DRM

Digital Right Management

Bronzetti Stefano
mat: 264848

A.A. 2007/2008

DRM(Gestione dei diritti digitali)

definizione: tutti quei sistemi tecnologici di controllo usati per limitare l'accesso e l'utilizzo a dati o hardware.
Chi detiene i diritti d'autore, può far valere i propri diritti in ambiente digitale grazie alla possibilità di rendere protetti, identificabili e tracciabili tutti gli usi in rete di materiali adeguatamente marchiati.
esempio: evitare duplicati senza autorizzazione (copy protection)

spinti da:

- Chi detiene i diritti d'autore: case discografiche/cinematografiche aziende software/videogiochi/ebook

osteggiati da:

- Gli utenti: Limitazione dei diritti degli utenti (chi compra regolarmente il materiale non può farne l'uso che vuole)

→ ***DRM = DIGITAL RESTRICTION MANAGEMENT***

FUNZIONAMENTO DEI SISTEMI DRM

idea semplice: i file audio/video vengono codificati e criptati in modo da garantire la protezione contro la copia e l'inoltro verso terzi non autorizzati, consentendo così un uso limitato(ad esempio nel tempo) e predefinito nella licenza d'accesso fornita agli utenti finali.

informazioni aggiuntive: la codifica permette di includere informazioni aggiuntive: copyright, licenza, biografia autore ecc..

accesso ai dati: procedure di autenticazione che permettono di distribuire i file richiesti nelle modalità previste dalla licenza sottoscritta dall'utente.

EFFETTI:

- Utenti infastiditi e limitati anche se in buonafede.
- Non riescono realmente ad arginare le copie illegali, in quanto sono sempre stati scavalcati in qualche modo.

PERCHE' I DRM?

- ***nuove tecnologie:*** banda larga, p2p, lettori mp3/mp4, telefonini di ultima generazione, lettori divx, negozi di contenuti multimediali online.
- ***tecnologia digitale:*** facile e veloce copiare senza perdita di qualità (diversamente dalla copia analogica).
- ***l'utente ha accesso a un mondo di contenuti digitali:***
  → major impensierite dalla pirateria:

cade il sistema autore – distributore - cliente

→ DRM per poter gestire il controllo su aspetti legati alla distribuzione e all'utilizzo dei prodotti.

DRM PIU' FAMOSI

- ***richiesta di keyword da manuale*** (obsoleto)
- ***registration key / Name and serial***
- ***attivazione software***
- ***CSS (Content Scambling System)***
- ***watermarking***
- ***rootkit Sony BRG***
- ***starforce***
- ***apple FairPlay***
- ***microsoft PlaysForSure***

RICHIESTA DI KEYWORD DA MANUALE

primo tentativo di far rispettare i diritti digitali
idea: se un utente ha il prodotto originale → possiede anche parte di esso, come manuale.
fuzionamento: All'avvio del software (soprattutto giochi) si chiede di inserire la parola numero x alla riga y della pagina z del manuale.
vulnerabilità: copie digitali del manuale cartaceo.

REGISTRATION KEY / NAME & SERIAL

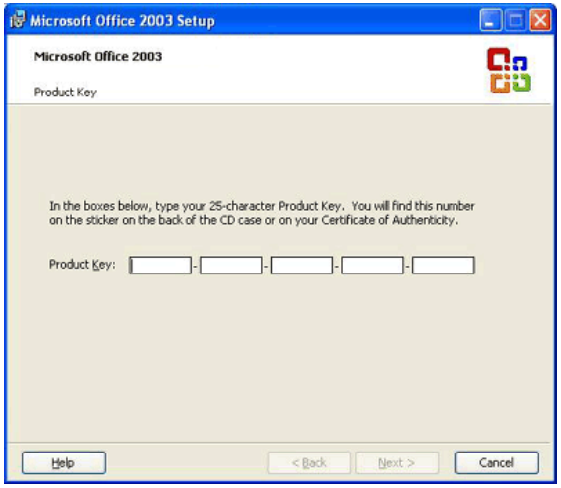
idea: attivazione tramite codice seriale.
funzionamento: per sbloccare i software, soprattutto quelli forniti in prova con licenze Shareware si chiede di inserire un seriale o di registrarsi attraverso una chiave che può essere fornita o su internet, o in dotazione col prodotto, o telefonicamente.
vulnerabilità: keygen (cioè programmi che permettono di generare un seriale valido per sbloccare il software)per la validazione del codice.

Dall'esame di molti seriali di un dato prodotto si riusciva a interpolare e ricostruire l'algoritmo di generazione dei codici, tenuto segreto dal produttore. A volte il "segreto" è proprio tramandato da un personaggio interno, l'anello debole della catena.

ATTIVAZIONE DEL SOFTWARE

Microsoft è stata la prima azienda a implementare questo meccanismo, dapprima con Microsoft Reader, che proteggeva gli eBook dalla copia non autorizzata, quindi con Windows XP e Office XP.

1. L'utente che acquista il prodotto originale riceve un codice alfanumerico a 25 caratteri, la cui validità viene inizialmente verificata dal SW stesso.
2. Entro 15 giorni l'utente deve eseguire una verifica on-line o telefonica comunicando un codice numerico generato in base alla Product Key e alla configurazione HW del PC su cui si è installato il prodotto.
3. Se la verifica ha successo il server risponde con un codice di conferma riconosciuto dal sistema, che sblocca tutte le sue funzionalità.



vulnerabilità: facilmente violabile per i prodotti più comuni. Ciò viene fatto usando la tecnica del Reverse Engeneering.

CSS (CONTENT SCAMBLIG SYSTEM)

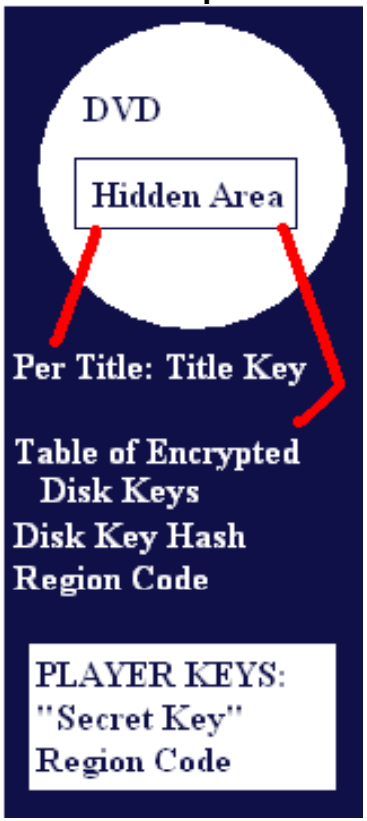
ideato per i film su DVD

idea: crittografare i supporti con una chiave segreta rilasciata ai produttori di hardware e software di lettura a patto di accettare specifiche condizioni di licenza e pagando una quota, tra cui il divieto ad esempio a fornire uscite audio digitali ad alta qualità.

→ Quindi DVD-Video non masterizzabili e non riproducibili su player senza decoder CSS

vulnerabilità: CSS è stato raggirato (DVD-Jon) → programmi come DeCSS e ANY-DVD permettono la copia (illegale).

funzionamento: CSS cripta i contenuti del DVD lavorando su 2 livelli:
1)impedisce accesso a unità DVD e la copia dei file VOB su hard-disk;
2)cripta i file VOB, che risultano illeggibili qualora si riesca a copiarli.



L'algoritmo lavora con chiavi crittografiche a 40-bits.
Le chiavi di accesso del titolo specifico sono memorizzate in un'area riservata del disco, detta *hidden area*.
Le chiavi di accesso funzionano in *cascade*, cioè una chiave di livello gerarchico superiore (la chiave del lettore) è usata per decriptare la chiave del disco; quest'ultima è utilizzata per decriptare la chiave del titolo.
I dati audio-video sono cifrati con le chiavi suddette, quindi la mera copia produrrà video illeggibili.

Computazionalmente la limitatezza del sistema CSS non sta nell'algoritmo ma nell'uso di chiavi a soli 40-bits.
Un semplice attacco "divide et impera" con una complessità di 2^16 permette di ottenere la chiave di cifratura e decriptare i file protetti

WATERMARKING

idea: inserire in un flusso digitale o analogico delle informazioni di identificazione del prodotto (ID) e dell'utente.
Tale sistema può essere: ben visibile, come il logo dell'emittente televisiva, oppure nascosto.
esempio: acquisto un DVD protetto da Watermark. Devo fornire un documento al venditore, che comunica i miei estremi alla casa produttrice che saprà così che "quel" disco (ha un ID) è acquistato da "quella" persona. Se in seguito metto in rete il film, la casa produttrice potrebbe identificarmi e perseguirmi penalmente.
problemi:

- troppa responsabilità verso il supporto: in caso di furto o smarrimento l'utente non è tutelato.
- collisione con le norme sulla privacy.

ROOTKIT SONY BMG (2005)

idea: Sony include, all'interno dei CD musicali un malicious software nascosto (rootkit) con l'obiettivo “supposto” di proteggere i propri interessi e prevenire l'uso e la copia illegale di musica.

funzionamento: quando si prova a fare una copia, violando i diritti, il sistema XCP (Extended Copy Protection) fa in modo che le tracce copiate producano rumore bianco “white noise”.

problemi:

- installato in maniera ingannevole, l’utente consente all’installazione pensando di installare un player → *scorrettezza*
- si rende invisibile, non è eludibile né disattivabile. Qualsiasi tentativo manuale porta irrimediabilmente a compromettere le funzionalità del sistema: anche le patch di rimozione Sony non hanno funzionato → *illecito*
- espone il PC ad alti rischi di sicurezza, rendendolo terreno fertile per gli hacker → *pericolo*

→ *Causa:* per chiudere il caso Sony paga 750mila dollari.

STARFORCE

idea: sistema DRM adottato da numerosi produttori che si insinua nel PC quando vengono installati i software. Opera "*a basso livello*" rispetto al SO infatti installa dei driver virtuali nascosti, attraverso cui controlla l'autenticità del disco inserito nel lettore ottico abilitando o disabilitando le periferiche.

funzionamento: misura l'angolo fisico tra il primo e l'ultimo settore scritto dal CD. La distanza creatasi, è una sorta di firma hardware che è identica in tutte le copie utilizzate dalla casa produttrice e diviene abbastanza difficile riprodurla quando un CD viene duplicato. Quando si tenta di masterizzare un prodotto protetto da Copyright si attiva il reboot del sistema,a prescindere da qualsiasi applicazione si abbia aperta al momento.

problemi:

- malfunzionamento dei dispositivi, anche danni fisici alle periferiche;
- impossibile da disinstallare;
- compromessa la stabilità del sistema operativo;

APPLE FAIRPLAY

iTunes Store: vendita online di audio/video digitale. Vende prodotti delle 5 maggiori etichette mondiali (3 milioni di canzoni).

iTunes: (ex SoundJam MP) programma freeware per interfacciarsi con iTunes Store. Serve a riprodurre, organizzare, sincronizzare e acquistare prodotti digitali. Grandi funzionalità. Non supporta WMA, ma ha una funzionalità che permette di convertire tali file,se non protetti nel formato ACC.

successo: Completamente integrato con iPod. ITunes detiene il 70% della musica “legale” scaricata al mondo.
Poca competizione: rispetto a Rhapsody offre una gestione dei diritti digitali (DRM) più liberale ed elastica.
Gli altri negozi online utilizzano principalmente la tecnologia proprietaria della Microsoft Windows Media Video, o formato WMV.

Apple FairPlay: è una tecnologia DRM integrata in iTunes, che gestisce le canzoni comprate su iTunes Music Store. Rispetto ad altri sistemi di DRM è meno restrittivo e invasivo.

formati: Canzoni codificate nel formato Dolby Advanced Audio Coding (ACC) a 128 kbits/s. Questa codifica ha una qualità equivalente a quella di un file MP3 codificato a 192 kbits/s. AAC è parte dello standard MPEG-4 contenuto nel pacchetto QuickTime 6. Sebbene tecnicamente ogni player digitale sia in grado di leggere i file AAC, solo Apple iTunes e iPod possono leggere i file AAC criptati con la tecnologia Apple FairPlay, cioè quelle scaricate da iTunes. Apple è costretta dalle etichette (tranne EMI) a fornire DRM, e se violato Fairplay deve agire in un tempo limitato per risolvere il problema.

restrizioni:

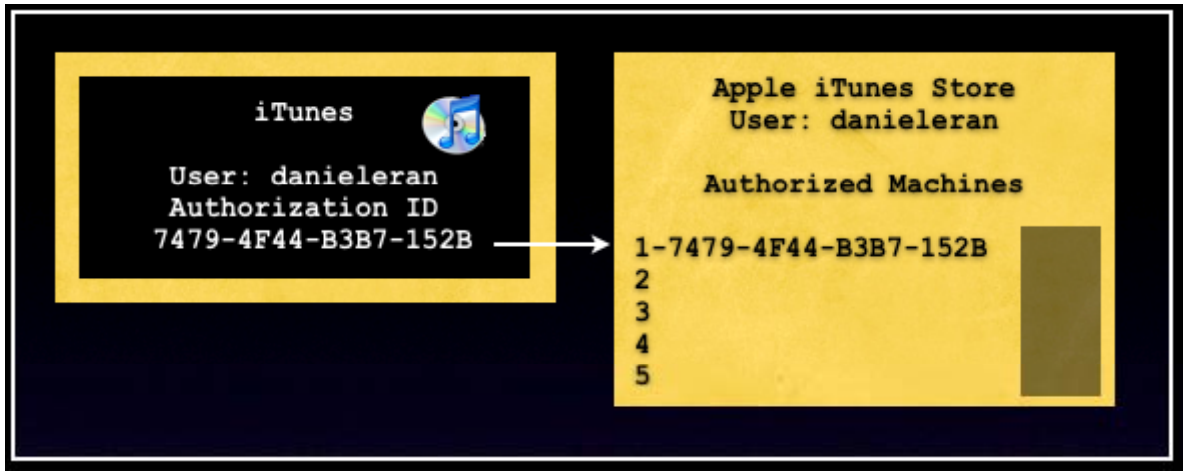
- Traccia ascoltabile soltanto su dispositivi compatibili con Quicktime;
- Traccia copiabile su quanti iPod vuoi
- Il file è copiabile e riproducibile su massimo 5 computer registrati simultaneamente.
- Il file può essere copiato su CD, in formato AudioCD un numero illimitato di volte.
- Una Playlist può essere copiata massimo 7 volte su CD.

vulnerabilità:

- Jon Johansen ha aggirato Fairplay con il Reverse Engeneering, DeDRM
- Si può rippare da cd.
- Esistono software come VirtualCD-RW che emula un'unità cd-rw e automaticamente rippa su un altro file senza restrizioni.

funzionamento:

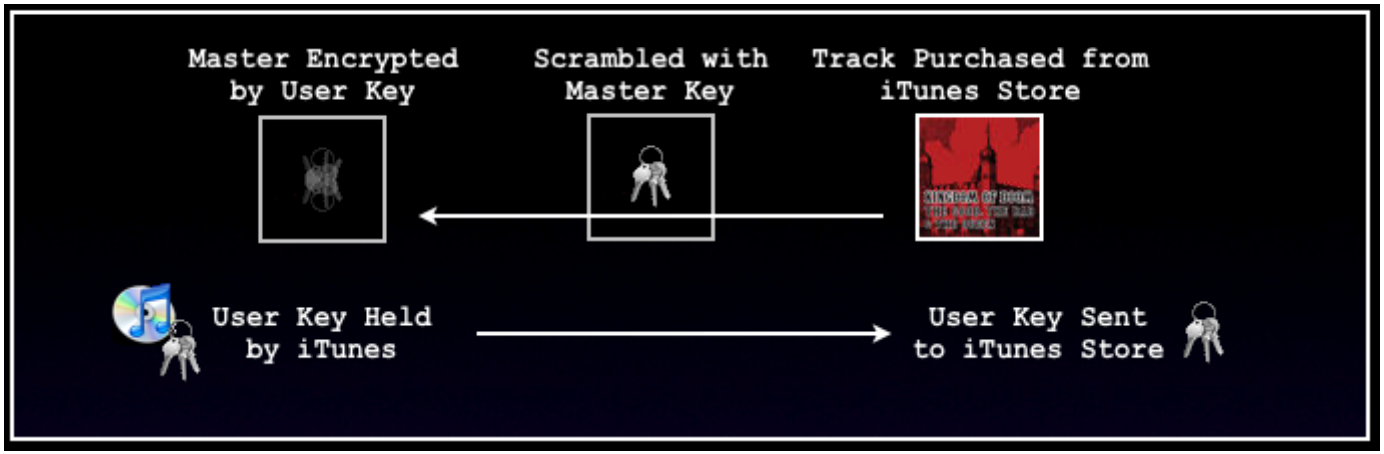
1. ***Creazione account e registrazione dispositivi:*** Prima di comprare su iTunes Store, un utente deve creare un account sul server Apple. In questa fase il software iTunes crea un ID globalmente unico per il computer sul quale si sta eseguendo iTunes in quel momento. Tale ID è spedito al server Apple, memorizzato nell'account utente e serve ad autenticare un PC o un Mac ad eseguire iTunes. Posso autorizzare fino a 5 macchine.



Esiste anche una procedura di deselezione di una macchina e riassegnamento del credito a un'altro dispositivo.

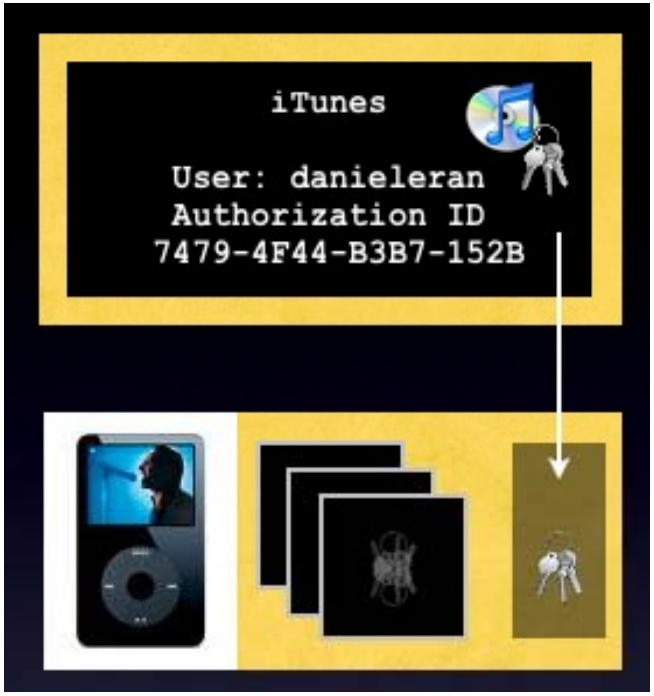
" e se perdo, mi si rompe, o mi rubano il pc??"

2. ***Acquistare canzoni da iTunes Store:*** viene creata da iTunes una “User Key” per quel determinato file. La canzone è criptata usando una “Master Key” separata che è anch’essa inserita nel file ACC da scaricare, ma è codificata usando la “User Key” che è spedita da iTunes al Server Apple.
La codifica del file con la “Master Key” viene fatta a livello locale da iTunes, semplificando e velocizzando la transizione.



Con questo sistema di autorizzazione iTunes non deve contattare il server ogni volta che deve riprodurre un file.
iTunes mantiene una collezione criptata di “user keys” per ogni file presente nella libreria locale di iTunes. Quando autentico un PC tra i dispositivi che "possono" riprodurre, l'intero set delle “User Key” scaricate da quell'account viene spedito al nuovo iTunes in esecuzione su quel nuovo dispositivo.

3. ***Riproduzione:*** Per riprodurre iTunes usa l'User Key per decriptare la "Master Key" contenuta nel file ACC. La "Master Key" è poi usata per decriptare i dati audio.
   La musica può essere riprodotta su tutti gli iPod senza restrizioni. Quando collego l'iPod al PC questo scarica tutte le "User Key" da iTunes, che gli serviranno per sbloccare e riprodurre le tracce protette.
   Non c'è modo che canzoni protette possano essere copiate sull'iPod senza che la "User Key" sia correttamente scaricata.



MICROSOFT PLAYSFORSURE

Certificazione per sistemi DRM.
Scopo: sottrarre una fetta di mercato a Apple.
Certificazione aperta: Microsoft ha cercato di coinvolgere più partner possibili, creando una coalizione tra produttori di software (Microsoft), negozi online (Napster, Rhapsody) e produttori di HW(Creative, ecc.)
Windows Media Player fa le veci di iTunes.
Problemi:

- L'interazione fra i player, il software e gli store era inefficiente e complicata.
- Esistono già tools per la rimozione del DRM Microsoft come FairUse4WM.
- Progetto abbandonato da Microsoft che punta tutto su PlayReady, che è implementato sul nuovo lettore Zune di Microsoft e sui telefoni di nuova generazione.

WMDRM : (Windows Media DRM). Progettato per assicurare un corretto uso di materiale scaricato da internet sul pc o su altri dispositivi. Fa parte di questo progetto anche PlayReady.
Windows Vista implementa massicciamente i sistemi WMDRM. Ad esempio include un sistema di protezione che vieta all'utente di visionare ad alta qualità contenuti protetti da DRM, se non è autorizzato a riprodurre certi file.

PROBLEMI DEI SISTEMI DRM:

Analog Hole:

la natura dell'analogico fa sì che nessun sistema DRM sia realmente efficace.

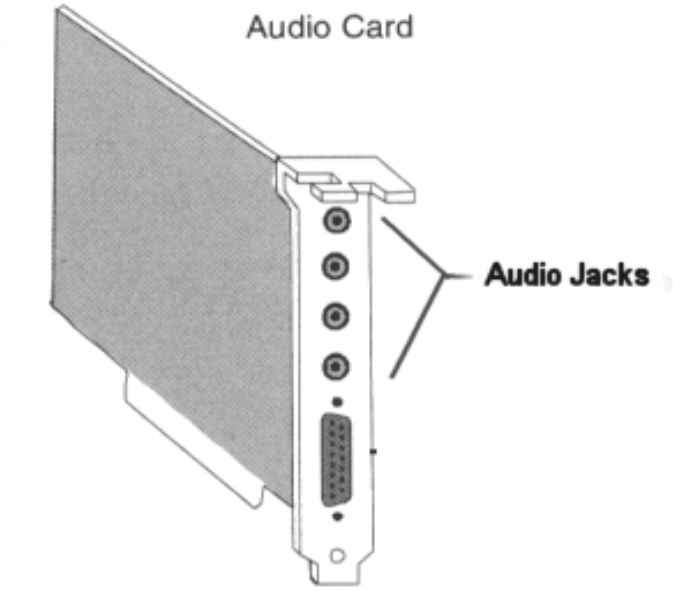
Un segnale digitale una volta convertito in analogico, è suscettibile di riconversione digitale in un formato non protetto (anche se con una perdita di qualità rispetto all'originale che può essere minimizzata con sistemi di registrazione professionale):

 falla nella protezione o nel controllo offerto dai DRM.

rimedi:

- Segnali analogici degradati per interferire o confondere alcuni dispositivi di registrazione come VCR e schede di cattura video.
- I costruttori di dispositivi digitali possono essere obbligati a riconoscere filigrane digitali sui segnali di ingresso e limitare la registrazione come condizione contrattuale. Tali tecniche possono essere aggirate tramite il *dithering*.

- I dispositivi dovrebbero essere in grado di disabilitare automaticamente l'uscita analogica se richiesto da una particolare programmazione (Selectable Output Control). Per prevenire la registrazione di particolari programmi, l'emittente può inviare un segnale per disabilitare tali uscite.
- le majors vorrebbero che venissero bandite per legge tutte le apparecchiature audio/video analogiche a favore delle uscite digitali con funzioni DRM e di crittazione dei segnali in uscita dai riproduttori, limitando gli acquirenti oltre che nella copia, anche nella riproduzione di file multimediali.



Attualmente i connettori audio/video (ad es jack) garantiscono l'interoperabilità tra apparecchiature audio e video.

È tecnicamente impossibile nascondere e mostrare allo stesso tempo un segnale:

Solitamente la sicurezza di un sistema coinvolge tre attori, due persone che parlano (trasmettitori o riceventi) e uno o più attaccanti.
Nel caso dei DRM, l'attaccante è lo stesso ricevente.
esempio: Mettiamo di comprare un DVD criptato con CSS. Per vederlo il mio riproduttore DVD deve avere un decodificatore CSS. Quindi, l'algoritmo con cui si cripta è ben noto, è CSS, il testo cifrato lo possiedo, ed è il DVD che ho comprato. Ora l'unico segreto è la chiave, che io non conosco. Ma la chiave è dentro il DVD, altrimenti come farebbe il riproduttore a riprodurre il film? Quindi ora posseggo: l'algoritmo, il metodo di crittatura e il dato criptato. Se fossi un genio, mi ci vorrebbe al massimo una settimana per aggirare il CSS.
conclusione: Alla fine, tutti i sistemi per il DRM condividono un errore comune: forniscono a chi li vuole infrangere il dato criptato, il metodo per criptare e la chiave. A questo punto, il segreto non è più tale.

problematiche:

- è difficile per un dispositivo sapere se quel particolare utilizzo è lecito o illecito e impedire ad un utilizzatore legittimo un uso illecito del materiale che ha legittimamente acquistato.
- Finchè esisteranno PC in libera vendita, con sistemi operativi non proprietari ed open source, e con la possibilità per gli utenti di scriversi da sé e scambiarsi i propri software, nessuna protezione software avrà modo di durare a lungo.

riuscire a inibire la produzione e la distribuzione di dispositivi e computer indipendenti, imponendo a tutti i mercati mondiali un unico prodotto standard proprietario, “blindato” che possa così effettuare l’enforcement delle limitazioni previste

Trusted Computing

TRUSTED COMPUTING

Trusted Computing Group (TCG): alleanza tra le più grandi aziende di informatica mondiali (Microsoft, Intel, IBM, HP, AMD, VIA, ecc..) per promuovere computer più “sicuri”, mediante l’uso di opportuni hardware e software.

→ Specifiche del Trusted Computing (TC, informatica fidata)

Obbiettivi:

- TC presentato e promosso come soluzione per ottenere computer più sicuri, affidabili, meno attaccabili da virus e programmi nocivi
- Spinto dalle majors, dai produttori di software e hardware per sbaragliare concorrenza, e dall’esercito americano.
- Obbiettivo nascosto: far rispettare i DRM
- Avere in ogni computer un “nocciolo” al di fuori del controllo dell'utente, che stabilisca cosa gli utenti possano o non possano fare con il proprio computer e stabilisca come e quando possono accedere ai propri file multimediali, quali file non possano visualizzare perchè provenienti da fonti non legittime.

sicurezza TC: Il TC è “trusted” (fidato) dal punto di vista non dell’utente, ma dal punto di vista dei canoni imposti dai produttori, tanto che tali sistemi potranno oltre che proteggere il software da manomissioni, imporre restrizioni su applicazioni ritenute dannose e non desiderabili o inaffidabile secondo i produttori.

“Non sarete voi a decidere se un certo programma potrà essere installato sulla vostra macchina”
(http://www.trustedcomputinggroup.org)

- il controllo del PC, passa dall’utente a chiunque abbia scritto il software che si utilizza.
- il TC aumenta la capacità di controllo dei sistemi da parte dei produttori di HW e SW.
- minaccia la libera competizione del mercato dell’ IT, l’open-source (es. morte di linux, apache).
- restrizione irragionevole di come i legittimi proprietari possano usare i propri computer.

→ Treacherous Computing (informatica traditrice)

oggi: Il progetto TC è già stato implementato, esistono già l'hardware e il software per poterlo fare e numerosi progetti.

- numero di serie unico nei pentium III (antenato);
- Microsoft NGSCB (Next Generation Secure Computing Base),ex-Palladium che verrà incluso nelle future versioni di Windows Vista;
- AMD Presidio;
- Intel LaGrande;
- Via Technologies PadLock.

realizzazione HW: "nocciolo" implementato a bassissimo livello sia HW (nel chipset) che SW (nel Sistema Op.). L'utente non può cambiare o aggiornare parti che implementano le restrizione del SO. E' invece obbligatorio che il SO sia aggiornabile a comando esterno, per tappare le falle che inevitabilmente verranno scoperte.
Il TC è realizzato tramite un chip detto "Chip Fritz" o unità TPM.

1) ogni singolo dispositivo è identificato univocamente da una sorta di passaporto elettronico;
2) la crittografia è eseguita a livello hardware in modalità sicura;
3) le informazioni possono essere firmate con la chiave della macchina e cifrate con la chiave della macchina;

Unità TPM: 5 funzionalità applicabili se il SW implementa TC:

- ENDORSEMENT KEY (chiave di approvazione): tecnica crittografica che impedisce a emulatori SW di avviare una transizione sicura con un programma, un dispositivo HW o un sistema remoto garantendo l'integrità del sistema.

Endorsement key: coppia di chiavi RSA a 2048 bit che identifica univocamente ogni TPM. generata al momento della produzione. Tale chiave non può essere estratta e il dispositivo HW riconoscerà di essere stato manomesso.

- SECURE I/O: meccanismi di cifratura a chiave asimmetrica rendono sicure le operazioni di I/O. Tutte le informazioni che transitano nel bus sono quindi cifrate, quindi transizioni sicure.
- MEMORY CURTAINING (Separazione della memoria): HW impedisce a ogni programma la r/w di zone di memoria utilizzate dagli altri applicativi in esecuzione. Anche dati in memoria saranno criptati.
- SEALED STORAGE (Memoria Sigillata): Protegge le informazioni per mezzo della cifratura, usando una chiave che deriva dal software utilizzato e dell'hardware su cui esso è in esecuzione.
- ATTESTAZIONE REMOTA: Protegge i dati dal software non autorizzato anche quando questi vengono utilizzati su altri computer. Un certificato digitale generato dall'HW che riporta quali software sono in esecuzione e mostrarsi non compromesso ad altri sistemi.

risultati:

- limitazioni dei diritti degli utenti, incubo per gli utenti.
- possibilità di censura, libertà di pensiero scavalcata.
- nuovo business per le majors.
- non si può vedere come è realizzato l'HW che implementa il TC per essere sicuri che sia implementato correttamente e non contenga backdoor e pericoli per la sicurezza.

disabilitare il TPM: Disabilitando il TC, il "Chip Fritz" non rilascerà le chiavi necessarie per decriptare i file ed accedere al conto corrente, le applicazioni TC non funzioneranno bene o per niente.

→ utente scavalcato, isolato, emarginato

vulnerabiltà:

- Prime versioni:chip installato sulla scheda madre → bastava craccare l'HW ripulendo i dati sul bus tra la cpu e il chip.
- Versione 2.0: chip incorporato nel processore, e ciò rende molto più difficile craccare il sistema, e a costi molto maggiori.
- Altra strada: prendere un PC "normale" ed emulare il Chip Fritz via software in modo che possa fare quello che vogliamo noi.

VALUTAZIONI FINALI SUI DRM

- Il DRM non è in grado di impedire l'uso illegale dei file. Ci sono moltissimi strumenti per rimuovere facilmente tali protezioni. E' sufficiente che anche una sola persona riesca a trovare il modo per violare la protezione di un file e lo renderà disponibile a tutti.
- Chi vende contenuti su CD sta già vendendo qualcosa di non protetto (ciò avviene nel 99% dei casi ad eccezione dei Cd col Sony rootkit).
- Il DRM ha un alto costo per i produttori che si riversa poi sugli utenti finali.
- Il DRM implementato soltanto via SW è craccabile: potrebbe funzionare solo se implementato hardware.
- Gli utenti che scaricano materiale legittimamente sono scontenti delle limitazioni che hanno sui prodotti e sono invogliati così a scaricare illegalmente
- Le majors chiedono ai tecnici di risolvere tecnologicamente delle questioni che andrebbero risolte in altro modo. Sono questioni economiche e legali. Da cambiare non è la tecnologia, ma le leggi sul diritto d'autore e la distribuzione.

LINK UTILI

DRM:
http://it.wikipedia.org/wiki/Digital_rights_management
http://en.wikipedia.org/wiki/Digital_Rights_Management
http://www.jus.unitn.it/users/caso/pubblicazioni/DRM/DRM.pdf
http://www.linux.it/GNU/opinioni/msftdrm.it.shtml

FairPlay:
http://en.wikipedia.org/wiki/Fairplay
http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html

Trusted Computing:
www.interlex.it/675/trustedcomp.htm
http://it.wikipedia.org/wiki/Trusted_computing

Anti-DRM: http://drm.info/
Anti-TC: http://www.no1984.org/