

# DOMENICO RUSSO

## CARATTERIZZAZIONE E PROTOTIPIZZAZIONE DI UN SISTEMA DRM PER SUONERIE TELEFONICHE

### RIASSUNTO GENERALE

ATTRAVERSO UNA BREVE ANALISI DI MERCATO, SONO STATI PROPOSTI DEI MODELLI DI CONTRATTO STANDARD PER LA VENDITA E LA DISTRIBUZIONE DELLE SUONERIE TELEFONICHE DA PARTE DEI CONTENT PROVIDER.

SONO STATI SUCCESSIVAMENTE ANALIZZATI GLI ASPETTI IMPORTANTI DELLE TECNOLOGIE DRM PER LA MUSICA, CON PARTICOLARE RIFERIMENTO AI SISTEMI DI IDENTIFICAZIONE (DOI), I RIGHTS EXPRESSION LANGUAGE (REL E ODRL) E I SISTEMI PER LA PROTEZIONE DEGLI OGGETTI DIGITALI (FINGERPRINTING, WATERMARKING, CRITTOGRAFIA E FIRMA DIGITALE).

E' STATO POI PROPOSTO UN SISTEMA DRM BASATO SULLE CARATTERISTICHE FONDAMENTALI DI UN AMBIENTE MOBILE E SULLE SPECIFICHE STANDARD DELLA OPEN MOBILE ALLIANCE. NEL CORSO DELLA RIFLESSIONE SULLE PECULIARITA' DI UN DOMINIO MOBILE, SONO EMERSI ANCHE ALCUNI ASPETTI ESTREMAMENTE VANTAGGIOSI NELL'IMPLEMENTAZIONE DI UN SISTEMA DRM MOBILE NEI CONFRONTI DELLE RETE APERTA DI INTERNET. QUESTE OSSERVAZIONI SONO STATE PRESE IN SEGUITO COME SPUNTO, NELL'ULTIMO CAPITOLO, COME FUTURE PROPOSTE DI RICERCA.

DOPO L'ANALISI DI UN PROFILO REL SPECIFICO, L'OBBIETTIVO DELLA TESI E' STATO COMPLETATO ATTRAVERSO LA FORMALIZZAZIONE DI LICENZE ODRL PER LA GESTIONE DELLE SUONERIE TELEFONICHE.

PER CONCLUDERE, E' STATO ANCHE DIMOSTRATO COME, ATTRAVERSO LA DEFINIZIONE DI UN VOCABOLARIO IDEALE E L'ESTENSIONE DI UNA LICENZA ODRL, E' POSSIBILE ASSEGNARE NUOVE FUNZIONALITA' ALLE LICENZE DELLE LE SUONERIE TELEFONICHE.

SEGUE, NELLE PAGINE SUCCESSIVE, UNA BREVE RICAPITOLAZIONE DI TUTTI I CONCETTI PRINCIPALI AFFRONTATI NELLA TESI.

- Alla base della distribuzione dei contenuti digitali ci sono delle licenze. Le licenze sono dei file contenenti i metadati, ossia delle istruzioni eseguibili che esprimono i diritti di utilizzo concessi dal proprietario dei contenuti, in base a dei termini e delle condizioni.
- Le licenze coinvolgono il proprietario dei contenuti, un eventuale intermediario e l'utente consumatore e sono gestite da un sistema DRM per il controllo e la protezione dei contenuti digitali.
- I diritti e le condizioni relative all'uso e alla distribuzione di un contenuto digitale sono specificati nelle licenze con un linguaggio REL. Un Rights Expression Language è una struttura di tag XML che permette di esprimere ed applicare i relativi diritti in maniera flessibile. Questa struttura è definita da una sintassi ed una semantica di base che può essere estesa per creare dei profili REL più specifici.
- Nelle licenze del dominio mobile, il linguaggio standard adottato dalla Open Mobile Alliance è ODRL. La motivazione di questa scelta è quella di impiegare un "open standard" capace di estendere le proprie funzionalità in base alle particolari caratteristiche di un sistema, come appunto quello mobile.
- Un dominio mobile è unico per molti aspetti: i dispositivi hanno minore capacità computazionale rispetto ai Personal Computer, inoltre hanno bisogno di supportare diritti, condizioni di utilizzo e distribuzione molto semplici, date le loro limitate interazioni con l'utente e l'ambiente controllato di un service provider. Una licenza ODRL dovrebbe quindi essere un file piuttosto leggero da gestire con la massima semplicità in un sistema DRM mobile.
- Un sistema DRM mobile può essere implementato come un'estensione di livello inferiore del sistema operativo di un dispositivo cellulare. Attraverso un DRM Manager (o agente DRM), che coinvolge e gestisce diverse applicazioni per la sicurezza, il sistema si occuperebbe di autenticare le licenze e i contenuti, analizzare ed applicare i diritti e fornire così i contenuti decifrati ad un'applicazione di tipo "trusted". Quindi, attraverso un meccanismo a chiave pubblica ed una funzione Hush, è possibile firmare digitalmente una licenza per impedire che questa venga successivamente riutilizzata per un altro oggetto digitale.
- Il file di licenza di un sistema DRM implementato in un terminale mobile 3G dovrebbe pertanto comprendere anche l'algoritmo di codifica del contenuto e la relativa chiave di decifrazione. Una volta che sia il contenuto che la relativa licenza

sono stati controllati, un'applicazione del dispositivo può quindi richiedere al DRM Manager di eseguire un'azione sul contenuto.

- Le azioni sul contenuto sono associate a determinati diritti. In un telefono cellulare possono essere ridotte a due semplici categorie: i diritti di riproduzione e i diritti di trasferimento. Il trasferimento di un contenuto come una suoneria può essere bloccato mediante il meccanismo del Forward Lock.
- La OMA distingue tre meccanismi fondamentali: il Forward Lock (blocco d'inoltro; l'utente non può ridistribuire il contenuto), il Combine Delivery (consegna del contenuto assieme alla licenza) ed il Separate Delivery (consegna separata della licenza). Il primo meccanismo si ottiene in assenza di una licenza, semplicemente impacchettando il contenuto in un messaggio MIME contenente l'istruzione di blocco. Il secondo meccanismo inserisce una licenza ODRL all'interno del messaggio MIME in cui è incapsulato il contenuto in una versione non cifrata. Il terzo meccanismo invia separatamente il contenuto cifrato ed il relativo file di licenza contenente la corrispondente chiave di cifratura. Il vantaggio di quest'ultimo metodo è quello di mantenere la protezione del contenuto, mediante la licenza, nella redistribuzione dello stesso.