Xifrat de fitxers ACA de HD-DVD amb AACS

Pau Figueras Collelldemont

Resum

Aquest projecte tracta de com es protegeixen els discs HD-DVD fent servir l'estàndard de protecció AACS de molt recent creació. S'expliquen també els mètodes criptogràfics que s'utilitzen: AES-128, SHA-1 i CMAC.

Dins dels discs HD-DVD hi ha dos tipus de continguts que es poden protegir, per una banda està el contingut audiovisual i per l'altra els fitxers de recursos avançats (ARF) que composen els menús de navegació, efectes de so, programació... i que s'acostumen a empaquetar dins d'uns fitxers anomenats ACA

Amb la finalitat d'acabar d'entendre tot el mecanisme de l'AACS i en concret el mètode de protecció d'aquests ACA s'ha dissenyat i implementat una aplicació que protegeix, desprotegeix i verifica aquests ARF abans d'empaquetar-se dins d'un fitxer ACA. Obtenint així fitxers ACA xifrats quan aquests es creen a partir dels ARF's protegits.

1. Introducció

La raó d'haver escollit aquest projecte és perquè em permetia combinar dos temes que m'interessen i dels que sempre he volgut saber més: la criptografia i el món audiovisual en alta definició (HD)

Poder ajuntar en un sol projecte aquests dos temes m'ha motivat enormement a portar a bon terme el treball fins al punt de no quedar-me en el tema inicial que consistia només a xifrar uns fitxers, no he pogut evitar voler descobrir com es desxifraven, verificaven i com funcionava tot el sistema de protecció del HD-DVD tant d'aquests fitxers com d'altres.

2. HD-DVD

El HD-DVD (High-Definition Digital Versatile Disc) de Toshiba és juntament amb el Blu-Ray un dels dos candidats a ser el disc òptic definitiu per emmagatzemar contingut audiovisual en l'alta definició, substituint així la definició estàndard (SD) que ofereixen els DVD actuals.

Els discs HD-DVD ofereixen 17 Gb d'espai d'emmagatzematge per capa, és a dir, els dics de doble capa tenen 34 Gb d'espai i els futurs discs de triple capa 51 Gb. L'objectiu d'aquests discs és emmagatzemar el vídeo i l'àudio amb la millor qualitat possible, arribant a una resolució de 1920×1080 píxels.

3. AACS al HD-DVD

Amb la comercialització de nous suports audiovisuals en alta definició, les companyies propietàries del contingut van estar treballant per a trobar un nou sistema per protegir els seus discs amb l'objectiu d'intentar evitar les falles de seguretat que tenien els sistemes de protecció dels DVD.

Un grup format per les empreses més poderoses del sector van idear un estàndard anomenat AACS (Advanced Access Content System) que oferia una protecció més robusta que la que hi havia als DVD convencionals. Alguns dels punts forts eren que es feia servir un nombre més elevat i variat de claus (cada títol tenia les seves pròpies), era un sistema dinàmic en constant actualització que permetia revocar reproductors dels que s'havia demostrat que no eren prou segurs per a la gestió de l'estàndard

AACS fa servir tres mètodes criptogràfics batant potents:

- AES-128: Està considerat un dels algorismes de xifrat simètrics més potents de l'actualitat. El concepte de xifrat simètric es refereix al fet que per xifrar i per desxifrar es fa servir la mateixa clau.

  La mida dels blocs i de les claus pots ser de 128, 192 o de 256 bits, permetent escollir la combinació que més desitgi. Tot i així, està marcat com a estàndard una mida de 128 bits de clau i de bloc.

  En el cas de l'AACS que fa servir 128 bits de mida de clau i de bloc, el xifrat es farà en 10 voltes composades de quatre funcions invertibles que aporten diferents nivells de protecció al xifrat.

- SHA-1: És una funció Hash creada pel NIST (National Institute of Standards and Technology). La finalitat d'aquesta funció aplicada a l'AACS és obtenir un resum del fitxer de tal manera que una lleugera variació del seu contingut alteraria el valor de hash generat, d'aquesta manera es pot validar la integritat del fitxer i assegurar que no ha estat modificat amb posterioritat.

- CMAC: també ofereix un resum de les dades que se li passen però amb l'afegit que inclou una clau en aquest càlcul (en el cas de l'AACS la clau és de 128 bits). El càlcul basat en xifrat en bloc CBC (Cipher Block Chaining) i fa servir AES128 per xifrar els resultats parcials.

Les claus més imortants que intervenen en el AACS són les següents.

- Title Key (Kt): És la clau que permet desxifrar el contingut protegit. Aquesta clau es troba emmagatzemada juntament amb altres Title Keys dins del fitxer xifrat "Title Key File" (TKF).

  Inicialment, aquesta clau és totalment aleatòria ja que el mètode de xifrat on es fa servir (AES-128) no té claus febles ni subfebles

- Volume Unique Key (Kvu): És la clau més important de tot el conjunt, s'encarrega de xifrar el fitxer on es troben emmagatzemades les "Title Keys", aquesta clau és l'objectiu de tothom que vulgui desxifrar el contingut protegit amb AACS i per tant s'ha de protegir amb molta cura.

- Volume ID (VID): Nombre únic per llançament, està format per dues parts: una que es troba a l'àrea BCA i l'altre que es troba a l'àrea Lead-In dels discs.

- Media Key Block: Fitxer facilitat per AACSLA que s'inclou a tots els HD-DVD protegits que permet obtenir la Media Key (Km).

- Media Key (Km): Clau que es genera a partir del Media Key Block.

- Device Keys: Són les claus que fa servir el reproductor per obtenir la Media Key (Km) a partir del MKB, si el reproductor ja no està validat per AACS, el MKB farà que la Km obtinguda no sigui la correcta i el disc no es pugui reproduir.

4. Tipus de protecció

- Protecció del contingut:

  El contingut audiovisual es protegeix dividint en blocs 1920 bytes els arxius de vídeo i xifrant-los amb, es calcula una nova clau a partir de la inicial i es xifra tot amb AES

- Protecció dels elements de recursos avançats:

  Els elements avançats són aquells que s'utilitzen com a material de navegació del disc, aquest grup inclou imatges, animació, programació del disc...

  Existeixen cinc mètodes diferents de protegir els fitxers, cada un aporta diferents mètodes de seguretat: xifrat, integritat, signatura digital...

  Segons el tipus de fitxer a xifrar i depèn de si el destí del fitxer és estar a un disc o a un emmagatzematge permanent, s'escull una protecció o una altra. Segons l'estàndard AACS es segueix el següent criteri:

Tipus de Fitxer	**Segons el destí del fitxer**	
	Disc	**Emmagatzematge Persistent**
JPG, PNG, CVI, MNG, LPCM/WAV, OTF, TTF, TTC	Xifrat	Xifrat
XML (XPL, MMF, XMU, XTS, XAX, XSS...)	Hash	MAC
ECMAScrip: JS	Xifrat i Hash	MAC
Fitxers sense protecció (altres)	No protegit	No protegit

Taula 1. – *Mètodes de protecció de d'ARF's*

Una vegada els fitxers estan protegits, es recomana que s'agrupin tots dins d'un fitxer d'empaquetament anomenat "ACA", aquesta acció permet endreçar els fitxers i millorar la velocitat d'accés a aquests..

- Xifrat: Protegeix totalment el contingut del fitxer xifrant-lo amb el robust algorisme AES-128 – Rijndael. Li aporta confidencialitat ja que només es pot recuperar el fitxer protegit si es disposa de la clau de 128 bits que s'ha fet servir per xifrar-lo.

- Hash: Assegura la integritat de les dades protegides emmagatzemant el valor de SHA-1 del fitxer a protegir dins la Taula de Hash #2 del disc AACS. Un dels punts febles d'aquest mètode és que tot s'emmagatzema en text clar, i només desencapsulant el fitxer protegit es pot recuperar l'original.

- Xifrat i Hash: És el més segur dels cinc mètodes, per una banda xifra el contingut amb l'algorisme AES-128 – Rijndael aportant confidencialitat al fitxer i per l'altra emmagatzema diversos valors de SHA-1 a la Taula de Hash #2 corresponents a blocs de 512 bytes del contingut xifrat.

- MAC: Assegura la integritat i la signatura de les dades protegides emmagatzemant el valor de CMAC del fitxer als últims 16 bytes del fitxer AACS. Un dels punts febles d'aquest mètode és que tot s'emmagatzema en text clar, i només desencapsulant el fitxer protegit es pot recuperar l'original, però en canvi per validar el fitxer s'ha de saber la clau amb la que s'ha creat la CMAC

5. Desprotecció i verificació

Abans de fer servir les taules de hash es comprova que el seu propi valor de hash no ha variat, per això s'ha de consultar el fitxer CONTENT_CERT.AACS que AACSLA ha signat durant la replicació del disc.

El reproductor a partir de les seves Device Keys i la MKB del disc ha d'anar seguint la relació de claus que s'ha vist anteriorment a la figura 6 fins a trobar la Title Key necessària per desprotegir un bloc de contingut audiovisual o un ARF (fitxer de navegació).

6. Implementació

L'aplicació s'ha implementat en C++ per poder-la compilar i executar des de Windows i des de Linux. Per la compilació en Windows s'ha utilitzat l'aplicació Microsoft Visual Studio 6.0 i per la compilació en Linux el compilador g++ versió 2.95.

Per poder protegir els fitxers cal fer servir tres classes criptogràfiques: AES/Rijndael, SHA1 y CMAC. Degut a la complexitat de la programació del AES/Rijndael i del SHA-1 s'ha decidit fer servir dues de les implementacions de codi lliure disponibles les qual són de les més utilitzades en aplicacions que necessiten d'aquests mètodes criptogràfics. En canvi per a la implementació de la CMAC s'ha decidit programar-la tota per dues raons: primer perquè el funcionament està molt ben documentat al "Recomendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication" i en segon lloc perquè com a mínim volia tenir l'oportunitat de programar un algorisme criptogràfic.

El programa s'ha dividit en els següents fitxers:

- main.cpp: Programa principal, s'encarrega de rebre els paràmetres que indica l'usuari, generar les rutes dels fitxers resultants i necessaris per a la protecció, comprovar que els fitxers que s'utilitzaran existeixen, escollir el tipus de protecció o desprotecció que s'utilitzarà en cada cas i mostrar els errors que puguin sorgir relacionats amb aquests aspectes.
- encapsula_fitxer.cpp: És on es troben els cinc mètodes per protegir i els corresponents cinc mètodes per desprotegir i verificar els fitxers. També hi ha un mètode que afegeix el valor de hash a la Taula de Hash #2 de AACS.
- encapsula_fitxer.hpp: Capçalera del fixer encapsula_fitxer.cpp
- cmac.cpp: S'encarrega de generar la CMAC a partir d'un text que se li passa i d'una clau.
- cmac.hpp: Capçalera de cmac.cpp
- externes/rijndael.cpp: Implementació de xifrat AES128 de codi lliure. Rep un búffer de text i una clau de 16 bytes i el torna xifrat.
- externes/rijndael.hpp: Capçalera de rijndael.cpp.
- externes/sha1.cpp: Implementació de signatura SHA1 de codi lliure. Rep un fitxer i torna el seu valor de SHA1, que equival a un "resum" únic del fitxer.
- externes/sha1.hpp: Capçalera de sha1.cpp.

7. Interpretació dels resultats

Tan important com el fet de poder protegir i desprotegir els fitxers és l'estudi dels resultats que ofereix el programa, l'encapsulació indica els resultats que s'obté de les funcions SHA-1 i CMAC.

La desprotecció s'ha fet de tal manera que s'intenta emular, dins les possibilitats, el comportament d'un reproductor AACS davant d'un fitxer protegit, es podrien extreure uns quants punts que cal destacar:

- Desencapsulació: No acostuma a fallar ja que es limita a treure del fitxer protegit les capçaleres i a desxifrar-lo si s'escau, en aquest punt no es valida res, ni tan sols si el fitxer obtingut té sentit.
- Validació de la integritat: Igual que faria un reproductor AACS, abans d'acceptar un fitxer que s'ha protegit per CMAC o per Hash és mirar que els valors que correspondrien al fitxer encapsulat són iguals que els valors novament generats a partir del fitxer desencapsulat. Això assegura que ningú ha modificat el contingut del fitxer protegit després d'haver-lo encapsulat (cosa que seria molt fàcil ja que tret dels dos mètodes on intervé el xifrat, tot s'emmagatzema en text clar).
    - CMAC: Es comprova si la CMAC emmagatzemada als últims bytes del fitxer protegit coincideix amb la generada amb la del fitxer desprotegit que es genera.
    - HASH: Es comprova si el valor de SHA1 de la Taula de Hash #2 que està apuntat per un apuntador emmagatzemat al fitxer protegit, coincideix amb el valor de SHA1 generat a partir del fitxer desprotegit que es genera.
- Validació del nom del fitxer: Tot i que sembli una comprovació sense importància, el fet de comprovar que el nom del fitxer emmagatzemat dins del fitxer protegit és el mateix que el nom del fitxer real ens assegura que no s'està intentant fer passar un fitxer per un altre, cosa que podria ser un gran perill perquè es podria executar codi maliciós dins el reproductor.

- Comportament del reproductor AACS: Després de desprotegir i desencapsular els fitxers, el reproductor AACS pot prendre dues decisions:
- Acceptar el fitxer: Quan el fitxer s'ha desencapsulat correctament i no ha fallat cap verificació (ni aquestes dues ni les que no s'han pogut implementar per falta d'accés a cert contingut xifrat dels discs, com per exemple verificar que la Taula de Hash #2 no ha estat modificada), el reproductor procedeix a fer servir el fitxer.
- Descartar el fitxer: Només pel fet que hagi fallat alguna de les verificacions, el reproductor descartarà el fitxer i actuarà com si el fitxer no existís, mostrant un error.

8. Conclusions

Els objectius s'han anat complint en gran part, m'hauria agradat anar una mica més lluny amb el xifrat i poder-lo provar en discs HD-DVD reals però malauradament no disposava de tecnologia suficient per portar-ho a terme. Tret d'això, em sento molt satisfet de fins on he pogut arribar, s'ha superat l'objectiu inicial de xifrar fitxers ACA i s'ha pogut desxifrar i verificar el contingut protegit. També s'ha pogut fer un estudi del funcionament de l'AACS amb la resta d'elements del disc, que inicialment no estava previst però que he trobat molt útil i interessant per acabar d'entendre punts que no em quedaven del tot clars.

En quan a la criptografia, el fet de poder-me familiaritzar amb l'aplicació pràctica de funcions criptogràfiques i fins i tot poder-ne programar una, m'ha ajudat enormement a entendre més els conceptes que havia après a nivell teòric, ara ho veig tot més clar i entenc perquè s'apliquen certs mètodes en detriment d'altres.

L'aplicació que s'ha desenvolupat s'ha fet de tal manera que es pot utilitzar en molts altres escenaris que no cal que estiguin forçosament relacionats amb AACS ni HD-DVD. Se li poden trobar moltes utilitats perquè xifra amb un nivell de seguretat molt elevat tot tipus de fitxers i a més, protegeix la integritat dels fitxers amb mètodes realment fiables.

De cara al futur, es podrien fer nous projectes relacionats amb AACS, seria un gran avanç poder tenir accés a la tecnologia de replicació dels dics que és realment on es fa la part més important del xifrat.

Tot i així, tal i com sembla que està evolucionant la guerra de formats entre HD-DVD i Blu-Ray, potser seria millor fer l'estudi de l'AACS sobre Blu-Ray ja que a més de ser obligatori en aquest suport, tot apunta que el suport de Sony serà el guanyador d'aquesta guerra.

9. Bibliografia

Lucena Lopez, Manuel J. (2007). Criptografía y Seguridad en Computadores.

http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto

National Institute of Standards and Technology.(2005). Recomendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf

Casals, Lluís. Balsells, Gómez, Carles. Jordi. Muñoz, Carolina, Criptografia (versió 2007). [Capítol 3: Algorismes de xifrat. Capítol 4: Autentificació i signatura digital].

UPC (Departament de Telemàtica)

AACS LA, Introduction and Common Cryptographic Elements

http://www.aacsla.com/specifications/specs091/AACS_Spec_Common_0.91.pdf

AACS LA, Pre-recorded Video Book

http://www.aacsla.com/specifications/AACS_Spec_Prerecorded_0.92.pdf

AACS LA, Recordable Video Book

http://www.aacsla.com/specifications/specs091/AACS_Spec_Recordable_0.91.pdf

AACS LA, HD DVD and DVD Pre-recorded Book

http://www.aacsla.com/specifications/AACS_Spec_HD_DVD_and_DVD_Prerecorded_0_912.pdf

AACS LA, HD DVD Recordable Book

http://www.aacsla.com/specifications/AACS_Spec_HD_DVD_Recordable_0.921_20060725.pdf

Armbrust, Christen M, Johnson, Crawford Charles G, Mark R. High-Definition DVD Handbook

McGraw-Hill Companies

Sonic

http://www.sonic.com/

ZONADVD, Alta Definición: Blu-ray y HD-DVD.

http://www.zonadvd.com/modules.php?name=Sections&op=viewarticle&artid=608