

1. INTRODUCERE ÎN SECURITATEA CONȚINUTULUI MULTIMEDIA

1.1. Tipuri de securitate

În ultimele decenii, apariția camerelor digitale foto și video, cât și a CD-urilor, a DVD-urilor sau a discurilor Blu-ray, a ușurat crearea, stocarea și vizualizarea informației multimedia digitale. În plus, apariția calculatoarelor mai rapide, combinată cu creșterea capacității de stocare și cu mărirea vitezei de transfer, facilitează utilizarea globală a tehnologiei digitale. Toate acestea au dus la o adevărată explozie în ceea ce privește folosirea datelor digitale și, cel puțin în domeniul media, putem considera că trăim într-o lume digitală.

Odată cu explozia digitală, a apărut și nevoia stringentă de securitate a informației digitale. Pe zi ce trece numărul companiilor care au nevoie de canale securizate crește; numărul persoanelor care doresc confidențialitatea informațiilor crește; numărul de persoane care își doresc protecția drepturilor de autor asupra proprietății lor intelectuale crește; și lista continuă. Din aceste dorințe de securitate și confidențialitate, existente de altfel de mult timp dar sub alte forme, s-au născut ideile, teoriile, programele și cercetările legate de securitatea informației.

Obiectivele securității informației sunt:

- Confidențialitatea: accesul la informații doar a celor care sunt autorizați;
- Integritatea: modificări ale informației numai de către entități autorizate și folosind căi autorizate;
- Disponibilitate: informația să fie disponibilă doar pentru cei autorizați.

Informația digitală poate fi protejată în diferite moduri și în diferite locații. Astfel, putem identifica trei mari domenii de securitate a informației digitale (vezi Figura 1.1):

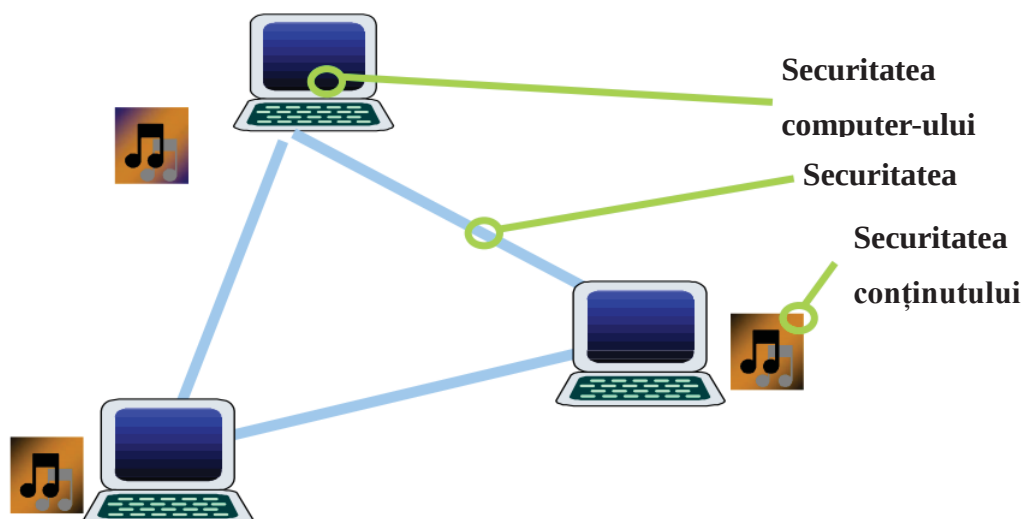


Figura 1.1. Tipuri de securitate a informației

- Securitatea computer-ului, ce asigură protecția datelor de pe calculator, de exemplu prin intermediul aplicațiilor de tip antivirus sau firewall;
- Securitatea rețelei, ce asigură protecția datelor în timpul transmisiunii acestora. Securitatea rețelelor de calculatoare este în acest moment parte integrantă a domeniului rețelelor de calculatoare și ea implică protocoale, tehnologii, sisteme, instrumente și tehnici pentru a securiza informația digitală transmisă și a opri atacurile rău intenționate.
- Securitatea conținutului, ce asigură protecția reprezentării digitale a datelor, ca de exemplu tehnici de protecție a proprietății intelectuale asupra materialelor multimedia, tehnici de autentificare a conținutului multimedia, tehnici de protecție la copiere, etc. Această carte este dedicată acestui domeniu de securitate a conținutului multimedia.

1.2. Securitatea conținutului multimedia

Conținutul digital are mari avantaje în ceea ce privește stocarea și procesarea. Mai mult, el poate fi reprodus fără a se pierde din calitate, permițând modificarea într-un mod ușor și imperceptibil. Acest lucru permite distribuirea de informație audio și vizuală de înaltă calitate și producerea de animații vizuale incredibil de reale în industria filmului.

Totuși, această digitalizare, creșterea numărului de metode de replicare și creșterea explozivă a Internetului au adus după ele și probleme: proprietatea intelectuală este mai greu de protejat și același lucru se întâmplă și cu conținutul original. De aceea au fost dezvoltate metode care să protejeze proprietatea intelectuală, să securizeze conținutul materialelor digitale, să asigure protecția la copiere și autenticitatea lor în cazul unor dispute.

Domeniul securității conținutului multimedia include toate mijloacele de protecție a datelor multimedia, de la crearea lor, prin asigurarea protecției drepturilor de autor, asigurarea confidențialității (datele ajung doar la destinatar), prin mijloace de criptare, autentificarea lor la destinatar (credibilitatea conținutului multimedia) și protecția lor împotriva furtului și a distribuției ilegale.

1.3. Sisteme DRM

Un sistem DRM (Digital Rights Management) este un sistem de management a drepturilor de utilizare și distribuire a informațiilor multimedia. El implică descrierea, identificarea, comerțul, protecția, monitorizarea și urmărirea tuturor formelor de utilizare a drepturilor asupra materialelor digitale, atât sub formă fizică, cât și digitală, incluzând și managementul relațiilor dintre proprietarii drepturilor intelectuale.

Un sistem DRM permite schimbul sigur de proprietate intelectuală sub formă digitală (muzică, imagini, video, text) în mediile electronice (Internet, CD, DVD, BlueRayDisk, rețele mobile). Aceste sisteme conțin lanțul de servicii și tehnologii hardware și software, ce guvernează utilizarea autorizată a conținutului digital, administrează toate consecințele acestei utilizări pe durata întregului ciclu de viață a conținutului respectiv. În Figura 1.2 sunt prezentate entitățile implicate în funcționarea unui DRM.

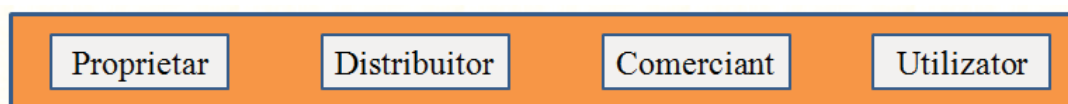


Figura 1.2. Entități implicate în funcționarea unui sistem DRM

Managementul digital al drepturilor de utilizare și distribuire a conținutului leagă anumite drepturi de utilizator de conținut pentru a controla accesul, duplicarea și partajarea datelor. În mod ideal, realizează un balans între accesul la informație, protecția informației și cost pentru a crea un mediu benefic pentru toate părțile implicate.

Managementul drepturilor asupra materialelor digitale include aspecte din sfere foarte diferite ale societății:

- Tehnologie, prin punerea la dispoziție a mecanisme și sisteme ingineresti
- Sfera afacerilor, prin oferirea de produse/servicii comerciale viabile
- Sfera socială, prin cerințe de confidențialitate și limite privind comportamentul utilizatorilor
- Sfera juridică, prin aplicarea legislație privind drepturile de autor și de distribuție a conținutului digital

Pentru a asigura funcții specifice, sistemele DRM utilizează diferite tehnologii. Cele mai importante funcții și tehnologiile asociate sunt date în Tabelul 1.1.

Tabelul 1.1. Tehnologii utilizate pentru sistemele DRM și funcțiile pe care le îndeplinesc

Tehnologie	Criptografie	Watermarking	Limbaje DRM
	Protocoale criptografice; Cifruri simetrice; Cifruri asimetrice; Semnături digitale; Funcții Hash;	Watermark vizibil; Watermark robust; Watermark fragil;	XrML; ODRL; MPEG REL;
Funcții îndeplinite	Autentificare utilizator în sistem; Condiționare acces; Verificare a integrității datelor;	Control al copierii; Identificare autor; Amprentare a conținutului; Autentificare a conținutului	Specificare a drepturilor de utilizare Interoperabilitate

1.3.1. Arhitectura unui sistem DRM

În Figura 1.3 este dată arhitectura de referință a unui sistem DRM. Acesta conține trei entități mari: serverul de conținut multimedia, serverul de licențe și clientul (utilizatorul). Funcționarea unui astfel de sistem este detaliată în cele ce urmează:

1. Clientul X trimite o cerere de conținut multimedia către serverul de conținut;
2. Serverul de conținut caută informațiile solicitate în depozitul de conținut;
3. Serverul de conținut criptează conținutul respectiv cu o cheie de criptare și trimite primul pachet de date către clientul X;
4. Acest pachet activează controller-ul DRM al clientului;
5. Controller-ul DRM al clientului trimite informația de licențiere către generatorul de licențe al serverului de licențe;
6. Generatorul de licențe autentifică identitatea clientului X, căutând în baza de date a utilizatorilor (identități);
7. Dacă identitatea clientului a fost confirmată, generatorul de licențe caută în baza de date drepturile pentru utilizatorul X;
8. Generatorul de licențe primește cheia de decriptare de la blocul de criptare și generează licența pentru utilizatorul X;

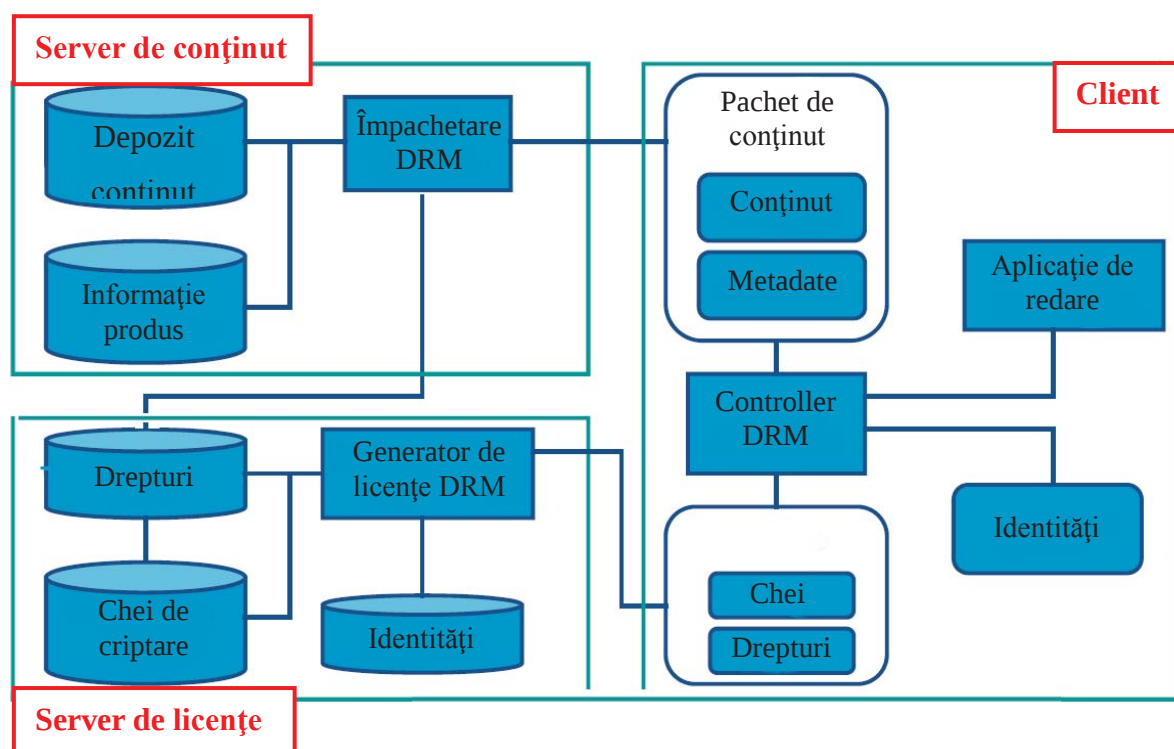


Figura 1.3. Arhitectura unui sistem DRM

9. Generatorul de licențe DRM al serverului de licențe trimite licența către controller-ul DRM al utilizatorul X;
10. Controller-ul DRM al clientului decriptează conținutul multimedia folosind cheia de decriptare livrată de serverul de licențe și transmite fluxul multimedia decriptat către aplicația de redare.

1.3.2. Limbaje DRM

Limbajele de exprimare a drepturilor de utilizare și distribuție a conținutului multimedia (REL-Rights Expression Language) sunt limbaje mașină folosite la sistemele DRM. Funcțiile unui REL sunt definirea de licențe și descrierea permisiunilor și restricțiilor pentru utilizarea conținutului multimedia aferent.

Majoritatea acestor limbaje pot fi exprimate în formatul XML (Extensible Markup Language) de definire și modificare a metadatelor, dar aceasta nu este o cerință, orice format putând fi utilizat. Chiar dacă aceste limbaje pot fi procesate direct, ele sunt de regulă încorporate ca metadata în alte documente, ca de exemplu cărți electronice, fișiere audio MP3 sau secvențe video descărcate de pe diverse servere.

Cele mai importante limbaje DRM sunt:

- XrML (eXtensible Rights Markup Language) este un limbaj proprietar ContentGuard, ce are la bază limbajul XML. Acest limbaj descrie drepturile și condițiile de utilizare, inclusiv plată, a conținutului multimedia. Standardul adaugă identificatori unici, chei publice sau private și alte informații în documentele multimedia pentru identificarea și verificarea autenticității proprietarului și utilizatorului resursei și include certificare pentru hardware și software care fac parte dintr-un mediu sigur.
- ODRL (Open Digital Rights Language) este un limbaj open source internațional, ce oferă mecanisme flexibile pentru utilizarea transparentă, distribuția și consumul de conținut digital în toate sectoarele. Standardul a fost dezvoltat de către ODRL Community Group, un grup membru al comunității World Wide Web (W3C), și și-a propus să exprime drepturi, reguli și condiții pentru interacționarea cu conținut multimedia online, incluzând formulări pentru permisiuni, interdicții, obligații, și revendicări.

- MPEG REL (MPEG-21 Rights Expression Language) este un standard internațional ISO/IEC 21000-5 din 2004 cu o arhitectură și tehnologie bazată pe XrML 2.0.

Specificațiile MPEG-21 au ca la bază un set de interfețe standard pentru sisteme de management și protecție a proprietății intelectuale (IPMP - Intellectual Property Management and Protection), descrise pentru prima dată de standardul MPEG-4.

În iunie 2002 MPEG (ISO/IEC JTC1 SC29 WG11) a început să lucreze la definirea de norme tehnologice pentru aplicațiile multimedia ale secolului 21. Această inițiativă a fost numită MPEG-21 „Multimedia Framework”.

MPEG-21 “Multimedia Framework” își propune să permită utilizarea resurselor multimedia între o gamă largă de rețele și dispozitive și să suporte tranzacții transparente și total automatizate având în special în vedere cerințele DRM și accesul și livrarea de conținut multimedia utilizând rețele și terminale eterogene.

În Figura 1.4 este dată structura unei licențe simple MPEG-REL. Licența este caracterizată prin *emitent (issuer)* și *grant*. Un *grant* conține:

- *principle* - persoana căreia îi este emisă licența;
- *right* - drepturile pe care le specifică licența;
- *resource* - resursele asupra cărora se aplică licența;
- *condition* - condiția care trebuie îndeplinită pentru ca drepturile să poată fi exercitate.

În continuare este dat un exemplu pentru o licență simplă și sunt identificate toate componentele acestei licențe:

„Un student poate să vizioneze filmul XYZ de la adresa www.videoserver.com timp de șase luni, dacă se loghează de pe un computer cu o adresă IP 186.125.14.X.”

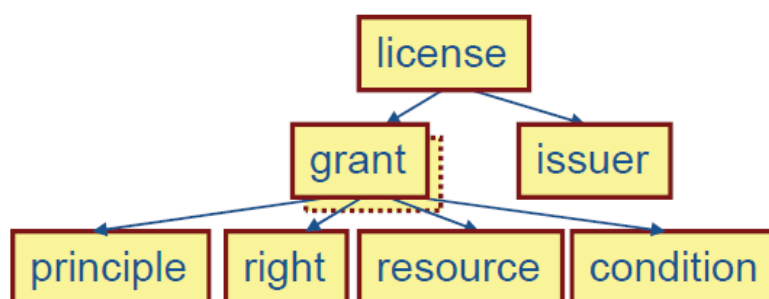


Figura 1.4. Structura unei licențe simple MPEG-REL

Componentele licenței sunt:

grant = „să vizioneze filmul XYZ de la adresa www.videoserver.com timp de șase luni,
dacă se loghează de pe un computer cu o adresă IP 186.125.14.X”

issuer = „www.videoserver.com”

principle = „student”

right = „să vizioneze”

resource = „filmul XYZ”

condiția1 (interval de validitate - *validityInterval*) = „șase luni”

condiția2 = „dacă se loghează de pe un computer cu o adresă IP 186.125.14.X”