OCHRONA PRAW CYFROWYCH: PODEJŚCIA TECHNICZNE

WPROWADZANIE

Odkąd publikacje i handel zostały wprowadzone do świata cyfrowego, zagrożenia dla własności intelektualnej i prywatności w cyberprzestrzeni stale rosły na porównywalnych, ale odrębnych ścieżkach. Te ścieżki się teraz zbiegły. Niestety, wiele razy działania antypirackie prowadzą do możliwych naruszeń prywatności.

Wysiłki mające na celu powstrzymanie napływu pirackiego oprogramowania na całym świecie pozostają przeciętne pod względem skuteczności; w nowym tysiącleciu piractwo wciąż jest wielkim biznesem. Według Business Software Alliance (BSA) „globalny wskaźnik piractwa oscylował w 2011 r. na poziomie 42 procent, podczas gdy stale rozwijający się rynek w krajach rozwijających się spowodował, że wartość komercyjna kradzieży oprogramowania wyniosła 63,4 miliarda dolarów". Co więcej, „te zaskakujące odkrycia pochodzą z ankiety przeprowadzonej wśród około 15 000 użytkowników komputerów w 33 krajach, którzy razem stanowią 82 procent światowego rynku komputerów PC"1. start-upy oprogramowania na całym świecie. Jednocześnie wolności tkwiące w Internecie sprawiły, że zachowanie prywatności danych osobowych stało się prawdziwym wyzwaniem. Kradzież tożsamości stale rośnie, ponieważ coraz więcej firm aktywnie angażuje się w gromadzenie danych klientów za pośrednictwem e-commerce. Płacąc rachunki, sprawdzając rachunki ubezpieczenia medycznego lub wypełniając podatki online, ludzie udostępniają swoje dane osobowe do gromadzenia, udostępniania i regurgitacji do tego stopnia, że po prostu „googlowanie" własnej tożsamości może naprawdę otworzyć oczy. Technologie mające na celu zapobieganie piractwu mogą potencjalnie wykorzystywać bogactwo dostępnych danych osobowych w sposób, który znacznie ogranicza prywatność osobistą. W szczególności niektóre z tych technologii rutynowo wysyłają do serwerów informacje umożliwiające identyfikację osób (patrz np. rozdział 42.4.2). Pomysł, że korporacja – lub rząd – może skanować, co konkretna osoba czyta, czego słucha lub co postrzega, jest powodem do niepokoju dla libertarian obywatelskich.

Prawa cyfrowe

W tym środowisku szybkich zmian zarówno w zakresie piractwa, jak i prywatności, nawet termin „prawa cyfrowe" jest niejednoznaczny. Kiedy firmy programistyczne i producenci muzyczni mówią o prawach cyfrowych, mają na myśli prawa chronione od dawna przez prawo autorskie, znak towarowy i prawo patentowe. Kiedy obrońcy prywatności spierają się o prawa cyfrowe, mogą jednak mówić o czymś zupełnie innym: że dana osoba nie traci praw osobistych, w tym prawa do prywatności, po prostu włączając komputer. Ten rozdział koncentruje się głównie na technologiach zaprojektowanych w celu ochrony tradycyjnych praw producentów treści, ale wymienia również obszary, w których technologie te zagrażają prywatności osobistej.

Prawa dotyczące patentów, praw autorskich i znaków towarowych.

Istnieją różnice między obowiązującymi przepisami i materiałami, które chronią. Patenty dają właścicielom wyłączne prawa do używania i licencjonowania ich pomysłów i materiałów; patenty generalnie chronią nieoczywiste wynalazki w dziedzinach mechanicznych i elektrycznych, a także te, które mogą być zawarte w oprogramowaniu i sprzęcie komputerowym. Prawa autorskie dają właścicielom wyłączne prawa do tworzenia dzieł pochodnych, powielania oryginalnych prac oraz wyświetlania, rozpowszechniania i prowadzenia ich prac. Prawa autorskie mają zastosowanie do oryginalnych dzieł autorskich, w tym obrazów, fotografii, rysunków, pism, muzyki, filmów wideo, oprogramowania komputerowego i wszelkich innych dzieł utrwalonych na materialnym nośniku. Prawa autorskie, ich naruszenie i środki zaradcze są opisane w ustawie o prawie autorskim z 1976 r.

Znaki towarowe dają właścicielom prawo do ograniczenia używania znaków wyróżniających w określonych kontekstach. Prawa te mogą dotyczyć słów, dźwięków, wyróżniających się kolorów, symboli i wzorów. Obszerne omówienie prawa własności intelektualnej znajduje się w rozdziale 11 niniejszego Podręcznika.

Piractwo

Piractwo, które kiedyś uważano za zwykłe naruszenie praw autorskich do druków lub produkcję podrabianej taśmy audio, rozwinęło się wraz z technologią i rozszerzyło się na własność intelektualną, dane cyfrowe, płyty DVD, CD, VHS, telewizję analogową i wysokiej rozdzielczości oraz media strumieniowe .Istnieje kilka rodzajów piractwa. Piractwo użytkowników końcowych ma miejsce, gdy użytkownicy końcowi używają jednej kopii oprogramowania do uruchamiania w kilku różnych systemach lub gdy rozpowszechniają kopie oprogramowania innym osobom bez zgody producenta oprogramowania. Piractwo sprzedawców ma miejsce, gdy pozbawieni skrupułów sprzedawcy dystrybuują wiele kopii jednego pakietu oprogramowania wielu klientom, wstępnie ładują to samo oprogramowanie w wielu systemach lub świadomie sprzedają fałszywe oprogramowanie klientom. Piractwo internetowe i tablice ogłoszeń (BBS) ma miejsce, gdy użytkownicy pobierają i przesyłają materiały chronione prawem autorskim oraz wykorzystują je lub udostępniają do użytku innym osobom bez odpowiednich licencji. Aby zrozumieć, dlaczego i w jaki sposób występuje piractwo oraz ogromny wpływ na społeczeństwo na całym świecie, musimy dobrze zrozumieć, co rozumiemy przez słowo „piractwo". Za każdym razem, gdy informacje są tworzone i publikowane w formie drukowanej, w Internecie lub włączone do oprogramowania, informacje te mogą być chronione prawem autorskim, patentowym lub prawem do znaków towarowych. Zasada ta dotyczy szerokiego spektrum materiałów, które obejmują na przykład specyfikacje braci Wright dla ich „latającej maszyny"; oprogramowanie Microsoft Windows; ikona Myszka Miki i wszystkie powiązane materiały; a także programy telewizyjne, sztuki teatralne, filmy i muzykę tworzone i wykonywane na żywo i na nagraniach. Wykonywanie nieautoryzowanych kopii takich materiałów na jakimkolwiek nośniku jest określane jako piractwo. W ciągu ostatnich trzech lat Stowarzyszenie Przemysłu Oprogramowania i Informacji „wniosło w Stanach Zjednoczonych ponad 100 pozwów przeciwko nielegalnym sprzedawcom eBay, a także sprzedawcom na innych stronach internetowych zajmujących się podrabianym, OEM, akademickim, specyficznym dla regionu i innym nielegalnym oprogramowaniem oraz publikacje. Oskarżeni zapłacili miliony dolarów odszkodowania, a w niektórych przypadkach ścigano zarzuty karne, a oskarżonych skazano na karę więzienia.

Prywatność

Podobnie jak w wielu aspektach bezpieczeństwa, użytkownicy końcowi są obecnie wzywani do ochrony swojej tożsamości online (i offline) poprzez staranne monitorowanie działań finansowych oraz programy uświadamiające skoncentrowane na prawach osobistych, prawach i obowiązkach związanych z korzystaniem z Internetu. Przeciętny użytkownik Internetu może dziś tworzyć i publikować w sieci blog lub osobiste wideo szybciej niż ten sam użytkownik może zastosować poprawki oprogramowania na komputerze stacjonarnym. Ta nowa funkcja jest tak powszechna, że prawo musi jeszcze dogonić potrzeby i oczekiwania użytkowników w społeczeństwie internetowym. Trudno jest zachować prywatność danych, gdy — jednym kliknięciem myszy — łatwo jest udostępniać dane osobowe całemu światu. Oprócz złych nawyków osobistych, które ograniczają prywatność, zupełnie nowa klasa aplikacji określanych jako zarządzanie prawami cyfrowymi (DRM) gromadzi więcej danych osobowych niż kiedykolwiek wcześniej w celu ograniczenia niewłaściwego wykorzystania materiałów chronionych prawem autorskim. Produkty DRM mogą rejestrować i raportować zwyczaje osoby związane z przeglądaniem sieci Web, rodzaje plików tworzonych i dostępnych przez określony program, liczbę zastosowań danego pliku lub programu, źródłowy adres IP systemu użytkownika oraz

obecność (lub brak) licencja na program. W imię ochrony praw cyfrowych dla producentów treści, konsumenci tych treści są katalogowani i śledzeni w sposób, którego twórcom praw autorskich trudno byłoby sobie wyobrazić.

TECHNIKI ANTYPIRACYJNE OPARTE NA OPROGRAMOWANIU

Stosuje się różne podejścia techniczne oparte na oprogramowaniu, aby zapobiec niewłaściwemu wykorzystaniu materiałów chronionych prawem autorskim lub w inny sposób chronionych w sieciach organizacji i w publicznym Internecie. Obecne metody obejmują zapewnienie właściwej konfiguracji działania systemu, monitorowanie zainstalowanego oprogramowania, szyfrowanie treści i wstawianie pewnego rodzaju klucza lub identyfikatora do samego produktu cyfrowego

Polityka organizacyjna

Kontrole w samodzielnych aplikacjach komercyjnych stanowią tylko jeden z technicznych środków ochrony treści cyfrowych. W tym zakresie przydatne są również istniejące kontrolki systemowe. Kontrola dostępu do systemu operacyjnego może określać, kto może uzyskać dostęp do określonej zawartości, podczas gdy szyfrowanie obsługiwane przez system operacyjny i inne aplikacje może ograniczyć dostęp do użytkowników posiadających odpowiedni klucz. Bardziej ogólnie, polityka organizacyjna powinna określać dobre praktyki w zakresie konfigurowania systemów operacyjnych i aplikacji w celu ochrony treści. Taka polityka obejmuje:

* Zezwalaj użytkownikom na instalowanie tylko niezbędnego oprogramowania.

* Szyfruj informacje, które nie powinny być widoczne publicznie.

* Zainstaluj oprogramowanie z najniższymi możliwymi uprawnieniami zgodnymi z możliwością wykonywania swojej pracy.

* Wyłącz aktywną zawartość (Java, JavaScript, ActiveX, pliki cookie itp.) tam, gdzie to możliwe.

* Użyj kontroli dostępu do sieciowego systemu operacyjnego, aby ograniczyć dostęp do udostępnionych multimediów chronionych prawami autorskimi członkom organizacji, dla których zakupiono licencje.

Liczniki wykorzystania oprogramowania

Pomiar oprogramowania jest popularny od kilku lat. Specjalne oprogramowanie monitoruje wykorzystanie systemu i inwentaryzuje oprogramowanie w systemie lub sieci. Tego typu oprogramowanie może być również używane do blokowania lub ograniczania korzystania z określonego oprogramowania, takiego jak przeglądarki i gry. Oprócz walki z piractwem może zmniejszyć obciążenie personelu IT, zmniejszając komplikacje spowodowane użyciem nieautoryzowanego oprogramowania.

Kontrolowanie równoległych instalacji

Produkty do pomiaru oprogramowania mogą monitorować współbieżne instalacje nawet w sieciach używanych przez osoby z różnych obszarów geograficznych, które mają różne wymagania i zainstalowane inne oprogramowanie. Oprogramowanie pomiarowe umożliwia administratorowi prowadzenie aktualnej i zaktualizowanej inwentaryzacji oprogramowania zainstalowanego w różnych lokalizacjach w sieci. Dzienniki pokazują, gdzie miała miejsce instalacja, kiedy wygasają licencje i kiedy konieczne są aktualizacje. Alerty można ustawić tak, aby powiadamiały administratorów systemu o zbliżającym się wygaśnięciu licencji lub zakończeniu aktualizacji.

Kontrolowanie równoczesnego użytkowania

Pomiar oprogramowania pozwala administratorom sieci identyfikować i rozwiązywać przypadki nielegalnej instalacji nieautoryzowanych kopii autoryzowanego oprogramowania, a także wyłapywać osoby, które instalują nieautoryzowane oprogramowanie na komputerach organizacji. Oprogramowanie pomiarowe pozwala również firmie raportować i analizować czasy logowania i wylogowania, śledzić wykorzystanie oprogramowania oraz licencje na oprogramowanie pomiarowe, aby zachować legalność w firmie. Oprócz unikania uwikłań prawnych monitorowanie może zmniejszyć zapotrzebowanie na zasoby systemowe, przepustowość sieci i personel wsparcia technicznego.

Przykłady i implementacja

Firma Microsoft ogłosiła w 2000 r., że w celu zwalczania piractwa nowe wersje programu Office 2000 będą zawierały funkcję zliczania powodującą nieprawidłowe działanie programów, jeśli właściciel nie zarejestrował oprogramowania po jego uruchomieniu 50 razy.4 Przed tym ogłoszeniem firma Microsoft opublikowała literaturę antypiracką i zapewnił szeroką edukację konsumencką dotyczącą wpływu piractwa komputerowego na społeczeństwo; utworzyła również infolinię ds. piractwa (1-800-RU-LEGIT). Novell (1-800-PIRATES), Adobe i Xerox to inne firmy, które mają silne programy antypirackie, chociaż nie ogłosiły jeszcze, że wbudowują mierniki w swoje produkty. Oprogramowanie pomiarowe wymaga licencji w dobrej wierze, aby zostało wdrożone. Zazwyczaj firmy tworzą klucze CD-ROM, które są drukowane na legalnych kopiach dysków instalacyjnych ich produktów lub pudełkach z biżuterią. Klucze zawierają sumy kontrolne lub kody uwierzytelniania wiadomości, które mogą być sprawdzone przez procedury instalacyjne. Algorytmy dla sum kontrolnych mają na celu sprawianie trudności osobom próbującym stworzyć fałszywe klucze. Bezpieczeństwo takich środków zależy od siły kryptograficznej kluczy walidacji. Liczniki oprogramowania do kontrolowania współbieżnego użycia muszą bezpiecznie przechowywać informacje, aby każda operacja ładowania zwiększała licznik, a każda operacja rozładowywania zmniejszała go. Jednak problemem bezpieczeństwa jest przechowywanie tych informacji w taki sposób, aby nieupoważnione osoby nie mogły ich łatwo modyfikować. Szyfrowanie danych w złożonej sekwencji operacji może powstrzymać większość nadużyć systemu, czyniąc wysiłek wymagany do obejścia mechanizmów bardziej kosztownym niż zakup licencji. Ostatnio, począwszy od Visty, kopie systemu operacyjnego Windows muszą zostać zarejestrowane (Microsoft nazywa to aktywacją kopii) zaraz po instalacji, w przeciwnym razie przejdą w tryb zmniejszonej funkcjonalności, w którym podstawowe funkcje są dostępne tylko przez godzinę pracy przed zalogowaniem ponownie. Do użytku domowego z pojedynczą kopią system Windows opiera się na kluczu licencyjnym zakodowanym na nośniku instalacyjnym. W przypadku wdrożeń systemu Vista w przedsiębiorstwach organizacja musi uruchomić serwery kluczy, aby umożliwić przeprowadzenie rejestracji.

SPRZĘTOWE TECHNIKI ANTYPIRACYJNE

Pracując nad teorią, że oprogramowanie jest podatne na błędną konfigurację i kompromisy, grupy antypirackie i badacze eksperymentowali z różnymi podejściami sprzętowymi, aby zapobiegać niewłaściwemu korzystaniu z chronionych treści. Techniki te obejmują klucze sprzętowe i wyspecjalizowane czytniki dołączone do sprzętu do czytania, nośniki zanikające przeznaczone do przeglądania lub odtwarzania tylko ograniczoną liczbę razy oraz klucze programowe wbudowane w nośnik i sprzęt do czytania.

Klucze sprzętowe

Klucze sprzętowe to sprzętowe urządzenia blokujące lub moduły, które łączą się z komputerem i komunikują z oprogramowaniem działającym na komputerze. Bez klucza sprzętowego urządzenie

zewnętrzne lub regulowane oprogramowanie nie działa w pełni lub w ogóle. Początkowo klucze sprzętowe kontrolowały drukowanie. Po zainstalowaniu na komputerze klucza sprzętowego nikt nie mógł drukować danych z komputera bez autoryzacji. Jednak obecnie istnieje konieczność ochrony wszystkich typów urządzeń. Teraz klucze sprzętowe są używane do ochrony skanerów; dyski zewnętrzne (np. dyski ZIP); Płyty CD-ROM i płyty CD-ROM wielokrotnego zapisu; DVD i DVD-R; rejestratory VHS; Systemy gier wideo PlayStation, Nintendo i Sega; a nawet osobistych asystentów cyfrowych (PDA). Najpopularniejszy typ klucza sprzętowego zapewnia port przelotowy do podłączenia kabla urządzenia. Zasadniczo klucz sprzętowy zawiera pewien rodzaj szyfrowania algorytmicznego we wbudowanych obwodach mikroelektronicznych. Zaawansowanie szyfrowania różni się w zależności od producenta i urządzenia. Wiele kluczy zapewnia dodatkową wbudowaną pamięć nieulotną, do której oprogramowanie ma dostęp. Niektóre modele mają nawet kontrole w czasie rzeczywistym, które śledzą informacje o dacie i godzinie, w tym o wygaśnięciu licencji aplikacji (tymczasowej lub dzierżawionej).

Klucze sprzętowe zapewniają pewne określone korzyści:

* Ponieważ klucz sprzętowy jest urządzeniem zewnętrznym, jego instalacja i dezinstalacja jest dość prosta. Wczesne klucze sprzętowe wykorzystywały porty szeregowe lub równoległe, ale USB stało się normą w ostatnich latach. W większości przypadków, ponieważ producenci wspierają swoje urządzenia, zwykły użytkownik może zainstalować i używać klucza bez pomocy działu IT.

* Klucze sprzętowe wymagają również rejestracji, co zapewnia odpowiednią kontrolę nad użyciem klucza, a tym samym zapewnia legalność zarówno urządzeniu, jak i użytkownikom. Rejestracja (zależna od zawartej umowy) może zapewnić obsługę zarówno oprogramowania, jak i sprzętu.

* Klucze sprzętowe obsługujące szyfrowanie zapewniają dodatkową warstwę ochrony, uniemożliwiając odczytanie przesyłanych danych, dopóki nie dotrą do miejsca docelowego, chyba że sprzęt jest na swoim miejscu. Istnieją również wady korzystania z kluczy sprzętowych:

* Konsumenci opierają się wymogom instalacji, konserwacji i dodatkowym kosztom. Większość dużych korporacji nie używa kluczy sprzętowych do swoich produktów.

* Klucze sprzętowe mogą zostać zgubione lub skradzione, a także mogą zawieść.

* Czasami klucz sprzętowy działa dobrze na wolnym komputerze, ale powoduje błędy, gdy jest zainstalowany na szybszym komputerze.

* Ponieważ nie każdy producent automatycznie wymienia zgubione lub skradzione klucze sprzętowe bez opłat, mogą wystąpić dodatkowe koszty związane z uzyskaniem zamienników.

* Klucze sprzętowe mogą stanowić poważny problem w zarządzaniu ryzykiem w przypadku krytycznych aplikacji, w których opóźnienia w uzyskaniu zamienników lub ich zarejestrowaniu mogą być niedopuszczalne.

* Podobnie jak w przypadku każdego urządzenia, może wystąpić poważny problem, jeśli producent klucza przestanie wspierać model klucza zainstalowanego przez firmę lub jeśli producent całkowicie zniknie z działalności.

* Przepisy dotyczące korzystania z szyfrowania różnią się w różnych krajach. Wyspecjalizowane klucze sprzętowe, które mogą być legalne w Stanach Zjednoczonych, mogą być nielegalne w innym kraju

Wyspecjalizowani czytelnicy.

Jedną z przeszkód w nielegalnym kopiowaniu była kiedyś trudność i koszt uzyskania specjalistycznego sprzętu i oprogramowania do wiernego odczytu i kopiowania materiałów zastrzeżonych. Jednak dzisiaj taki sprzęt do kopiowania jest niedrogi i łatwy do znalezienia. Ponadto media do rozpowszechniania nielegalnych kopii są tańsze niż kiedykolwiek.

Audio

Według Amerykańskiego Stowarzyszenia Przemysłu Nagraniowego (RIAA), światowy przemysł audio traci co roku ponad 4 miliardy dolarów z powodu piractwa na całym świecie7. RIAA twierdzi, że w samych Stanach Zjednoczonych traci się 1 milion dolarów dziennie na samym fizycznym produkcie. Utrata przychodów z usług pomocniczych powoduje wzrost danych. Ale RIAA twierdzi, że liczby te są niskie, ponieważ szacuje, że w niektórych krajach do 98 procent używanej muzyki pochodzi z nielegalnych kopii. W ramach ogólnobranżowego, zorganizowanego podejścia do podkreślania i ograniczania problemu piractwa muzycznego, RIAA podjęła bardzo aktywną rolę w prowadzeniu działań prawnych przeciwko podejrzanym o piractwo. W latach 90. i trwając do obecnej dekady, największym problemem z piractwem audio były nielegalnie kopiowane płyty CD. Na przykład w 1998 roku RIAA skonfiskowała 23 858 nielegalnych płyt CD w pierwszej połowie roku. W tym samym roku Operacja Copycat – wspólne śledztwo prowadzone przez RIAA, Motion Picture Association of America (MPAA) i Departament Policji Nowego Jorku – doprowadziła do aresztowania 43 piratów CD i zamknięcia 15 nielegalnych zakładów produkcyjnych. Wiele płyt skonfiskowanych w tego typu operacjach najwyraźniej pochodziło z Azji i Europy Wschodniej, finansowanych przez zorganizowaną przestępczość związaną z narkotykami i prostytucją. Do 2002 r. do problemu przyczyniły się nawet sklepy spożywcze na rogu, dostarczając na monety kopiarki CD podobne do kserokopiarek, wraz ze znanym napisem ostrzegawczym przenoszącym odpowiedzialność na użytkownika. Biorąc pod uwagę ogromne zyski, problem był po prostu zbyt duży i powszechny, aby organy ścigania mogły je kontrolować. W 2005 roku RIAA skonfiskowała około 5 milionów nielegalnych płyt CD. Niedawno RIAA skupiła się na problemie plików muzycznych nielegalnie udostępnianych w Internecie. Korzystając z bezpłatnego oprogramowania, czasami już dołączonego do komercyjnych systemów operacyjnych, każdy może pobierać utwory muzyczne i nagrywać płyty CD. Format plików muzycznych MP3 stał się wszechobecnym sposobem udostępniania muzyki innym. RIAA początkowo protestowała przeciwko odtwarzaczom MP3, ale fenomenalny sukces osobistych cyfrowych odtwarzaczy muzycznych, zwłaszcza Apple iPod, sprawił, że takie wysiłki są daremne. Niektórzy muzycy i niezależne wytwórnie płytowe przyjęli format MP3 do promowania swoich płyt, co pokazuje, że sama technologia nie ma nieodłącznych związków z piractwem. Ci muzycy i studia nagraniowe twierdzą, że są zadowoleni z tego, że konsumenci pobierają muzykę i są w sprzeczności z RIAA. Niektóre grupy muzyczne eksperymentowały nawet z całkowitym zerwaniem powiązań z tradycyjnym przemysłem muzycznym, wykorzystując strony internetowe i serwisy społecznościowe do reklamowania i rozpowszechniania cyfrowych plików muzycznych bezpośrednio wśród swoich słuchaczy. Ponieważ coraz więcej muzyków zaczyna korzystać z Internetu jako uzupełnienie lub zamiast tradycyjnych modeli dystrybucji, sam model dystrybucji muzyki ulega zmianom. Tymczasem przemysł muzyczny nadal boryka się z poważnymi stratami finansowymi z powodu nielegalnego pobierania. Przemysł, za pośrednictwem RIAA, stosuje środki prawne. Niektóre ważne procesy sądowe odbiły się szerokim echem w prasie i odegrały zasadniczą rolę w egzekwowaniu lub zmianie istniejących przepisów lub we wspieraniu opracowywania nowych przepisów. Na przykład celowe naruszenie praw autorskich spowodowało przyznanie Universal Studios 50 milionów dolarów odszkodowania ustawowego i 3,4 miliona dolarów opłat prawnych w sprawie przeciwko usłudze muzycznej MyMP3.com. MyMP3 stworzył bazę danych zawierającą ponad 80 000 albumów, które w połączeniu z oprogramowaniem MyMP3 umożliwiają użytkownikom dostęp i przechowywanie muzyki w formie cyfrowej, bez ponoszenia opłat. Prawdopodobnie najbardziej rozpoznawalną nazwą w dziedzinie muzyki w odniesieniu do piractwa był

kiedyś Napster, witryna umożliwiająca osobom udostępnianie utworów muzycznych przez Internet. Witryna udostępniała bezpłatne oprogramowanie do pobrania i odtwarzania plików MP3. Zasadniczo oprogramowanie Napster zmieniło komputer użytkownika w część rozproszonej sieci serwerów, która publikowała dostępne pliki muzyczne. Witryna szybko pozyskała grupę milionów użytkowników, którzy po „samplowaniu" muzyki mogli następnie udać się do sklepu i kupić całą płytę CD. Ponieważ jednak witryna Napster nie ograniczała długości pobierania, wielu użytkowników po prostu pobrało cały utwór. Większość nigdy nie kupiła komercyjnej wersji muzyki. Do udanych prób piractwa przyczynił się rozwój i dostępność napędów CD wielokrotnego zapisu. Coraz więcej użytkowników Napstera decydowało się na pobieranie utworów muzycznych, które chcieli, a następnie wypalanie własnych płyt CD bez kupowania płyt CD wyprodukowanych przez artystów nagrywających i firmy muzyczne. Stwarzając poruszenie w branży i ostatecznie przełomową sprawę sądową, Napster został zmuszony do radykalnej zmiany działalności w marcu 2000 roku po przedłużającym się postępowaniu sądowym. W werdykcie Jack Valenti, prezes i dyrektor generalny MPAA, skomentował, że konsument odniósłby największe korzyści z orzeczenia sądu, ponieważ „nie można zabrać za darmo tego, co należy do kogoś innego". Jednak temat Napstera i piractwa audio pozostaje bardzo kontrowersyjny. Chociaż niektórzy twierdzili, że mało znani artyści zostali ujawnieni, czego mogliby nigdy nie uzyskać bez bezpłatnej usługi udostępniania plików, inni, zwłaszcza duże firmy muzyczne i artyści nagrywający, twierdzą, że odmówiono im tantiem, na które zasługują. Napster próbował odtworzyć się jako płatna usługa pobierania muzyki za subskrypcję, ale odkrył, że wytwórnie płytowe nie chcą z nią współpracować. W 2002 roku Napster spasował; nazwa została ostatecznie kupiona przez Roxio, Inc., aby zmienić nazwę własnej usługi subskrypcji. W międzyczasie inne protokoły i aplikacje do udostępniania plików peer-to-peer (P2P) wypełniły pustkę pozostawioną przez Napstera. Zanim iTunes Music Store stał się potężnym konkurentem z poparciem firmy muzycznej i ochroną praw autorskich, świat bezpłatnego udostępniania plików został ożywiony przez nazwy takie jak Gnutella, FastTrack, Grokster, Limewire i Kazaa. W ciągu ostatnich kilku lat przemysł muzyczny zidentyfikował uniwersytety jako podatny grunt dla nielegalnych działań związanych z pobieraniem plików. W 2007 roku RIAA rozpoczęła nową rundę prób postawienia piratów muzycznych przed wymiarem sprawiedliwości, wysyłając listy oferujące ugodę ze studentami zidentyfikowanymi jako prawdopodobnie udostępniający pliki chronione prawem autorskim, przed jakimkolwiek procesem. Taktyka RIAA wzbudza w społeczności szkolnictwa wyższego irytację, a przeciwnicy krytykują listy jako graniczące z wymuszeniem. Niektóre uniwersytety odmawiają przekazania listów studentom; jeden uniwersytet zgodził się na przesłanie listów, ale obiecał naliczyć RIAA 11 dolarów za każdy list, aby zapłacić za czas jego pracowników.

Wideo

Jeśli chodzi o wideo, firma Scour, Inc. zapewniła bezpłatne pobieranie filmów cyfrowych, a także oprogramowanie umożliwiające użytkownikom udostępnianie pobranych plików między sobą bez korzystania z centralnego serwera. Scour.com stał się dość popularny w krótkim czasie. Wprowadzony na rynek w 1997 roku, z funkcją wyszukiwania w Internecie dodaną w 1998 roku i późniejszym narzędziem P2P, Scour ostatecznie przyciągnął negatywną uwagę przemysłu filmowego i muzycznego. W lipcu 2000 r. MPAA, RIAA i National Music Publishers Association (NMPA) pozwały Scour, oskarżając go o kradzież na dużą skalę materiałów chronionych prawem autorskim i handel skradzionymi utworami. Do listopada 2000 roku firma przestała działać. Ta sprawa nie powstrzymała podrabiania nośników wideo. Pomimo coraz wyższych grzywien, orzeczeń sądowych, a nawet nalotów ze strony różnych organów ścigania, podrabiane filmy są łatwo dostępne. Wzdłuż Piątej Alei w Nowym Jorku za 5-10 dolarów każdy może kupić najnowsze filmy i płyty DVD; na rynkach w Hongkongu, Azji Południowo-Wschodniej i Indiach kopie są jeszcze tańsze. Prawdą jest, że niektóre z dostępnych kopii mogły zostać „legalnie wyprodukowane", ale jest bardziej niż prawdopodobne, że fałszywe lub nieuczciwe kopie zostały wykonane nielegalnie z kopii wzorcowej, która została pożyczona lub

skradziona. Postępy w elektronice użytkowej wspierają ten trend, ponieważ wiele komputerów jest obecnie wyposażonych w odtwarzacz DVD z możliwością nagrywania/wielokrotnego zapisu jako standardowy komponent. Argumenty o legalności przesuwania w czasie i przestrzeni, które kiedyś broniły praktyki tworzenia osobistych miksów na kasecie audio, przeniosły się teraz do sfery cyfrowego wideo.

Telewizja (analogowa)

Telewizja nadawcza jest jedną z najbardziej udanych technologii w historii, a interesy finansowe wciąż są ogromne, pomimo rozwoju usług kablowych i satelitarnych. W styczniu 2000 r. główne firmy telewizyjne, National Football League i National Basketball League, złożyły skargi przeciwko iCraveTV, kanadyjskiej firmie, która istniała zaledwie od roku. Zgodnie ze skargami, iCraveTV nielegalnie wykorzystywał nadawane sygnały telewizyjne bez autoryzacji lub płatności i przesyłał je na stronę internetową iCrave w celu bezpłatnego oglądania. Chociaż praktyka ta najwyraźniej nie naruszała w tamtym czasie kanadyjskich praw autorskich, amerykańscy sędziowie ogłosili w lutym 2000 r., że nieautoryzowane transmisje sygnałów nadawczych do Stanów Zjednoczonych za pośrednictwem Internetu stanowią bezpośrednie naruszenie amerykańskiego prawa autorskiego, a iCraveTV otrzymał rozkaz powstrzymania ćwiczyć. Wkrótce po tym, jak iCraveTV zgodził się na zawarcie ugody pozasądowej, witryna internetowa została zamknięta, a iCraveTV zbankrutował. Hakowanie dekoderów kablowych to kolejna technika uzyskiwania usług bez płacenia za nie. Chociaż kupowanie, instalowanie lub modyfikowanie sprzętu do konwersji zakodowanych sygnałów telewizji kablowej od płatnych programów telewizji kablowej lub innych komercyjnych dostawców nie jest nielegalne, nielegalne jest używanie takich dekoderów do uzyskiwania usług bez płacenia za nie. W Stanach Zjednoczonych Kongres nakazał, aby po 17 lutego 2008 r. wszystkie stacje telewizyjne nadawały wyłącznie w formacie cyfrowym (DTV).

Telewizja (HDTV)

Pierwszy obraz telewizyjny powstał w 1884 roku, kiedy Paul Nipkow stworzył mechaniczny dysk skanujący. Przy rozdzielczości zaledwie 18 linii obraz był słaby. Obecne transmisje telewizyjne w standardzie National Television System Committee (NTSC) są realizowane z szerokością pasma nieprzekraczającą 6 MHz. Obecny system analogowy nadaje 30 klatek na sekundę i 525 linii na ramkę. Telewizja wysokiej rozdzielczości (HDTV) to system telewizji cyfrowej, który oferuje dwukrotnie wyższą rozdzielczość poziomą i pionową niż obecny system telewizyjny. HDTV ma możliwość dostarczania wideo składającego się z około 1125 linii na klatkę i 60 klatek na sekundę. Widzowie widzą wtedy jakość obrazu zbliżoną do filmu 35 mm. Oczywiście przesyłanie obrazów zawierających tak dużą ilość informacji audio i wideo wymaga szerokiego pasma, w rzeczywistości około 18 MHz. Taka szerokość pasma pozwoliłaby na transmisję 1050 linii po 600 pikseli na linię. Jednak Federalna Komisja Łączności (FCC) postanowiła ograniczyć HDTV do maksymalnej przepustowości 6 MHz. Aby spełnić ten wymóg, zastosowana zostałaby kompresja MPEG. Kompresja MPEG stosuje algorytmy do grup pikseli i rejestruje informacje, które zmieniają się w ramce, a nie wszystkie informacje we wszystkich ramkach. Dźwięk jest zsynchronizowany z wideo. Korzystanie z MPEG pozwala zaoszczędzić miejsce na dane i wymagania dotyczące transmisji, zachowując jednocześnie wysoką jakość obrazu i dźwięku. Zgodnie ze standardem Advanced Television Committee Standard (ASTC), FCC wymaga, aby kompresja audio i wideo oraz transmisja sygnałów naziemnych HDTV były zgodne z tym standardem. Podobnie jak w przypadku wszystkich innych transmisji i mediów, istnieją poważne obawy dotyczące piractwa transmisji i programów HDTV. W chwili obecnej, mimo że wiele transmisji telewizyjnych jest zaszyfrowanych w celu udaremnienia odbioru, dość proste, choć nielegalne, jest zakup deszyfratora i rozszyfrowanie transmisji. Jednak widzowie domowi mogą nagrywać programy na własny użytek. Przestrzeń rynkowa HDTV ewoluuje, a zapotrzebowanie konsumentów na urządzenia obsługujące HD

eksplodowało w ciągu ostatnich kilku lat. Próby amerykańskich producentów telewizyjnych mające na celu ochronę siebie i swoich treści za pomocą różnych schematów szyfrowania i szyfrowania, w tym systemów szyfrowania treści (CSS), utrudniły częste zmiany w sprzęcie i formatowaniu sygnału, które towarzyszyły tej gwałtownej ekspansji rynkowej. Szyfrowanie programów telewizji naziemnej zabezpieczyłoby transmisję, ale według Koalicji na rzecz praw do nagrywania w domu (HRRC), takie szyfrowanie zagrozi ustanowionym prawom do nagrywania w domu. HRRC twierdzi, że sekcja 1202 (k) ustawy Digital Millennium Copyright Act zapewnia starannie wyważone podejście do praw do analogowego nagrywania w domu i stanowi, że nie wolno stosować nakazanej technologii w celu zakłócania nagrywania przez konsumentów bezpłatnych, naziemnych programów naziemnych. Ponadto HRRC twierdzi, że szyfrowanie bezpłatnych treści telewizyjnych nie będzie zachęcać konsumentów do przejścia ze zwykłej telewizji analogowej na cyfrową. HRRC twierdzi, że zamiast udaremniać atak cyfrowym piratom, silne szyfrowanie nałoży na konsumentów nieuczciwe, a nawet nielegalne ograniczenia.

Akceptacja przez konsumentów wyspecjalizowanych czytelników

Nielegalne udostępnianie treści chronionych prawem autorskim jest powszechne w Internecie. Kiedy powstało Software Publishing Association (SPA), grupa wraz z organami ścigania dokonała nalotów na fizyczne siedziby firm, które, jak się sądzi, używały pirackiego oprogramowania. W wyniku znalezienia ilości pirackiego oprogramowania, SPA wygrało wiele postępowań prawnych i związanych z tym ugód. Niektórzy ludzie postrzegają szyfrowanie jako wyzwanie i pracują nad łamaniem algorytmów, aby móc pirackie dane — cyfrowe, wideo lub audio. Ponadto brak standaryzacji prawa we wszystkich branżach i krajach doprowadził do kontrowersji i ciągłego piractwa. Chociaż przeciętni konsumenci nie uważają się za piratów własności intelektualnej, wielu skądinąd uczciwych obywateli otrzymuje i używa nielegalnych programów, aplikacji, gier, ścieżek audio, płyt CD, DVD, kaset VHS i sygnałów telewizyjnych. Sytuację tę można przypisać brakowi edukacji etycznej, ale wiele osób lubi oszczędzać pieniądze i po prostu nie wierzy, że zostaną złapani i ukarani za takie kradzieże. Badanie przeprowadzone w 2001 roku przez Pew Internet & American Life Project, oparte na wywiadach telefonicznych z 4205 osobami dorosłymi w wieku 18 lat i starszymi, z których około 2299 było użytkownikami Internetu, sugeruje, że około 30 milionów mieszkańców USA pobrało muzykę z Internetu. Zwrot „pobrał muzykę z Internetu" był w zasadzie odpowiednikiem „nielegalnie pobrał muzykę z Internetu", ponieważ legalne sposoby na to nie zostały jeszcze rozwinięte. Od czasu tego raportu ogłoszenie przez Apple w 2001 r. produktów iTunes i iPoda oraz uruchomienie sklepu muzycznego iTunes w 2003 r. zapoczątkowały ruch w celu zapewnienia przyjaznych konsumentom sposobów pobierania muzyki, które zapewniają również rekompensatę właścicielom praw autorskich. iTunes wykorzystuje uwierzytelnianie urządzenia i zastrzeżone formaty kodowania, aby ograniczyć redystrybucję pobranych utworów i filmów. Pomimo – a może właśnie z powodu – prób przestrzegania przez Apple praw autorskich, jasne jest, że Apple spełnił postrzeganą potrzebę na rynku, ponieważ wygenerował zarówno wielu konkurentów, jak i znaczną sprzedaż. Konsumenci pobrali pierwszy milion piosenek z iTunes Store w pięć dni, a cały rynek muzyki cyfrowej wzrósł do co najmniej 790 milionów dolarów rocznie. Przy cenie 0,99 USD za utwór liczba pobrań z iTunes Music Store przekroczyła granicę 1 miliarda dolarów 23 stycznia 2006 r.

Zanikające media

Istnieje wiele interpretacji terminu zanikające media. Szeroka interpretacja obejmuje obrazowanie cyfrowe, optykę, multimedia i inna sztuka elektroniczna oraz dane, które są krótkotrwałe lub przemijające. Gdy takie media są oryginalnymi, twórczymi dziełami, społeczeństwo ma interes w ochronie ich przed piractwem. Ponieważ większość ulotnych mediów obejmuje pewne aspekty wizualne, a także tekst, techniki antypirackie obecnie używane lub rozważane w przypadku innych

rodzajów danych mogą mieć zastosowanie. Takie techniki obejmują wcześniej omówione klucze sprzętowe, klucze oprogramowania, znaki wodne, szyfrowanie i zarządzanie prawami cyfrowymi. Częścią problemu przy wyborze i wdrażaniu rozwiązania jest brak istniejących standardów, które konkretnie dotyczą tej nowej dziedziny sztuki i nauki.

Klucze oprogramowania

Do zabezpieczania danych i sprzętu używane są różnego rodzaju klucze programowe. Klucz oprogramowania to zazwyczaj ciąg cyfr używany do celów identyfikacyjnych, aby umożliwić dostęp do sprzętu lub umożliwić autoryzowane drukowanie, przetwarzanie lub kopiowanie danych. Jak opisano wcześniej w dyskusji na temat kluczy sprzętowych, większości urządzeń sprzętowych do przeciwdziałania kopiowaniu towarzyszy oprogramowanie, które działa w parze ze sprzętem. Klucz programowy aktywuje lub dezaktywuje blokadę sprzętową. Gdy oprogramowanie działa idealnie, na ogół nie ma żadnych trudności. Jednak całe oprogramowanie może działać nieprawidłowo, a gdy tak się stanie, mogą wystąpić poważne problemy z uruchomieniem sprzętu. Dodatkowe problemy pojawiają się, gdy komputer zawierający klucz oprogramowania działa nieprawidłowo, a klucz oprogramowania nie może działać na komputerze zastępczym.

Kasety wideo a kopiarki

Znak wodny jest jedną z poważnie rozważanych technik ochrony kaset wideo i płyt DVD. W 1995 roku ASTC utworzyło Techniczną Grupę Roboczą ds. Ochrony Praw Autorskich, która wydzieliła specjalną podgrupę zajmującą się znakami wodnymi i kodowaniem danych osadzonych. Grupa posiada szeroką reprezentację, w tym przedstawicieli rynku komputerów PC, rynku komputerów Macintosh, MPAA, stowarzyszenia producentów elektroniki użytkowej (CEMA) oraz powiązanych producentów, techników i użytkowników. Ich zadaniem jest poszukiwanie technologii i usług, które mogą wykorzystywać ukryte wskazówki dotyczące danych jako sposób na powstrzymanie lub uniemożliwienie piractwa cyfrowego. Użycie ukrytego znaku wodnego, który można osadzić w treści, uniemożliwiłoby maszynom wykonywanie kopii lub zaalarmowało operatora, że kaseta wideo jest oznaczona, a nieautoryzowane kopie zostaną uznane za pirackie.

Kodowanie obszaru DVD

Cyfrowe wideo wymaga bardzo dużej przestrzeni dyskowej - zbyt dużej, aby pomieścić jedną płytę CD. Jednak dzięki zastosowaniu technik kompresji cyfrowy obraz wideo może zostać skompresowany do maksymalnej pojemności cyfrowej płyty wideo wynoszącej 17 gigabajtów. Do kodowania zawartości audio i wideo na DVD używane są dwa różne typy kompresji: kompresja ze stałą szybkością bitów (CBR) i ze zmienną szybkością bitów (VBR). Aby zapobiec piractwu zawartości DVD, wiele firm korzysta z szyfrowania. Skompresowane dane są enkapsulowane za pomocą algorytmu matematycznego, który można odszyfrować tylko za pomocą klucza deszyfrującego.

Wdrożenie

W przypadku krótszych programów CBR jest idealny. W oparciu o kodowanie MPEG-2, CBR kompresuje każdą klatkę audio i wideo o wartość wybraną przez użytkownika. Ten stopień kompresji jest następnie stosowany do całego programu. Korzystając z VBR, możliwe jest stworzenie bazy danych treści wideo na podstawie ilości zmian w każdej klatce lub scenie. Jest to szczególnie przydatne w programach o długim formacie. Aby skonstruować bazę danych, oprogramowanie kodujące wykonuje kilka przejść analitycznych głównego materiału filmowego, a następnie wykonuje ostatnią fazę digitalizacji. Z utworzonej bazy danych komputer może kodować wideo ze zmienną szybkością transmisji danych, umożliwiając wyższą szybkość transmisji dla scen z panoramowaniem, powiększaniem i szybkim

ruchem oraz dając sceny z niewielkim ruchem lub bez ruchu z niską szybkością transmisji danych. Dzięki znacznej kompresji obszarów o mniejszej szczegółowości, obszary o wyższych szczegółach mogą mieć więcej miejsca i zużywać mniej kompresji.

Znaki wodne

Znak wodny polega na osadzeniu jednego zestawu danych w większym zestawie danych. Wbudowany zestaw danych identyfikuje pochodzenie lub własność konkretnego dzieła, podobnie jak znak wodny na papierze. Używanie cyfrowych znaków wodnych może pomóc właścicielom praw autorskich w śledzeniu wykorzystania wszystkiego, co cyfrowe, w tym muzyki, filmów, zdjęć i klipartów. Cyfrowy znak wodny jest szeroko stosowany do ochrony obrazów. Na przykład fotografowie często publikują wersje swoich zdjęć w niskiej rozdzielczości (niskiej rozdzielczości) w publicznych witrynach internetowych i używają widocznych cyfrowych znaków wodnych, aby wyraźnie oznaczyć obrazy o niskiej rozdzielczości jako chronione prawem autorskim. Po uiszczeniu odpowiedniej opłaty klient otrzymuje wersję zdjęcia w wysokiej rozdzielczości, prawdopodobnie z usuniętymi co najmniej widocznymi znakami wodnymi. Stosowanie niewidocznych znaków wodnych w celu zapobiegania niewykrytemu udostępnianiu po zakupie treści cyfrowych jest bardziej kontrowersyjne i bardziej podatne na pytania o wiarygodność wykrywania; na przykład, ile wystąpi fałszywie pozytywnych i fałszywie negatywnych wyników? Do tego dochodzi kwestia przetrwania samego znaku, który przechodzi różne przekształcenia. Przemysł muzyczny flirtował z cyfrowymi znakami wodnymi w celu ochrony plików muzycznych, począwszy od 1998 roku, kiedy utworzono Secure Digital Media Initiative (SDMI), konsorcjum organizacji zajmujących się technologiami, bezpieczeństwem i muzyką. SDMI opracowało kilka schematów znakowania wodnego, aw 2000 r. zaoferowało nagrodę każdemu, kto potrafił złamać kod i usunąć znak wodny z utworu chronionego technologiami SDMI. Fundacja Electronic Frontier zwróciła się do społeczności internetowej o bojkot konkursu, podkreślając, że korzystanie z technologii DMAT (Digital Music Access Technology) oznaczałoby, że producenci i użytkownicy byliby zmuszeni do przyjęcia formatu DMAT w sprzęcie i generowałyby dodatkowe koszty dla producentów i konsumentów . Zespół naukowców pod kierownictwem profesora Princeton Eda Feltena był w stanie usunąć niewidzialne znaki wodne. Kiedy Felten próbował opublikować wyniki swojego procesu, adwokaci SDMI zagrozili, że pozwą go na mocy ustawy Digital Millennium Copyright Act (DMCA). SDMI nigdy nie złożył pozwu. ale sam Felten pozwał o orzeczenie deklaratywne w celu wyjaśnienia sprawy. Pozew Feltena został oddalony przez sędziego federalnego, ale nie wcześniej niż rząd i RIAA uzgodniły, że naukowcy nie powinni być karani na mocy ustawy DMCA za testowanie technologii w celu ochrony praw autorskich19. SDMI jest nieaktywne od 2001 roku.

ZARZĄDZANIE PRAWAMI CYFROWYMI

Uznając, że piractwo jest ogromnym problemem moralnym i finansowym, twórcy oprogramowania przyjęli i zmodyfikowali inny rodzaj systemu, który można zastosować do mediów drukowanych, audio, wideo i strumieniowych. Nazywany Digital Rights Management (DRM), system został pierwotnie opracowany w celu ochrony informacji zastrzeżonych i informacji wojskowych. Ideą systemu jest ochrona wszelkiego rodzaju intelektualnej zawartości cyfrowej przed każdym, kto by ją zabrał bez zgody dewelopera (ów) lub właścicieli. Duże firmy, takie jak Microsoft, Adobe i IBM, opracowują i wprowadzają na rynek systemy DRM, a dziesiątki mniejszych firm powstają.

Cel

Celem DRM jest ochrona wszystkich treści cyfrowych, które twórcy lub właściciele chcą chronić. DRM pozwala dystrybutorom treści elektronicznych na kontrolowanie dostępu do przeglądania tych treści. Treścią może być tekst, druk, muzyka lub obrazy. Zasadniczo systemy DRM wykorzystują formę niestandardowego szyfrowania. Gdy użytkownik końcowy kupuje prawa do oglądania, słuchania lub

drukowania, dostarczany jest indywidualny „klucz”. System działa na zasadach, co oznacza, że chociaż klucz jest dostarczany, zazwyczaj zawiera ograniczenia dotyczące kopiowania, drukowania i redystrybucji. Niestety nie ma zgody na rozwiązanie DRM. Brak standardów utrudnia firmom rozwijanie inicjatyw biznesowych online. Ponieważ jest tak wiele firm promujących własne niezgodne formy DRM, klienci będą musieli pobrać megabajty kodu dla każdej wersji. Utrzymanie, aktualizacja i zarządzanie wszystkimi tymi różnymi wersjami to poważny problem dla klientów. Wydaje się, że nie ma prostego rozwiązania; zamiast być kwestią technologii, jest to tak naprawdę kwestia biznesu i polityki.

Aplikacja

Zazwyczaj, gdy użytkownicy stają się potencjalnymi właścicielami praw cyfrowych, pobierają plik treści. Oprogramowanie DRM sprawdza tożsamość użytkowników, kontaktuje się z finansową izbą rozliczeniową w celu zorganizowania płatności, a następnie odszyfrowuje żądany plik i przypisuje użytkownikom klucz. Klucz służy do przyszłego dostępu do treści. Ponieważ system działa na zasadach, możliwe jest nałożenie ograniczeń. Jeden użytkownik może płacić tylko za przeglądanie materiałów, podczas gdy inny użytkownik może chcieć mieć uprawnienia do drukowania. Trzeci użytkownik może chcieć pobrać zawartość na swój własny komputer, a czwarty użytkownik może chcieć mieć uprawnienia do przeglądania przez określony czas. Czterech różnych autoryzowanych użytkowników korzystałoby zatem z tej samej treści, a każdy z nich płaciłby zgodnie z taryfą ustaloną przez dystrybutora treści. Podczas wszystkich transakcji każdy użytkownik potrzebowałby mechanizmu, który umożliwia bezpieczną transmisję i identyfikuje tego użytkownika oraz związany z nim poziom uprawnień dostępu. Chociaż takie podejście do publikowania może wydawać się dość proste, jest naprawdę dość złożone. Oprócz zapewniania różnym użytkownikom dostępu do materiałów zgodnie z ustalonymi zasadami i płacenia zgodnie z harmonogramem, dystrybutorzy treści muszą również obsługiwać zaplecza aplikacji. Każda osoba zaangażowana w tworzenie, produkcję i dystrybucję treści musi uczciwie zapłacić za korzystanie z treści. Płatności są szczególnie ważne, ponieważ coraz więcej dostawców treści digitalizuje materiały, które mogą wyświetlać lub drukować na żądanie. Wielu użytkowników będzie czytać książki online, ale niektóre fizyczne drukowanie na papierze będzie kontynuowane. Jednak wydawcy będą mogli drukować dokładnie te tomy, które są wymagane. Takie podejście zapewni spersonalizowane drukowanie (np. duże wydania), a także zaoszczędzi papierową i fizyczną przestrzeń magazynową.

Przykłady

Istnieje kilka różnych typów systemów DRM. Eksperci są zgodni, że najlepsze systemy DRM łączą w sobie zarówno sprzętowe, jak i programowe mechanizmy dostępu. Wraz z pojawieniem się eBooka, cyfrowego tabletu, modemów PDA, urządzeń dostępu do Internetu i coraz mniejszych laptopów, powiązanie praw dostępu bezpośrednio z nośnikami danych daje wydawcom i dystrybutorom kontrolę nad tym, gdzie i przez kogo są wykorzystywane treści. Wraz z uchwaleniem Ustawy o podpisach elektronicznych w handlu światowym i krajowym, określanym mianem E-Sign Bill oraz rosnącym wykorzystaniem podpisów cyfrowych, oryginalne dokumenty (np. prawne, medyczne lub finansowe) będą przechowywane cyfrowo. Prezydent Clinton podpisał ustawę o podpisie elektronicznym 30 czerwca 2000 r. w Sali Kongresowej w Filadelfii za pomocą ceremonialnego pióra i cyfrowej karty inteligentnej. Ustawa weszła w życie 1 października 2000 r. E-Sign Bill nadaje podpisowi online ten sam status prawny, co podpis wyryty na papierze i sprawia, że dokument cyfrowy jest oryginałem. Każdy wydruk będzie uważany za kopię, więc możliwość cyfrowego przeglądania dokumentów i filmów (np. testamentów życia) faktycznie da widzowi dostęp do oryginału. Ostatecznie zapisy dotyczące leczenia i dokumenty dotyczące badań mogą być całkowicie cyfrowe i mogą wymagać przesłania i przeglądania w formie cyfrowej. Kiedy stanie się to normą, a nie wyjątkiem, ścisłe przestrzeganie DRM w celu

zachowania prywatności, a także zapewnienia rekompensaty, będzie miało pierwszorzędne znaczenie. Ponadto takie systemy ochrony treści zapobiegną nieautoryzowanym modyfikacjom danych cyfrowych, które w przeciwnym razie przyczyniłyby się do oszustw. Na przykład IBM wypuścił technologię antypiracką o nazwie Electronic Media Management System, która umożliwia pobieranie utworów muzycznych, ale kontroluje liczbę kopii, które można wykonać, lub pozwala na wstawienie ograniczenia długości kopii. W ten sposób można było pobrać minutę muzyki, aby dać słuchaczowi posmak, ale nie miała szansy na pirackie całego utworu muzycznego. Aby uzyskać cały utwór, użytkownik musiałby uiścić opłatę. Firma Microsoft dystrybuuje bezpłatne oprogramowanie, które osadza metatagi w każdym pliku audio. Metatagi odnoszą się z powrotem do centralnego serwera, na którym przechowywane są reguły biznesowe. Takie podejście wymaga oznaczania materiału w trakcie jego tworzenia; w przeciwnym razie, jeśli zostanie wydany bez osadzonych znaczników, może zostać nielegalnie skopiowany. Duże firmy, takie jak Xerox, Microsoft, IBM i Adobe, mocno zaangażowały się w produkcję i używanie tego oprogramowania w latach 90., a wiele mniejszych firm otworzyło sklep. Podobnie jak w przypadku innych wprowadzanych na rynek nowych technologii, w końcu wiele małych firm zakończyło działalność lub zostało kupionych przez większe firmy. Niektóre małe firmy, takie jak ContentGuard, w chwili pisania tego tekstu nadal istnieją niezależnie.

TECHNOLOGIE WZMACNIAJĄCE PRYWATNOŚĆ

Chociaż DRM może wydawać się dobrym rozwiązaniem problemu piractwa, dysydenci uważają, że DRM i inne środki antypirackie dają producentom i dystrybutorom zbyt dużą kontrolę. Uzasadnienie jest takie, że nadmiernie restrykcyjne zarządzanie prawami może podważać prawa konsumentów i naukowców do dozwolonego użytku. Częściowo w wyniku tych sprzecznych punktów widzenia wielu konsumentów coraz częściej korzysta z technologii wzmacniających prywatność (PET), szerokiego terminu określającego szereg technologii zaprojektowanych w celu ukrywania tożsamości i działań poszczególnych użytkowników i komputerów, gdy ich ruch przechodzi przez Internet.

Sieciowy serwer proxy

Jedna szeroka klasa taktyk i narzędzi stosowanych w celu zwiększenia prywatności opiera się na koncepcji sieciowego serwera proxy. W swojej najbardziej ogólnej formie serwer proxy przyjmuje żądanie połączenia sieciowego od klienta i przekierowuje je do ostatecznego miejsca docelowego, zmieniając nagłówki adresu, aby wyglądało na to, że oryginalne żądanie pochodzi od samego serwera proxy. Gdy serwer docelowy odpowie, serwer proxy zwraca wyniki do żądającego klienta. Serwery proxy są od dawna używane w organizacjach, zarówno do ochrony użytkowników wewnętrznych, gdy wysyłają żądania do niezaufanych sieci, jak i do śledzenia, a czasem blokowania dostępu do niepożądanej zawartości. Więcej informacji na temat korzystania z serwerów proxy w filtrowaniu i monitorowaniu treści internetowych znajduje się w rozdziale 31 tego podręcznika. Ostatnio, poza granicami sieci korporacyjnych, zastosowano proxy, aby umożliwić anonimowe połączenia przez Internet. Te tak zwane anonimizujące serwery proxy czasami używają szyfrowania, aby ukryć ruch w tranzycie, a tym samym zapewnić ochronę przed analizą ruchu. Anonimizujące serwery proxy stanowią poważne zagrożenie dla organizacji, które chcą (lub są wymagane przez prawo) monitorować i blokować użytkownikom dostęp do niektórych rodzajów informacji. Bardziej zaawansowane wersje tej koncepcji wykorzystują wiele routerów w celu ukrycia ścieżki, jaką przechodzi żądanie przez sieć publiczną. Ogólnie rzecz biorąc, są one znane jako sieci mieszające. Jednym z przykładów opisanych już w 1981 r. jest Chaum Mix.22 Ostatnio koncepcja znana jako routing cebulowy stała się popularna w swoim wcieleniu jako Tor (router cebulowy), który wykorzystuje zagnieżdżone warstwy szyfrowania ruchu, gdy sesja przechodzi od jednego routera do Następny.

Ukryte systemy operacyjne

Zamiast polegać na technologiach sieciowych, niektórzy użytkownicy decydują się na prywatność swoich działań w sieci, używając ukrytych systemów operacyjnych. Powszechne są dwa podstawowe podejścia: maszyna wirtualna i system startowy. Maszyna wirtualna to system działający w innym systemie operacyjnym. Od dawna używane ze względu na kompatybilność między platformami i możliwość uruchamiania wielu systemów na jednej platformie sprzętowej, maszyny wirtualne, takie jak wirtualna maszyna Java, VirtualPC i VMware, są również używane do ukrywania aktywności przed tymi, którzy by się na to nie zgodzili (administratorami systemu , rodzice, organy ścigania itp.), ponieważ działania maszyny wirtualnej mogą być niewidoczne dla maszyny hosta. Podejście systemu rozruchowego przechowuje jednak cały system operacyjny na jakimś nośniku rozruchowym, takim jak płyta CD lub urządzenie USB. Jeśli komputer może uruchomić się z takiego nośnika i zapisać pobraną zawartość na urządzeniu peryferyjnym, a nie na dysku twardym systemu operacyjnego hosta, przy następnym uruchomieniu hosta nie pozostanie żaden zapis użycia.

POLITYCZNY I TECHNICZNY SPRZECIW WOBEC DRM.

Wokalni przeciwnicy DRM zorganizowali się za pomocą sieci, aby wywierać presję na dostawców korzystających z tych technik; hakerzy kryminalni i inni opracowali i rozpowszechnili oprogramowanie do wyłączania DRM.

Opozycja polityczna.

Electronic Frontier Foundation (EFF) to powszechnie szanowana organizacja, która opisuje się następująco:

Od Internetu po iPoda, technologie zmieniają nasze społeczeństwo i wzmacniają nas jako mówców, obywateli, twórców i konsumentów. Kiedy nasze wolności w świecie sieciowym zostają zaatakowane, Electronic Frontier Foundation (EFF) jest pierwszą linią obrony. EFF wkroczyła na nowy teren, kiedy została założona w 1990 roku – na długo przed tym, zanim Internet znalazł się na radarze większości ludzi – i nadal stawia czoło najnowocześniejszym problemom w obronie wolności słowa, prywatności, innowacji i praw konsumentów dzisiaj. Od samego początku EFF bronił interesu publicznego w każdej krytycznej bitwie mającej wpływ na prawa cyfrowe. Łącząc doświadczenie prawników, analityków politycznych, aktywistów i technologów, EFF odnosi znaczące zwycięstwa w imieniu konsumentów i ogółu społeczeństwa. EFF walczy o wolność przede wszystkim w sądach, wnosząc i broniąc procesów sądowych, nawet jeśli oznacza to walkę z rządem USA lub dużymi korporacjami. Mobilizując ponad 140 000 zaniepokojonych obywateli za pośrednictwem naszego Centrum Akcji, EFF odpiera złe ustawodawstwo. Oprócz doradzania decydentom, EFF edukuje prasę i opinię publiczną25

EFF niezłomnie argumentuje przeciwko DRM:

Technologie zarządzania prawami cyfrowymi (DRM) próbują kontrolować, co możesz, a czego nie możesz zrobić z zakupionymi mediami i sprzętem.

* Kupiłeś e-booka od Amazon, ale nie możesz go przeczytać na wybranym czytniku e-booków? To jest DRM.

* Kupiłeś DVD lub Blu-Ray, ale nie możesz skopiować wideo na przenośny odtwarzacz multimedialny? To jest DRM.

* Kupiłeś grę wideo, ale nie możesz w nią dziś zagrać, ponieważ „serwery uwierzytelniania" producenta są offline? To jest DRM.

* Kupiłeś smartfon, ale nie możesz korzystać z aplikacji lub usługodawcy, którego chcesz na nim? To jest DRM.

Korporacje twierdzą, że DRM jest niezbędny do zwalczania naruszeń praw autorskich w Internecie i ochrony konsumentów przed wirusami. Ale nie ma dowodów na to, że DRM pomaga w walce z którymkolwiek z nich. Zamiast tego DRM pomaga dużym firmom tłumić innowacyjność i konkurencję, ułatwiając wyeliminowanie „nieautoryzowanych" zastosowań mediów i technologii.

DRM rozprzestrzenił się dzięki ustawie Digital Millennium Copyright Act z 1998 r. (DMCA), która usiłowała zakazać wszelkich prób ominięcia DRM. Fani nie powinni być traktowani jak przestępcy, a firmy nie powinny otrzymywać automatycznego weta w sprawie wyboru użytkownika i innowacji. EFF prowadził wysiłki na rzecz uwolnienia iPhone'a i innych smartfonów, pracuje nad odkryciem i wyjaśnieniem ograniczeń dotyczących nowego sprzętu i oprogramowania, walczy o prawo do kopiowania płyt DVD i pozwał Sony-BMG za „rootkit" CD schemat ochrony przed kopiowaniem.26

Fundacja Wolnego Oprogramowania stworzyła kampanię Defective by Design w maju 2006 roku i zorganizowała pierwszy Międzynarodowy Dzień Walki z DRM. Ósme wydarzenie miało miejsce 3 maja 2013 roku. Ostatnia kampania to Stop DRM w HTML5, która jest opisana w następujący sposób:

Konsorcjum World Wide Web (W3C) rozważa propozycję wplecenia Zarządzania Ograniczeniami Cyfrowymi (DRM) w HTML5 – innymi słowy, w samą tkankę sieci. Miliony internautów zebrały się, by pokonać SOPA/PIPA, ale teraz potentaci Big Media korzystają z kanałów pozarządowych, próbując przemycić cyfrowe ograniczenia do każdej interakcji, jaką mamy w sieci. Giganci tacy jak Netflix, Google, Microsoft i BBC stoją za tą katastrofalną propozycją, która stoi w sprzeczności z misją W3C polegającą na „doprowadzeniu World Wide Web do pełnego potencjału".

Wadliwy projekt to

…[A] partycypacyjna i oddolna kampania ujawniająca urządzenia i media obciążone DRM takimi, jakimi naprawdę są: Wadliwymi z założenia. Wspólnie pracujemy nad wyeliminowaniem DRM jako zagrożenia dla innowacji w mediach, prywatności czytelników i wolności użytkowników komputerów. Nasze działania obejmują identyfikowanie i ukierunkowanie wadliwych produktów, naciskanie na sprzedawców mediów i producentów sprzętu, aby przestali wspierać DRM, ujawnianie ogromnej koncentracji władzy nad mediami stworzonymi przez DRM oraz podnoszenie świadomości na temat DRM w bibliotekach, szkołach i osobach na całym świecie.

Zwolennicy DRM w branży nazywają to „zarządzaniem prawami cyfrowymi", tak jakby to oni byli ostatecznym autorytetem przyznającym nam nasze prawa, jakby to oni powinni mieć pełną i całkowitą kontrolę nad tym, w jaki sposób korzystamy z naszych mediów i wchodzimy z nimi w interakcję. To, co naprawdę robią, to zarządzanie ograniczeniami, które nakładają na nasze media i urządzenia, nad którymi normalnie mielibyśmy kontrolę w przypadku braku DRM. Powinniśmy być właścicielami naszych mediów, a nie być na łasce firm medialnych. Z tego powodu nazywamy to „Zarządzaniem ograniczeniami cyfrowymi"

Defective by Design twierdzi, że DRM jest rażąco nachalny i niesprawiedliwy:

Nowa usługa pobierania filmów Amazon nazywa się Unbox i określa, co oznacza DRM. Umowa użytkownika wymaga, abyś zezwolił oprogramowaniu Unbox DRM na monitorowanie Twojego dysku twardego i zgłaszanie aktywności do Amazon. Raporty te zawierałyby zatem listę: całego zainstalowanego oprogramowania; całą muzykę i wideo, które masz; wszystkie interakcje komputera

z innymi urządzeniami. Zrzekasz się swojej wolności do takiego stopnia, że będziesz w stanie odzyskać kontrolę jedynie poprzez usunięcie oprogramowania. Ale jeśli usuniesz oprogramowanie, usuniesz również wszystkie swoje filmy wraz z nim. Jesteś ograniczony nawet geograficznie i tracisz swoje filmy, jeśli kiedykolwiek wyprowadzisz się z USA. Oczywiście musisz zgodzić się, że mogą zmienić te warunki w dowolnym momencie. Zaktualizowana umowa użytkownika Microsoft Windows Media Player 11 (WMP11) zawiera podobny zestaw warunków.

Zatrzymaj DRM teraz! argumentuje na tych samych zasadach, co Defective by Design: DRM istnieje na wyłączną korzyść producentów i dostawców treści. Firmy takie jak Disney, Sony i Lion's Gate twierdzą, że DRM jest potrzebny, aby uniemożliwić ludziom piractwo muzyki, filmów i innych dzieł w sieciach P2P lub w inny sposób. Nie powiedzą ci, że naprawdę próbują kontrolować kto, co, kiedy, gdzie i jak uzyskujesz dostęp do swojej muzyki i filmów. Na przykład, kupując utwór w sklepie muzycznym Apple iTunes, kupujesz utwór, który może być odtwarzany tylko przez aplikacje multimedialne obsługujące QuickTime lub Apple iPod. Załóżmy, że w przyszłym roku chcesz kupić nowy przenośny odtwarzacz muzyki? Zamiast mieć wybór, musisz teraz kupić innego iPoda, jeśli chcesz odtwarzać muzykę, którą już kupiłeś.

Techniczne środki zaradcze

Inżynieria odwrotna.

Inżynieria wsteczna umożliwia programiście pracę wstecz od gotowego programu lub produktu. Klucze szyfrowania można wyodrębnić za pomocą oprogramowania do odtwarzania inżynierii wstecznej. Inżynieria wsteczna może obejść większość rozwiązań antypirackich. W rezultacie producenci oprogramowania i sprzętu antypirackiego zdecydowanie sprzeciwiają się zezwalaniu na inżynierię wsteczną. Ustawa DMCA zezwala na inżynierię wsteczną, ale postanowienia DMCA nie miały na celu umożliwienia obchodzenia technicznych środków ochrony (TMP) w celu uzyskania nieautoryzowanego dostępu do lub wykonania nieautoryzowanych kopii dzieł chronionych prawem autorskim.

Opublikowane ataki

Najbardziej znaczący atak na klucz oprogramowania miał miejsce, gdy licencjobiorca CSS zaniedbał zaszyfrowanie klucza odszyfrowywania. Uzyskując klucz za pomocą inżynierii wstecznej XingDVD od Xing Technologies, hakerzy byli wtedy w stanie odgadnąć wiele innych kluczy. To pozostawiło hakerom kolekcję kluczy deszyfrujących; nawet jeśli klucz XingDVD został usunięty, nadal mogli kopiować płyty DVD za pomocą innych kluczy. Wykorzystując wyniki tego kompromisu, grupa ludzi, w tym norweski nastolatek Jon Lech Johansen, opracowała program o nazwie DeCSS do odszyfrowywania płyt DVD zaszyfrowanych CSS i odtwarzania ich na maszynach z systemem Linux. Różne grupy, w tym DVD CCA, pozwały Johansena za narzędzia do publikowania w celu obalania ochrony praw autorskich. Johansen był dwukrotnie uniewinniany w sądach norweskich. W 2007 r. wszystkie pozostałe pozwy przeciwko niemu zostały wycofane, a wiele programów, takich jak DeCSS, jest dostępnych bezpłatnie w Internecie. W następnej sekcji omówiono powszechną dostępność narzędzi do łamania DRM.

Narzędzia do łamania DRM

W sieci jest mnóstwo oprogramowania do łamania kontroli DRM. Istnieją metody obejścia ograniczeń dotyczących:

*Kopiowanie CD

* Kopiowanie DVD

* Kopiowanie Blu-ray

* Kopiowanie z iTunes

* Wyodrębnianie treści PDF

* Aktywacja oprogramowania

PODSTAWOWE PROBLEMY

Wielu ekspertów zwróciło uwagę, że wszystkie opisane metody zapobiegania nielegalnemu kopiowaniu materiałów cyfrowych mają zasadnicze wady. Bruce Schneier, szanowany kryptograf, wielokrotnie wyjaśniał, że wszystkie informacje cyfrowe muszą zostać przekonwertowane do postaci zwykłego tekstu (niezaszyfrowanej), zanim zostaną wyświetlone lub wykorzystane w inny sposób. Schneier nazywa to „piętą achillesową wszystkich systemów ochrony treści opartych na szyfrowaniu". Ponieważ wersja jawnego tekstu musi znajdować się gdzieś w pamięci ulotnej lub nieulotnej przynajmniej przez pewien czas, aby była użyteczna, teoretycznie możliwe jest uzyskanie kopii wersji jawnego tekstu niezależnie od złożoności metod, które pierwotnie ukrywały lub w inny sposób ograniczały dostęp do danych. Na przykład, jeśli na monitorze ma być wyświetlany film DVD wykorzystujący złożone kodowanie regionalne, w pewnym momencie sprzęt i oprogramowanie, które dekodowały DVD, muszą wysłać ten strumień danych do sterownika monitora. Dekodowany strumień danych jest podatny na przechwycenie. Modyfikując procedury niskiego poziomu w sterowniku monitora, można przekierować kopię nieprzetworzonego strumienia danych do urządzenia pamięci masowej w celu nieautoryzowanego odtwarzania lub odtwarzania. Podobnie można opracować system zapobiegający bezpośredniemu drukowaniu na drukarce więcej niż jednej kopii dokumentu; jednak o ile system nie uniemożliwia wykonywania zrzutów ekranu, użytkownik może obejść ograniczenia, kopiując ekran jako obraz bitowy i przechowując ten obraz do późniejszego, nieautoryzowanego użycia. Chociaż urządzenia sprzętowe, takie jak dedykowane odtwarzacze DVD lub CD, mogą przez pewien czas skutecznie zakłócać piractwo, problem nasila się w obecnych popularnych systemach operacyjnych, które nie mają jądra bezpieczeństwa, a tym samym umożliwiają dowolnym procesom dostęp do dowolnego regionu pamięci bez względu na poziom bezpieczeństwa

STRESZCZENIE

Piractwo to szybko narastający problem społeczny, który dotyka wielu ludzi i branż. Chociaż producenci mogą ponieść największe straty finansowe, ma to znaczny wpływ na konsumentów. Pirackie kopie są na ogół gorszej jakości i czasami są wadliwe. Jeśli coś pójdzie nie tak, pirackie kopie, które są nielegalne, nie są obsługiwane. Dodatkowo straty finansowe producentów spowodowane pirackimi kopiami mogą podnieść koszt legalnych kopii. Detaliści i dystrybutorzy również cierpią z powodu utraty sprzedaży piratom. Nielegalne kopie są zazwyczaj sprzedawane taniej niż legalne kopie, więc detaliści i dystrybutorzy nie mogą konkurować ceną. Talenty twórcze, niezależnie od tego, czy są to twórcy oprogramowania, pisarze, muzycy, artyści czy wykonawcy, a także wszyscy ludzie, którzy pomogli stworzyć książkę, czasopismo, płytę, występ, malarstwo, koncert lub inne media, są oszukiwani z tantiem przez piratów. Często, ze względu na ilość czasu i wysiłku potrzebnego do stworzenia produktu końcowego, twórcy są uzależnieni od opłat licencyjnych za swoje utrzymanie. Ponadto słaba jakość skradzionych koncepcji może nieodwracalnie zaszkodzić reputacji talentu twórczego. Wydawcy, wytwórnie płytowe, handlarze dziełami sztuki oraz inne osoby i firmy, które inwestują umiejętności artystyczne i techniczne wraz z pieniędzmi i wysiłkiem, aby stworzyć oryginalne dzieło, również tracą dochody, gdy ta praca jest piracka. Ze względu na wydatki już poniesione na stworzenie oryginalnego produktu, firmy często muszą rekompensować swoje straty, podnosząc ceny dla konsumenta. Ze względu na wyrafinowanie systemów i zwiększone wykorzystanie Internetu piractwo stało się bardziej

rozpowszechnione i ma jeszcze większy wpływ finansowy na całym świecie. Wiele różnych rodzajów systemów i technik antypirackich zostało opracowanych i wdrożonych w celu ograniczenia coraz większej liczby przypadków piractwa. Wadą wszystkich systemów jest brak standardów stosowanych do oprogramowania, audio, wideo i innych mediów. Jednym z najbardziej obiecujących systemów antypirackich jest zarządzanie prawami cyfrowymi. Jednak nawet systemy evenDRM nie są jeszcze ustandaryzowane, co powoduje jeszcze większe zamieszanie co do tego, co jest najlepsze i czego użyć. Branża medialna wciąż zastanawia się, które rozwiązanie DRM lubi najbardziej, czy też lubi DRMat wszystkie. W 2007 roku Steve Jobs z Apple ogłosił, że duża część katalogu piosenek EMI będzie dostępna do pobrania bez DRM z iTunes Music Store, w cenie tylko 0,30 USD za utwór niż standardowa 0,99 USD. Wcześniej pobrane utwory z DRM będą mogły zostać uaktualnione do wersji wolnej od DRM za różnicę w dwóch cenach. Ten ruch jest echem ostatnich komentarzy Jobsa zachęcających przemysł muzyczny do odejści od DRM. Pomimo działań Apple, niektórzy konsumenci i organizacje zajmujące się ochroną prywatności nadal walczą z tym, co postrzegają jako poważne zagrożenia dla prywatności osób, w ramach rodzących się wysiłków DRM. Korzystanie z serwerów proxy i ukrytych systemów operacyjnych utrudnia wykrywanie niewłaściwego wykorzystania treści, a tym bardziej zapobieganie lub ściganie ich. Ponieważ równowaga między producentami treści a konsumentami wypracowuje się sama, wydaje się prawdopodobne, że o wiele więcej technologii pojawi się i zniknie, a DRM może być zwiastunem tego, co nadejdzie lub niefortunnym wyborem na drodze do odważnego, nowego modelu biznesowego dla przemysł medialny.