

Pułapka DRM

15 czerwca 2009

FAŁSZYWE ROZUMOWANIE DRM

Bez względu na to, czy jesteś zaawansowanym technicznie użytkownikiem komputera, czy też nie, ostatnio słyszysz wokół siebie dużo na temat DRM, czyli zarządzania prawami (eufemizm na restrykcje) cyfrowymi, znanego też jako IRM („I” od informacji). Czasem wspomina się o tym wyraźnie, innym razem jest ukryte w cechach oprogramowania, które będzie twierdzić, że potrafi ograniczyć sposób, w jaki ktoś inny będzie używał danych, które mu dałeś. DRM jest na przykład częścią pakietu Microsoft Office 2003.

Ale dlaczego powinno Cię to obchodzić? W tym artykule postaram się podsumować i krótko wyjaśnić czym jest DRM, jakie są z nim problemy i dlaczego NIE POWINIENES się na ten system zgadzać.

CZYM JEST DRM/IRM?

DRM (lub IRM jak Microsoft nazwał to w Office 2003 – bez różnicy) jest ogólnym określeniem na mechanizm, który umożliwia komuś umieszczenie arbitralnych restrykcji na nośniku cyfrowym. Zawartością nośnika może być cokolwiek, od nagrania dźwiękowego/muzycznego do dokumentu tekstowego. Na przykład dostawca DRM twierdzi, że muzyk używający DRM może sprzedawać nagrania w „niekopiowalnej” postaci cyfrowej. Podobnie, poprzez DRM, twórca dokumentu przed rozpoczęciem jego dystrybucji w cyfrowej formie może nałożyć na niego ograniczenia takie jak np.: „nie możesz tego wydrukować” lub „możesz przeglądać ten dokument tylko 5 razy”.

Zapytasz pewnie, w czym tkwi problem? Pozornie niektóre z zakładanych celów DRM wydają się brzmieć sensownie, np. chronienie dokumentów poufnych przed rozpowszechnianiem. Jeśli jednak uważniej zastanowisz się nad konsekwencjami, zorientujesz się, że jest to nie tylko błędna u podstaw, ale

również przerażająca technologia. Jeśli zostanie zaakceptowana i użyta na masową skalę, dogłębnie dotknie społeczności, które opierają się głównie na cyfrowej komunikacji.

– Wyobraź sobie książkę, której strony zostaną na stałe sklejone po tym jak ją przeczytasz.

– Wyobraź sobie dokument, który ulegnie samozniszczeniu, jak w filmie Mission Impossible, jeśli spróbujesz opuścić pomieszczenie.

– Wyobraź sobie telefony, które działają tylko wtedy, gdy obaj rozmówcy mają ten sam typ i model aparatu.

Brzmi niedorzecznie? To tylko łagodny przedsmak tego, w jaki sposób DRM może Cię dotknąć.

„TRUSTED COMPUTING”?

Sprzedaż DRM i pokrewnych technologii, przy nacisku sprzedawców na opinię publiczną, odbywa się pod sztandarem inicjatyw eufemistycznie nazywanych „trusted computing”, których DRM jest częścią i dzięki którym Twój komputer będzie rzekomo bardziej godny zaufania i bezpieczniejszy. Jak na ironię prawdziwe jest odwrotne twierdzenie. DRM odbiera Ci kontrolę nad Twoim komputerem i przekazuje ją firmom trzecim. Jak powiedział Richard Stallman w swoim artykule pt. „Czy możesz ufać swojemu komputerowi?": „Większości ludzi uważa, że ich komputery powinny być posłuszne im, a nie komuś innemu. Zgodnie z planem zwanym „trusted computing” wielkie korporacje medialne (włączając w to wytwórnie filmowe i nagraniowe) wraz z firmami komputerowymi, jak Microsoft i Intel, planują uczynić Twój komputer posłuszny im, nie Tobie.”

„Trusted computing” oznacza tak naprawdę, że firmy trzecie (np. wytwórnie filmowe i nagraniowe) zyskają pewność, że Twój komputer nie robi rzeczy, których nie chcą, żeby robił.

Firmy opracowujące niektóre rodzaje DRM i związany z DRM

sprzęt/oprogramowanie twierdzą, że DRM jest w zasadzie nieszkodliwe i neutralne, i że jest całkowicie dobrowolne. Faktycznie istnieje kilka potencjalnie nieszkodliwych zastosowań DRM, ale w rzeczywistości w DRM chodzi tylko o przejęcie kontroli nad Twoim własnym komputerem i jeśli zostanie ono zaakceptowane, będzie dobrowolne w takim samym stopniu, w jakim dobrowolne jest posiadanie konta bankowego – możesz go nie posiadać, ale we współczesnym społeczeństwie nie będziesz mógł bez niego zrobić wielu rzeczy.

PRZENOŚNA PRZEGRYWARKA, NIEKOMPATYBILNOŚĆ RZĄDZI

Przenośność zawsze była problemem w komputerowym świecie. Przez dekady ludzie używający różnych typów systemów komputerowych musieli pokonywać przeszkody, by wymieniać dokumenty i inne dane. Jest to spowodowane brakiem ogólnie przyjętych standardów. Wcale jednak tak być nie musi. Ostatnimi laty wraz ze wzrostem znaczenia Internetu i sieci WWW, zostały podjęte kroki w kierunku uzyskania przenośności.

Internet po prostu nie mógłby istnieć bez przenośności, która jest kluczem do jego sukcesu. Wspólne standardy komunikacji oznaczają, że istnieją różnorodne programy sieciowe, które porozumiewają się między sobą w przejrzysty sposób – właśnie tak, jak powinno być. Wysyłasz komuś e-mail i on może go odczytać, nawet jeśli używa kompletnie innego rodzaju sprzętu i oprogramowania. Podobnie, możesz przeglądać tę stronę w jednej z tysiąca przeglądarek, z których o wielu nawet nie słyszałeś (Opera, Mozilla, Netscape, Internet Explorer, Konqueror...). Mógłbyś nawet napisać własną przeglądarkę, jeślibyś poczuł taką potrzebę. Tak samo, nie ma znaczenia, czy używasz Linuksa, Windowsa, MacOS-a, AmigaOS-a, Solarisa, BeOS-a czy jakiegokolwiek innego systemu operacyjnego, a wszystko dlatego, że istnieją uzgodnione standardy przechowywania, przesyłania i odczytywania strony internetowej. Protokoły i standardy są językiem komputerowej przenośności. Gdyby każdy posługiwał się własną mową, nikt by się nie mógł porozumieć z resztą.

DRM jest śmiertelnym zagrożeniem dla komputerowej przenośności. Opiera się ono na niejawnym oprogramowaniu i formatach („językach”), które mogą być odczytane jedynie przez „uprawnione” oprogramowanie, co oznacza, że musisz użyć (i często za nie zapłacić) tego samego oprogramowania jakiego używa dostarczyciel dokumentu/e-maila/innego pliku, nawet jeśli go nie chcesz, ani nie potrzebujesz. A może dojść do tego, że nie będziesz w stanie uruchomić niezbędnego oprogramowania na swoim komputerze. W takich przypadkach możesz oczekiwać, że oprogramowanie zdoła obejść problemy (np. łamiąc DRM), tak jak to się działo w przeszłości z niekompatybilnymi formatami plików itp. Jest to z pewnością technicznie wykonalne. Ale po co to robić, skoro to strata zasobów, które mogłyby być lepiej wykorzystane do sprawienia, by nasze komputery lepiej dla nas pracowały. Jednak ta sama grupa, która promuje DRM, po cichu wywiera naciski na prawodawstwo, by jeszcze bardziej rozszerzyć wpływ swojego oligopolu poprzez zakazanie ludziom tworzenia kompatybilnego oprogramowania – ustawy Digital Millennium Copyright Act (DMCA) w Ameryce i EU Copyright Directive (EUCD) w Europie. Te drakońskie prawa uczynią nielegalnym pisanie programów wymierzonych przeciw DRM. Innymi słowy, zostaniesz postawiony przed wyborem między całkowitym brakiem dostępu do treści zabezpieczonej DRM a przymusowym zaakceptowaniem niepotrzebnego i wybrakowanego oprogramowania, które tą treść obsługuje.

POZWOLENIE FIRMOM NA USTANAWIANIE PRAWA

DRM pozwala firmom i innym twórcom rościć sobie prawa, które im nie przysługują. Na przykład, zgodnie z prawem autorskim obowiązującym w większości państw, wolno Ci skorzystać z fragmentów chronionych materiałów (jak muzyka, książki, filmy itp.) w celu recenzji. Gdy jednak te materiały są chronione przez DRM, osoby trzecie (jak np. twórca dzieła) mogą zapobiec skorzystaniu z tego prawa. A dzięki wyżej wymienionym ustawom, które wsparli monopolisci świata IT, istnieje spore

prawdopodobieństwo, że zostaniesz uznany za przestępcę próbując wyegzekwować prawo do korzystania z materiałów chronionych w celu recenzji. A zatem udało im się wymusić stosowanie ich własnych praw, które stały się nadrzędne do naszych (i tak w przypadku praw autorskich skierowanych przeciwko konsumentowi).

GROŻNE KONSEKWENCJE

Istnieje prawie nieskończona liczba przykrych, niezamierzonych konsekwencji DRM i nie ma wątpliwości, że wraz z upływem czasu dużo nowych wyjdzie na jaw – ale wtedy będzie już za późno. Mogę tu jedynie delikatnie poruszyć ten temat. Na przykład, zagłębiając się w poruszony powyżej wątek niszczenia dokumentów, konsekwencje oszustw są okropne i – w kontekście Enronu i podobnych spraw – niemal niewyobrażalne. Wyobraź sobie pracę dla oszukańczej firmy – jesteś w posiadaniu dowodu, że kradną miliony funtów, bądź nielegalnie produkują broń. Ale jedynym dowodem jest wewnętrzny dokument. Jeśli ten dokument jest chroniony przed kopiowaniem, drukowaniem i rozsyłaniem przez DRM, co możesz zrobić?

A co z elektronicznymi gazetami zabezpieczonymi przez DRM? W usieciowionym świecie prawdziwie orwellowska wizja (jak ta przedstawiona w książce „Rok 1984”) fałszowania historii mogłaby się spełnić. DRM mógłby pozwolić autorowi na zmianę dokumentu i elektroniczne zniszczenie pozostałych kopii, gdziekolwiek na świecie by się nie znajdowały. Czy to tylko przesadzona paranoja? Nie, to jest rzeczywistość i jest możliwa teraz – jedyną przeszkodą jest fakt, że DRM nie jest – na razie – powszechny.

CZYNNIK SPRZĘTOWY

Uświadomiwszy sobie, że dopóki użytkownicy będą posiadali kontrolę nad swoimi komputerami, będzie można złamać lub obejść DRM (nawet przy zniechęcającym do tego prawie), orędownicy DRM we współpracy z producentami sprzętu, takimi

jak Intel, mają nadzieję na połączenie tajnego oprogramowania ze specjalnym sprzętem wbudowanym w komputer, tak aby wyprodukować rozwiązanie „nie do złamania”, które odbierze użytkownikom prawo do wpływania na pracę ich komputera, przynajmniej jeśli chcą używać DRM. Więcej informacji można znaleźć na FAQ dotyczącym TCPA/Palladium.

FAŁSZYWE ROZUMOWANIE DRM: TECHNICZNE ROZWIĄZANIA SPOŁĘCZNYCH PROBLEMÓW

Podsumowując, DRM podejmuje próbę rozwiązania zbioru domniemyanych problemów (które, jeśli nawet rzeczywiście istnieją, są problemami społecznymi) poprzez technologię. Jakby tego było mało, tworzy podstawy do historycznie bezprecedensowego państwa policyjnego, gdzie nawet codzienne czynności stają się przedmiotem elektronicznych ograniczeń i nadzoru.

DRM zmusza społeczeństwo do dokonania jasnego wyboru. DRM może zostać przechytzone. Aby mogło działać musi być usankcjonowane prawnie i muszą być ponoszone tego konsekwencje. Nawet jeśli miałyby to oznaczać niewinnych ludzi, którzy zostaliby uwięzieni jedynie za napisanie programu umożliwiającego im przeczytanie książki lub odsłuchanie utworu muzycznego. Bezkarne byłyby przestępstwa popełniane przez korporacje, gdyż dowody mogłyby być natychmiastowo niszczone lub nie mogłyby opuścić określonego otoczenia. Mamy prosty wybór i Ty masz prosty wybór dotyczący wsparcia DRM lub nie. Czy warto zapłacić tę cenę?

CO MOŻNA ZROBIĆ?

DRM niestety już tu jest. Jest dość prawdopodobne, że masz w komputerze aplikacje współpracujące z DRM (choć możesz sobie nie zdawać z tego sprawy). Wciąż jednak możesz powstrzymać największe zagrożenia płynące z DRM poprzez podjęcie świadomej decyzji o nieakceptowaniu go – ani w życiu prywatnym, ani zawodowym. Tu jest kila rzeczy które możesz zrobić:

- Nie kupuj, ani nie instaluj oprogramowania współpracującego z DRM.
- Nie kupuj materiałów (takich jak muzyka, filmy, e-booki itp.) zabezpieczonych przez DRM. Nie chcesz wybrakowanego produktu, więc go nie akceptuj. Domagaj się, aby zaopatrywano Cię w produkty o otwartym formacie, które dają wolność użytkowania w sposób, który odpowiada Tobie, a nie sprzedawcy.
- Kiedy ktoś pierwszy wysyła Ci (lub proponuje wysłanie) dokument, e-mail czy inny plik, który da się otworzyć jedynie przez oprogramowanie wspierające DRM, odmów przyjęcia. Wyjaśnij uprzejmie sytuację i gdy nadawca nie ufa Ci na tyle, by wysłać Ci plik w niezastrzeżonym formacie, niech Ci go w ogóle nie wysyła.
- Przede wszystkim nie pozwól na zmuszenie Cię do przyjęcia DRM.

Autor: Tim Jackson

Źródło: [Wiki Jakilinux.org](http://Wiki.Jakilinux.org)

Na licencji Uznanie autorstwa – Użycie niekomercyjne 3.0 Unported