šifriranih podataka stvara vlasnik sadržaja. Ona sadrže podatke o tome tko smije pristupati sadržaju i kakva su ograničenja vezana uz njegovo umnažanje te se koriste i kod postupka dešifriranja kako bi se spriječila njihova neovlaštena izmjena [2].



Slika 6. Logička podjela praznih optičkih medija pod zaštitom AACS-a

3.3. Mehanizmi autentikacije

Uz šifriranje i dešifriranje sadržaja potrebna je i ugradnja mehanizma autentikacije između diskova i uređaja za reprodukciju štićenog sadržaja. Takav mehanizam koristi se kako bi se utvrdilo da je uređaj za reprodukciju upravo onaj s odgovarajućim ovlastima za reprodukciju.

Mehanizam autentikacije u AACS-u prilično je jednostavan. Replikator stvara sažetak šifriranog sadržaja i šalje ga specijaliziranim web servisima u AACS LA kako bi se digitalno potpisao preko privatnog ključa entiteta. Takav potpis naziva se certifikat sadržaja. Sažetak se, zajedno s certifikatom sadržaja, zapisuje na optički disk. Uređaj ili aplikacija za reprodukciju posjeduje javni ključ AACS LA-a te preko njega može provjeriti autentičnost certifikata sadržaja. Rezultat neuspješne provjere autentičnosti nemogućnost je reprodukcije sadržaja. Uređaj ili aplikacija za reprodukciju sadržaja također stvara sažetak dešifriranog sadržaja i uspoređuje ga sa sažetkom zapisanim na disku. Na taj način provjerava se je li narušen integritet zaštićenog sadržaja te se, ukoliko provjera bude neuspješna, reprodukcija zabranjuje.

3.4. Dodatni mehanizmi zaštite

Uz opisane, AACS ima ugrađene i dodatne mehanizme od kojih svaki na svoj način pomaže pri zaštiti sadržaja od neovlaštenog umnažanja ili pristupa. Radi se o digitalnim vodenim žigovima i implementaciji tzv. *traitor tracing* tehnike, audio vodenim žigovima te tehnici vođenog umnažanja.

3.4.1. *Traitor tracing*

Traitor tracing je tehnika otkrivanja narušavanja autorskih prava koja pokušava otkriti sam izvor kompromitacije. Radi na sljedećem principu: distributer zapisuje jedinstvenu vrijednost na svaku kopiju koju izdaje. Pomoću nje onda po objavljivanju neke od kopija može doći do onoga tko je tu kopiju neovlašteno objavio.

AACS standard omogućuje šifriranje različitih inačica kratkih dijelova filma pomoću različitih ključeva. Pojedini uređaj može dešifrirati samo po jednu inačicu svakog od tih dijelova. Umetanjem digitalnih vodenih žigova (eng. *Digital Watermark*) u različite dijelove filma i analizom koji se od žigova pojavljuju u piratiziranoj inačici moguće je utvrditi kompromitirane ključeve i opozvati ih.

3.4.2. Audio vodeni žigovi

U konačnoj specifikaciji AACS standarda opisana je i implementacija sustava za upravljanjem digitalnih prava poznatog pod imenom „Cinavia“. Radi se o sustavu koji se sastoji od dvije osnovne komponente: posebnog i neprimjetnog audio vodenog žiga (eng. *Audio Watermark*) koji se ugrađuje u štićeni sadržaj te uređaja koji može opaziti takve

žigove. Primjeri takvih uređaja su Playstation 3 i noviji uređaji za reprodukciju sadržaja *Blu-ray* diskova. Kod reprodukcije štićenog sadržaja uređaj zadužen za reprodukciju u jednom trenutku prepoznaje takav vodeni žig i određuje ima li adekvatne ovlasti za nastavak reprodukcije. Ako to nije slučaj (primjerice kod neovlaštenih kopija komercijalnih *Blu-ray* diskova gdje se AACS ne koristi), prekida se reprodukcija i ispisuje odgovarajuća poruka.

3.4.3. Vođeno umnažanje

Pod vođenim umnažanjem (eng. *Managed Copy*) podrazumijeva se mehanizam koji omogućuje krajnjim korisnicima da izrađuju ovlaštene kopije zaštićenog sadržaja, a koje će ostati zaštićene AACS-om.

Postupak zahtijeva da uređaj koji provodi umnažanje kontaktira poslužitelj vlasnika sadržaja na Internetu i dobije odgovarajuće ovlasti. Detaljan opis načina na koji je moguće obavljati vođeno umnažanje sadržaja zaštićenog AACS standardom nalazi se u konačnim specifikacijama standarda [1].

4. Sigurnost standarda

Uz sve opisane sigurnosne mehanizme čini se da je AACS vrlo siguran i robustan sustav. Ipak, javlja se sljedeće pitanje: ako je to slučaj, zašto je na tržištu i dalje prisutan tako velik broj nelegalnih kopija raznovrsnih sadržaja zapisanih na HD DVD i *Blu-ray* diskovima?

Odgovor leži u činjenici da su zlonamjerni korisnici i napadači uspjeli otkriti mnoge od ključeva koji se koriste u postupcima šifriranja i dešifriranja sadržaja štićenog AACS standardom. Od prosinca 2006. godine, otkriveni su naslovni ključevi za svaki od dotad objavljenih naslova analizom memorijskog prostora koji koriste neki programski dekoderi i aplikacije za reprodukciju HD DVD i *Blu-ray* sadržaja. Najčešće se radilo o aplikacijama namijenjenim radu na operacijskim sustavima Windows (primjerice WinDVD). Takve analize mogu se relativno jednostavno provesti posebnim programima za pronalaženje pogrešaka (eng. *debugger*) koji su u mogućnosti pregledati memorijski prostor u trenutku kada aplikacije reproduciraju zaštićen sadržaj. Ranjivije aplikacije će potrebne ključeve za dešifriranje sadržaja imati na vidljivom mjestu u memoriji.

Jednom kada je naslovni ključ kompromitiran, sadržaj s tim naslovom može biti šifriran ili dešifriran po želji, čime se zaobilazi standardni AACS mehanizam. Uz naslovne ključeve, kompromitirani su i ključevi obrade, praktički na isti način, pregledom memorijskog prostora koje koriste ranjivije aplikacije za reprodukciju zaštićenog sadržaja. Isto tako, postoje naznake da su otkriveni i mnogi ključevi uređaja te privatni ključevi računala (eng. *Host Private Keys*) koji se koriste za autentikaciju između samog računala i uređaja za reprodukciju sadržaja.

Ubrzo potom, pojavili su se prvi nezaštićeni filmovi u HD DVD i *Blu-ray* formatima. Neki od ključeva, poput ključa obrade bili su javno objavljeni na Internetu, nakon čega je AACS LA bio primoran poslati službena upozorenja kako bi se povukla njihova objava.

Premda AACS posjeduje mehanizam za ukidanje starih i kompromitiranih ključeva te je u mogućnosti objaviti nove (kroz nove objave zaštićenog sadržaja) problem je u činjenici da se kompromitiranim ključevima starijih inačica nekog sadržaja omogućuje njegovo, barem privremeno, neovlašteno umnažanje i reproduciranje. Neki od ključeva mogu se iskoristiti i za kompromitiranje novijih sadržaja.

Nadalje, sve skupa jasno upućuje na pravi problem prisutan kod svih sustava za upravljanje digitalnim pravima, a koji omogućuju aplikacijama na osobnim računalima reprodukciju zaštićenog sadržaja. Bez obzira na to koliko su složeni mehanizmi šifriranja, ne postoji mogućnost pružanja potpune zaštite jer ključevi korišteni u postupku dešifriranja zaštićenog sadržaja moraju biti prisutni negdje u memoriji računala kako bi reprodukcija bila moguća. Današnja osobna računala ne pružaju adekvatnu mogućnost zaštite od neovlaštenog pregleda memorijskog prostora u potrazi za takvim ključevima.

Jedino rješenje ovdje je promjena načina na koji osobna računala funkcioniraju uvođenjem koncepta povjerljivog računarstva (eng. *Trusted Computing*). Takav koncept temelji se na činjenici da se računala u svakom trenutku ponašaju sukladno s nekim, konzistentnim obrascima kojima upravljaju i programske i sklopovske komponente primjenom kriptografije. Više o samom konceptu može se pronaći u literaturi [11].

4.1. Usporedba AACS-a i CSS-a

Sigurnost AACS sustava stalan je predmet rasprava među stručnjacima iz različitih područja. Kao nasljednik sustava za zaštitu sadržaja na DVD-ima (CSS), AACS je kvalitetu zaštite trebao unaprijediti ispravljajući najznačajnije mane prethodnika. Problem je u tome što je CSS nakon 1999. godine i objave programa DeCSS (koji može dešifrirati bilo koji sadržaj zaštićen CSS sustavom) u potpunosti izgubio funkcionalnost.

Osnovna razlika između AACS-a i CSS-a leži u organizaciji ključeva dešifriranja unutar uređaja za reprodukciju. Kod CSS-a svi uređaji istog modela imaju jednak ključ za dešifriranje. Sadržaji su šifrirani prema ključu ovisnom o naslovu, a taj je ključ zatim šifriran pomoću ključa vezanog uz model uređaja. Zbog toga svaki disk sadrži nekoliko stotina ključeva šifriranja, po jedan za svaki licencirani model uređaja za reprodukciju. Takav pristup omogućuje opoziv tek određenog modela uređaja za reprodukciju izuzimanjem njegovog ključa dešifriranja iz budućih izdanja. Dodatni nedostatak je i povećana ranjivost zbog jednog ključa pohranjenog u velikom broju uređaja, što jasno pokazuju brojni slučajevi probijanja zaštite iz sredine 90-ih godina prošlog stoljeća [3].

Kod AACS-a svaki uređaj ima jedinstven skup ključeva za dešifriranje koji se koriste u mehanizmu difuznog šifriranja (ključevi uređaja). Takav pristup vlasniku licence omogućuje opozivanje pojedinog uređaja za reprodukciju, odnosno njegova skupa ključeva za dešifriranje. Ako zlonamjeran korisnik probije zaštitu određenog uređaja i objavi njegove ključeve, AACS LA može povući kompromitirane ključeve uređaja i onemogućiti reprodukciju budućih naslova na spomenutom uređaju [3].

Uz samu organizaciju ključeva, kod AACS-a su prisutni i *traitor tracing* te digitalni audio žigovi. Što se algoritama šifriranja tiče, AACS koristi 128-bitne ključeve i algoritam AES, dok CSS koristi tek 40-bitne ključeve u kombinaciji sa specifičnim, vlastitim algoritmom šifriranja.

4.2. Napadi na AACS

Već i prije objave AACS tehnologije na tržištu su postojale velike sumnje u njen konačan uspjeh. Jedan od osnovnih razloga bila je sličnost s CSS-om, sustavom koji na kraju krajeva nije uspio pružiti učinkovitu zaštitu sadržaja od neovlaštenog pristupa i umnažanja. Autori aplikacije DeCSS koja je uspješno probila CSS zaštitu procijenili su kako će AACS biti probijen krajem 2006. godine ili početkom 2007. (početne specifikacije bile su objavljene u travnju 2005.).

4.2.1. Zaobilaženje zaštite metodom “digitalne rupe“

Premda je u razvoju AACS standarda velika pažnja posvećena sigurnosnim mehanizmima od zaštite sadržaja na optičkim medijima, pa sve do njegove reprodukcije na osobnim računalima korisnika, u srpnju 2006. godine otkrivena je mogućnost kopiranja kadrova filmova s pojedinih HD DVD i *Blu-ray* diskova korištenjem funkcije *Print Screen* na operacijskim sustavima Windows. Teoretski, na taj je način moguće izraditi savršenu kopiju cijelog filma slično načinu na koji su se kopirali filmovi na DVD diskovima prije probijanja CSS-a. Ideja se temelji na automatizaciji *Print Screen* mogućnosti nekih aplikacija za reprodukciju HD DVD i *Blu-ray* sadržaja (npr. Intervideov WinDVD) za sve kadrove filma. Za sada niti jedna tako izrađena kopija filmova s HD DVD i *Blu-ray* diskova nije otkrivena.

Opisan nedostatak uklonjen je novijim inačicama aplikacija za reprodukciju filmova. Ipak, ostaje kao primjer neizravne ranjivosti AACS-a koja je prisutna i kod svih ostalih sustava za upravljanje digitalnim pravima, a poznata je pod slikovitim nazivom “analogna rupa“ (eng. *analog hole*). Riječ je o metodi zaobilaženja sustava za upravljanje digitalnim pravima koja se temelji na iskorištavanju činjenice da je za reprodukciju zaštićenog sadržaja potrebna njegova pretvorba iz digitalnog u analogni oblik (svjetlosne i zvučne komponente kroz prikaz slika, reprodukciju filma i glazbe itd.). Takvim, analognim signalom moguće je po volji rukovati jer sustavi za upravljanje digitalnim pravima nad njime nemaju nikakve kontrole.

4.2.2. Probijanje zaštite otkrivanjem ključeva šifriranja

U prosincu 2006. godine korisnik s aliasom *muslix64* objavio je aplikaciju BackupHDDVD i njen izvorni programski kod na forumu za DVD dešifriranje internetske stranice *Doom9* (http://www.doom9.org/). BackupHDDVD se može koristiti za dešifriranje sadržaja zaštićenog AACS-om pod uvjetom da je poznat ključ šifriranja. Autor je tvrdio da je

naslovne ključeve i ključeve diskova jednostavno pronašao u glavnoj memoriji prilikom reprodukcije HD DVD filmova na vlastitom računalu.

U siječnju 2007. isti je autor objavio novu inačicu BackupHDDVD-a koja je imala podršku za određivanje jedinstvenog ključa diska. Otprilike u slično vrijeme na forumu su se javili i ostali korisnici s detaljnim uputama kako otkriti raznovrsne naslovne ključeve analizom radne memorije prilikom rada programa WinDVD. U to vrijeme na Internetu se pojavila i prva nelegalna kopija nekog HD DVD filma (Serenity).

Tijekom 2006. i 2007. godine došlo je do otkrivanja i javne objave velikog broja ključeva vezanih uz rad AACS-a. Radi se o naslovnim ključevima, ključevima uređaja, privatnim ključevima računala i ključu obrade za prvu inačicu bloka medijskih ključeva preko kojeg se mogao dešifrirati sav AACS-om zaštićen sadržaj objavljen do tog trenutka. Logično, sve više se nezaštićenih HD DVD i *Blu-ray* filmova počelo pojavljivati na Internetu. Svojevrstan vrhunac napada dogodio se 2007. godine kada je na velikom broju internetskih stranica objavljen spomenuti ključ obrade vezan uz prvu inačicu bloka medijskih ključeva. AACS LA se, zajedno s udrugom MPAA (eng. Motion Picture Association of America), pokušao obračunati s javnim otkrivanjem ključeva slanjem službenih upozorenja i molbi za uklanjanjem ključa te svih poveznica i članaka vezanih uz njega. Upozorenja su se pozivala na DMCA (eng. *Digital Millenium Copyright Act*) koji predstavlja nadogradnju američkog zakona o autorskim pravima u kojem se kriminalizira stvaranje i širenje tehnologija namijenjenih zaobilaženju sustava za zaštitu autorskih prava. Prema tom zakonu, zaobilaženje tehnologije koja štiti određeni sadržaj ilegalno je ukoliko je počinjeno s namjerom nanošenja štete vlasniku autorskih prava. Većina internetskih stranica postupila je u skladu s upozorenjima.

Kriza je eskalirala u svibnju 2007. godine kada je poznata stranica za razmjenu novosti i internetskog sadržaja, Digg, zaprimila spomenuto upozorenje. Zbog njega su sa stranice uklonjeni svi sporni članci, a velikom je broju korisnika koji su ponovno stavljali kontroverzne sadržaje zabranjen daljnji pristup stranici. To je pokrenulo svojevrsnu digitalnu revoluciju u kojoj je došlo do masovne objave spornih ključeva i članaka, kako na Diggu, tako i na cijelom Internetu. Autori su prvenstveno bili krajnji korisnici koji su tako pokazali svoje nezadovoljstvo AACS-om i sve rigoroznijim metodama upravljanja digitalnim pravima, te načinom na koji takve tehnologije mogu ograničiti prava vlasnika legalnih kopija.

U travnju 2007. godine konzorcij za AACS tehnologiju objavio je da su kompromitirani ključevi uređaja koje su koristile aplikacije poput Cyberlinkovog PowerDVD-a te InterVideovog WinDVD-a povučeni. Objavljene su zakrpe koje su trebale pružiti bolju zaštitu novih ključeva. Da bi mogli reproducirati nove filmove i ostale zaštićene sadržaje, korisnici su bili primorani koristiti objavljene zakrpe.

U svibnju 2007. godine objavljen je ključ obrade nužan za dešifriranje nove inačice bloka medijskih ključeva. Kao što je već navedeno, nikakvi složeniji mehanizmi šifriranja nisu u mogućnosti spriječiti korisnike da analiziraju radnu memoriju prilikom reprodukcije zaštićenog sadržaja i pronađu ključeve koji se tamo moraju nalaziti.

Narednih godina uslijedilo je još nekoliko povlačenja kompromitiranih ključeva, objava zakrpi s novim ključevima te, ubrzo potom, i objava pronađenih ključeva kojima se dešifriraju novi blokovi medijskih ključeva. Trenutno je aktualna sedamnaesta inačica blokova medijskih ključeva dok su posljednji javno objavljeni otkriveni ključevi bili vezani uz njenu desetu inačicu.

Određen napredak očito je ostvaren, premda su nove kontroverze, što zbog konkretne implementacije AACS-a, a što zbog prirode samih sustava upravljanja digitalnim pravima, vrlo izvjesne.

5. Nedostaci AACS sustava

AACS sustav za zaštitu digitalnog sadržaja kao i sve ostale tehnologije upravljanja digitalnim pravima od samih početaka razvoja prate dva velika nedostatka.

Prvi je vezan uz ograničavanje uporabe sadržaja vlasnicima legitimnih kopija. Tehnologije upravljanja digitalnim pravima temelje se na činjenici da moraju ostvariti učinkovit mehanizam koji će zaštititi sadržaj od neovlaštenog pristupa i neovlaštenog umnažanja. To je vrlo teško ostvariti bez da se do neke razine vlasnicima legitimnih kopija zaštićenog, izvornog sadržaja ne ograniči ili barem donekle ne oteža pristup i upravljanje takvim sadržajem. Uvođenje ograničenja nad uporabom takvih sadržaja

može predstavljati narušavanje zakonskih prava vlasnika legalnih kopija (eng. *fair use rights*). Uz to, tehnologije upravljanja digitalnim pravima otežavaju, a u nekim slučajevima i potpuno onemogućuju učinkovito arhiviranje sadržaja. Protivnici sustava za upravljanje digitalnim pravima ističu kako takvi sustavi nisu učinkoviti u sprječavanju ilegalnih kopija sadržaja koje bi trebali štititi, jer niti jedan takav sustav nije u potpunosti otporan na napade. Uz sve pravne i korisničke kontroverze jedno je sigurno, AACS je punokrvna tehnologija upravljanja digitalnim pravima i kao takva će uvijek biti povezana sa spomenutim kontroverzama te nailaziti na velik otpor dijela legitimnih krajnjih korisnika, a i onih koji to nisu.

Drugi osnovni nedostatak AACS sustava povezan je s tehničkom prirodom tehnologija upravljanja digitalnim sadržajem. Naime, vlasnici legitimnih kopija zaštićenog sadržaja moraju biti u mogućnosti takav sadržaj koristiti i to na način da im je omogućen pristup svim alatima i informacijama potrebnim za njegovu reprodukciju. Ipak, nakon predaje kriptografskog algoritma, zajedno s ključevima i šifriranim sadržajem korisnicima na današnjim osobnim računalima, samo je pitanje vremena kada će doći do kompromitiranja sustava. Osnovni problem vezan je uz nužno prisustvo tajnih ključeva u radnoj memoriji osobnih računala prilikom reprodukcije sadržaja. Tako nešto, bez značajnije promjene načina na koji suvremena osobna računala funkcioniraju, nije moguće ostvariti. Napokon, postavlja se pitanje isplativosti ulaganja velikih novčanih sredstava i ljudskih resursa u tehnologiju koja je u današnjim uvjetima osuđena na neuspjeh.

6. Zaključak

Analizom AACS sustava za zaštitu digitalnog sadržaja brzo se mogu uočiti njegovi osnovni i prilično veliki nedostaci – ograničavanje uporabe zaštićenog sadržaja vlasnicima legitimnih kopija te nužna dostupnost kriptografskih algoritama s tajnim ključevima i šifriranim sadržajem na računalima korisnika. Spomenuti nedostaci ujedno su i nedostaci cjelokupne tehnologije upravljanja digitalnim pravima te ih nije moguće ukloniti bez drastičnih promjena u distribuciji i pristupu zaštićenim sadržajima.

Ipak, određen napredak objavom AACS tehnologije je postignut. Riječ je o iznimno složenom i naprednom mehanizmu koji je u stanju poprilično otežati zlonamjernim korisnicima probijanje njegove zaštite i objavu rezultata. Pozitivan pomak djelomično se očituje u činjenici da zlonamjerni korisnici sve više zaostaju u svojim pokušajima da kompromitaciju cjelokupne tehnologije zadrže aktualnom. Koliki će napredak ostvariti eventualne nove tehnologije na ovom području, ostaje za vidjeti.

Budućnost tehnologija upravljanja digitalnim pravima temelji se upravo na sustavima kao što je AACS. Riječ je o sustavima koji su u stanju dinamički prepoznati uređaje i aplikacije s važećim pravima pristupa sadržaju i njegove reprodukcije. Po kompromitaciji tajnih ključeva pojedinih uređaja ili aplikacija, takvi sustavi mogu povući njihove postojeće ovlasti te ih ponovno dodijeliti objavom nove serije tajnih ključeva i sigurnosnih zakrpi. Analizom povijesti napada na AACS te trenutnih sigurnosnih trendova vezanih uz njega, može se zaključiti da je spomenuti pristup prilično uspješan u tome da uspješno obeshrabri daljnje napore većine zlonamjernih korisnika i dodatno im otežа posao svakom novom objavljenom zakrpom. Kao takav, neće nikada biti u potpunosti probijen. Uz to, eventualni novi mehanizmi zaštite vjerojatno će učiniti buduće sustave upravljanja digitalnim pravima još uspješnijima.

7. Reference

[1] AACS LA: Advanced Access Content System Home Site, http://www.aacsla.com/home, veljača 2011.

[2] Henry, K., Sui, J., Zhong, G.: An Overview of the Advanced Access Content System (AACS), David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Kanada, 2007.

[3] CARNet, Nacionalni CERT i LS&S: Upravljanje digitalnim pravima (DRM), dokument iz područja računalne sigurnosti, listopad 2007.

[4] Liddell, C.: Advanced Access Content System, Power Point prezentacija, 2007.

[5] Wikipedia: Advanced Access Content System, http://en.wikipedia.org/wiki/Advanced_Access_Content_System, veljača 2011.

[6] Wikipedia: Security of Advanced Access Content System, http://en.wikipedia.org/wiki/Security_of_Advanced_Access_Content_System, veljača 2011.

[7] Wikipedia: AACS encryption key controversy, http://en.wikipedia.org/wiki/AACS_encryption_key_controversy, veljača 2011.

[8] Wikipedia: Digital rights management, http://en.wikipedia.org/wiki/Digital_rights_management, veljača 2011.

[9] Wikipedia: Advanced Encryption Standard, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard, veljača 2011.

[10] Wikipedia: Block cipher modes of operation, http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation, veljača 2011.

[11] Wikipedia: Trusted Computing, http://en.wikipedia.org/wiki/Trusted_Computing, veljača 2011.

[12] Wikipedia: Integrity, http://en.wikipedia.org/wiki/Integrity, veljača 2011.

[13] Naor, D., Naor, M., Lotspiech, J.: Revocation and Tracing Schemes for Stateless Receivers, znanstveni članak, veljača 2001., www.wisdom.weizmann.ac.il/~naor/PAPERS/2nl.pdf, veljača 2011.