Digital Rights Management

Łukasz Jachowicz

wersja robocza z: 06/05/2006, godz. 20:26

Uwagi proszę zgłaszać na stronie

http://7thwiki.7thguard.net/index.php/DRM

1 Digital Rights Management

1.1 Definicja DRM

Digital Rights Management (DRM) to ogólna nazwa systemów ułatwiających twórcom, producentom lub nadawcom danych cyfrowych (zwykle multimedialnych) kontrolę nad treścią. W założeniu mają umożliwić ograniczenie użytkownika i uniemożliwienie mu działań nieprzewidzianych przez nadawcę treści. Najczęściej stosowany system DRM, Content Scrambling System (CSS) został zaprojektowany w taki sposób, żeby uniemożliwić stworzenie "nielicencjonowanych" odtwarzaczy DVD. Oznacza to między innymi, że w większości krajów bez łamania licencji nie da się napisać lub używać oprogramowania odtwarzającego płyty DVD rozprowadzanego wraz z kodem źródłowym.

Systemy DRM mogą służyć do nałożenia restrykcji na dowolną treść w formie cyfrowej: e-książkę, film, muzykę i oprogramowanie.

Przykładowe możliwości systemów DRM

- ograniczenie kopiowania,
- ograniczenie odtwarzania,
- utrudnienie konwersji do formatu mp3/ogg,
- ilościowe limitowanie odtworzeń/kopii,
- utrudnienie nagrania sygnału TV/video/audio,
- uniemożliwienie przewinięcia fragmentu filmu,
- utrudnienie odczytu programem innym niż dostarczony przez producenta,

W ostatnich latach próbowano wielokrotnie stworzyć "idealny", dający minimum praw użytkownikowi a ich pełnię producentowi system DRM, każda próba zakończyła się fiaskiem. Z jednej strony jest to spowodowane tym, że coraz częściej w systemach prawnych legalizujących tego typu rozwiązania pojawia się punkt mówiący o konieczności umożliwienia użytkownikowi wykonywania jego prawa do dozwolonego użytku, z drugiej strony ograniczeniem jest technika. Aby użytkownik mógł skorzystać z "zabezpieczonej" treści, musi ona zostać choć na chwilę rozszyfrowana w jego odwarzaczu. W chwili, kiedy jest ona rozszyfrowana, dostęp do niej może otrzymać dowolny program zainstalowany na tym samym urządzeniu.

Co więcej, systemy typu DRM nie uniemożliwiają kopiowania treści. Tu przykładem jest chociażby wspomniany wcześniej CSS. Autor programu dekodującego dane na płytach DVD był oskarżany o ułatwienie ich kopiowania, tymczasem same płyty DVD można kopiować, a po skopiowaniu odtwarzać bez znajomości działania algorytmu CSS. Z kolei systemy DRM mające w założeniu utrudnić kopiowanie, a zaimplementowane przez Sony... nie działają pod kontrolą systemu operacyjnego innego niż Windows (według niektórych źródeł pojawiła się też wersja działająca pod kontrolą MacOS). W praktyce oznacza to tyle, że danej płyty nie da się skopiować bez dodatkowego wysiłku na komputerze z Windows, da się - na każdym innym.

W niniejszym opracowaniu przybliżę od strony technicznej kilka najbardziej znanych systemów DRM, pokażę ich założenia, cechy i słabości, przez co nie spełniają roli przewidzianej przez ich autorów.

2 Istniejące systemy DRM

2.1 CSS – Content Scramble System

Dotyczy: płyty DVD.

Obejście: trywialne.

Przygotowany w połowie lat dziewięćdziesiątych system szyfrowania stosowany w sprzęcie DVD. W założeniu miał uniemożliwić odtworzenie zaszyfrowanej płyty DVD na nielicencjonowanym odtwarzaczu. Utrudniał też kopiowanie płyt z jednoczesną modyfikacją danych na nich nagranych, nie miał wpływu na kopiowanie ich oryginalnej zawartości.

W chwili, kiedy okazało się, że to ograniczenie utrudnia odtwarzanie niektórych płyt DVD pod kontrolą tzw. wolnych systemów operacyjnych, konieczne stało się ich obejście. Oficjalnie pierwszą osobą, której się to udało, był nastolatek – Jon Lech Johansen. Wraz z dwoma programistami, których tożsamość jest nieznana, napisał procedury dekodujące nagrania na zaszyfrowanych płytach DVD. Utajniony wcześniej CSS okazał się być słabym, 40-bitowym algorytmem szyfrującym.

Kod źródłowy programu dekodującego CSS można pobrać ze strony http://decss.zoy.org/

2.2 Płyty DVD – regionalizacja

Dotyczy: płyty DVD.

Obejście: trywialne.

Płyty DVD zostały zaprojektowane w taki sposób, żeby ich wydawca mógł zadecydować, w której części świata można sprzedawać dany krążek. Służą do tego kody regionów określające, w której części świata można odtwarzać płytę. Skutkowało to tym, że zapro-

jektowane na rynek europejski odtwarzacze DVD nie odtwarzały płyt przewidzianych na rynek amerykański czy azjatycki.

W chwili obecnej wiele sprzętowych odtwarzaczy nie uznaje tego typu ograniczeń, odtwarzając bezproblemowo wszystkie płyty, niezależnie od ich oznaczenia regionalnego. Również odtwarzacze programowe, działające na komputerze, najczęściej ignorują te oznaczenia.

2.3 Płyty DVD – zakazane działania

Dotyczy: płyty DVD.

Obejście: trywialne.

Część płyt DVD ma kod nakazujący odtwarzaczowi czasowe wyłączenie pewnej funkcjonalności. Najczęściej chodzi o uniemożliwienie oglądającemu ominięcie reklam lub informacji o prawach autorskich.

Większość programowych odtwarzaczy DVD oraz nowszych odtwarzaczy sprzętowych ignoruje te oznaczenia.

2.4 Adobe eBook i ograniczenia plików PDF

Dotyczy: książki elektroniczne

Obejście: w większości przypadków – trywialne.

Jedna z najsłynniejszych batalii prawnych dotyczących systemów DRM była związana z programem Advanced eBook Processor napisanym przez rosyjską firmę ElcomSoft. Program ten jako jeden z pierwszych umożliwiał ominięcie ograniczeń nakładanych przez wydawców na elektroniczne książki.

Najpopularniejszym formatem książek elektronicznych jest Adobe PDF. Teoretycznie twórca plików PDF może zabronić użytkownikowi kopiowania fragmentów pliku metodą kopiuj-i-wklej, drukowania zawartości lub odtwarzania jej za pomocą 'obcego' oprogramowania – na przykład używanych przez osoby mające problemy ze wzrokiem narzędzi do syntezy mowy.

Ograniczenia te okazały się mało skuteczne, czego dowodem jest fakt, że w internecie dostępnych jest wiele programów o funkcjonalności zbliżonej do tej dawanej przez Advanced eBook Processor. Co więcej, użytkownicy niektórych programów do oglądania PDFów (np niektórych wersji xpdf czy GhostView) mogą nawet nie zdawać sobie sprawy z istnienia ograniczeń – część popularnego oprogramowania ignoruje większość restrykcji.

Poza standardowym systemem ograniczeń zaprojektowanym przez firmę Adobe[1], twórcy książek mogą stosować zewnętrzne "wtyczki" realizujące podobną funkcjonalność. Opis ominięcia[2] "zabezpieczeń" stosowanych przez największą internetową księgarnię, Amazon.com, zajmuje 50 linijek. Przygotowana na konferencję DefCon 2001 prezentacja Dmitrija Sklyarova[3] jest analizą poważnych słabości kilku innych komercyjnych systemów.

Najprostszym, niewymagającym od użytkownika instalacji jakiegokolwiek oprogramowania sposobem obejścia restrykcji wbudowanych w pliki PDF jest skorzystanie z opcji "Zobacz jako HTML" wbudowanej w wyszukiwarkę Google oraz system pocztowy GMail.

2.5 AACS – Advanced Access Content System

Dotyczy: płyty Blue-ray, HD-DVD

Obejście: Autor kodu DeCSS Jon Johansen zapowiada złamanie na przełom 2006/2007 r.

[1] Informacja o jego obejściu: `http://www.cs.cmu.edu/~dst/Adobe/Gallery/anon21jul01-pdf-encryption.txt`

[2] `http://www.cs.cmu.edu/~dst/Adobe/Gallery/amazon-remedy.txt`

[3] `http://www.cs.cmu.edu/~dst/Adobe/Gallery/defcon.ppt`

Advanced Access Content System (AACS) to standard ograniczania dostępu i kopiowania zaprojektowany z myślą o dyskach optycznych i DVD następnej generacji. Według jego specyfikacji technicznej, odtwarzanie danych z płyt korzystających z AACS będzie możliwe tylko przy pomocy sprzętu i oprogramowania wyprodukowanego przez producenta, który podpisał umowę licencyjną z twórcami standardu. Standard przewiduje możliwość uniemożliwienia odtwarzania nowych płyt przez urządzenia, których klucze deszyfrujące zostałyby upublicznione. Daje również producentom płyt możliwość zablokowania ich odtwarzania w przypadku, gdyby dany krążek był masowo klonowany.

Informacje o zablokowanych urządzeniach oraz płytach, które mimo poprawności kodów nie będą mogły być odtwarzane będą rozprowadzane na nowo wydanych filmach. W praktyce oznacza to, że nawet posiadacze licencjonowanych filmów mogą zostać pozbawieni możliwości ich oglądania, jeśli taka będzie decyzja ich producenta.

Podstawą standardu, podobnie jak w przypadku opisanego wcześniej CSS, jest tajność kluczy deszyfrujących. Oznacza to, że w przypadku prawnego zakazu obchodzenia AACS, niedozwolone będzie napisanie oprogramowania odtwarzającego dane z dysków AACS dostępnego wraz z kodem źródłowym.

2.6 Broadcast flag

Dotyczy: Cyfrowe radio i telewizja

Obejście: Brak znanych urządzeń i nadawców wykorzystujących BF

Broadcast Flag to informacja nadawana jednocześnie z cyfrowym sygnałem telewizyjnym lub radiowym, która wskazuje, m.in. czy dany program może zostać nagrany przez odbiorcę. Możliwe ograniczenia to: zakaz nagrywania, zakaz tworzenia kopii raz stworzonego nagrania, zmniejszenie jakości podczas nagrywania, zakaz przewijania reklam (możliwość

udostępniana przez system TIVO).

Według propozycji prawnych w niektórych krajach, urządzenia, które są w stanie interpretować te flagi, nie mogłyby przesyłać sygnałów do urządzeń ich nie obsługujących. Uniemożliwiłoby to np. nagranie obrazu z cyfrowego odbiornika na analogowym magnetowidzie lub wyprodukowanym wcześniej urządzeniu nagrywającym DVD, zaś cyfrowy magnetowid wykorzystujący BF nie mógłby zostać podłączony do starszego telewizora.

Broadcast Flag nie jest jeszcze stosowana w praktyce.

2.7 Trusted Computing

Do dopisania.

2.8 XCP – Extended Copy Protection, First4Internet i Sony BMG

Dotyczy:
Obejście:

Do dopisania.

3 dalej są moje notatki

W odpowiedzi na pytania, czym ma być ten dokument i czy nie mówi przypadkiem “wprowadzajmy DRM, bo i tak niegroźny”. Ta - przedstawiająca tylko fakty, a nie opinie - analiza ma towarzyszyć innym tekstom, które będą wyjaśniać, dlaczego DRM nie jest systemem chroniącym autorów, lecz w połączeniu ze zmodyfikowanym systemem prawnym będzie służyć raczej zawłaszczaniu przez producentów rynku i zmuszaniu klientów do kilkukrotnego

płacenia za to samo.

- Microsoft is incorporating features into its next-generation operating system, Windows Vista, to take advantage of DRM capabilities of trusted platform module (TPM) chipsets. TPM chipsets have the capability to store the keys, passwords or certificates attached to DRM-enabled files and only allow decoding by authorized users.
- usunięcie analogowych wyjść do 2010
- obniżanie rozdzielczości
- pary kluczy, niewpuszczanie konkurencji na rynek (tivo, vcr, Slingbox)
- it allows the seller to retain control of the use of the disc forever," says Evangelist.
- hdtv
- analog hole
- związki technical measures (skuteczne/techniczne) a trusted computing
- co z kluczem procesora? czy jest wykorzystywany

Spis treści

1 Digital Rights Management **1**

1.1 Definicja DRM 1

2 Istniejące systemy DRM **3**

2.1 CSS – Content Scramble System 3

2.2 Płyty DVD – regionalizacja 3

2.3 Płyty DVD – zakazane działania 4

2.4 Adobe eBook i ograniczenia plików PDF 4

2.5 AACS – Advanced Access Content System 5

2.6 Broadcast flag 6

2.7 Trusted Computing 7

2.8 XCP – Extended Copy Protection, First4Internet i Sony BMG 7

3 dalej są moje notatki **7**