Mirosław Roman
Wydział Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego.

Piractwo kontra copyright: czyli o zagrożeniach związanych z łamaniem praw autorskich.

We współczesnym świecie, w dobie powszechnego dostępu do Internetu i digitalizacji danych, poważny problem stanowi nielegalne wykorzystywanie i rozpowszechnianie cudzej własności intelektualnej, najczęściej bez wiedzy i zgody autorów. Łamanie praw autorskich, powszechnie zwane dziś „piractwem" obecnie dotyczy głównie sfery multimedialnych rozrywek elektronicznych, tj. filmy, muzyka, gry elektroniczne, oraz wirtualnych narzędzi środowiska pracy, tj. systemy operacyjne, pakiety biurowe, zaawansowane programy użytkowe, bez których trudno sobie wyobrazić dzisiejszy świat. Moje rozważania będę opierał głównie o wyżej wymienione przykłady produktów.

Co przyczyniło się do rozwoju piractwa na taką skalę, jaką dziś doświadczamy i jakie są związane z tym zagrożenia? Częściowo, z pewnością jest nim powszechny dostęp do Internetu, który umożliwia szybką i praktycznie bezproblemową wymianę wszelkiego rodzaju danych pomiędzy użytkownikami. Jednak moim zdaniem najlepszą odpowiedzią na pierwszą część pytania jest znane przysłowie: „*Jeśli nie wiadomo o co chodzi, to chodzi o pieniądze*". Jak wiemy, światem rządzi pieniądz i to on jest w znacznej mierze wyznacznikiem kierunku rozwoju naszej cywilizacji. Obecne firmy dążą do maksymalizacji zysków z sprzedaży swoich produktów, zaś nabywcy – konsumenci tych produktów, do minimalizacji kosztów związanych z użytkowaniem owych produktów. Głównym czynnikiem napędzającym łamanie praw autorskich, jest duża rozbieżność pomiędzy możliwościami finansowymi potencjalnego konsumenta, do opłat za użytkowanie produktów jakie życzą sobie producenci.

Aktualnie za najbardziej rozpowszechniony oryginalny system operacyjny, czy pakiet biurowy w Polsce, zapłacimy od kilkuset do kilku tysięcy złotych, co często przekracza możliwości finansowe przeciętnego Kowalskiego. Nic zatem dziwnego, że ludzie szukają innych sposobów na pozyskiwanie tychże produktów, bez których trudno jest się odnaleźć w obecnym świecie. Najłatwiejszym i najczęstszym sposobem jest pobranie takich plików z Internetu, udostępnianych przez piratów (i nie tylko) wykorzystując do tego jakże dziś popularne sieci p2p, p2m czy coraz popularniejsze sieci bit torrent. Istnieje co prawda alternatywne oprogramowanie tzw. Open source lub free software, oparte o licencje GNU czy darmowe licencje typu freeware, które często dorównują komercjalnym odpowiednikom, a niejednokrotnie nawet je przewyższają pod względem jakości. Jednak wciąż duża grupa ludzi nie korzysta z nich, w większości przez niewiedze o istnieniu takich alternatyw, lub z niechęci do nauki czegoś nowego, czegoś czego wcześniej nie poznali, lub też często zakładając że płatne oprogramowanie musi być lepsze od darmowego.

Zagrożenia wynikające z takiego sposobu postępowania dotyczą zarówno uczciwych konsumentów, jak i producentów tychże produktów i mogą one dotyczyć sfery finansowej czy prywatności. Prosty przykład ukazujący zależności pomiędzy piractwem a ochroną własności intelektualnej i związanych z tym konsekwencji. Za określone filmy umieszczanych na płytach Blu-Ray czy HD-DVD oraz gry elektroniczne średnio trzeba zapłacić od kilkudziesięciu do kilkuset złotych. Cześć potencjalnych nabywców zdecyduje się na zakup, część nie. Ta druga grupa, dążąc do redukcji kosztów, stara się zdobyć kopie z innego, nielegalnego źródła, tym samym traci na tym autor tych produktów, gdyż wyprodukowanie i zatrudnienie osób zaangażowanych w powstawanie danego produktu kosztuje**.** Im większa skala piractwa, tym większe straty ponosi producent, który z kolei, aby utrzymać poziom produkcji na obecnym etapie i nie chcąc tracić przy tym, podwyższa ceny za swoje produkty. Taki zabieg znów prowadzi do zwiększenia liczebności osób, których nie stać na zakup oryginalnego produktu i sięgających do źródeł nielegalnych. To po raz kolejny prowadzi do

strat poniesionych przez producentów , którzy starając się ograniczyć taką sytuację, coraz więcej nakładów finansowych przeznaczają na bardziej zaawansowane systemy zabezpieczeń przed kopiowaniem i użytkowaniem nielegalnych kopii, co znów prowadzi do wzrostu cen, gdyż więcej pieniędzy trzeba wyłożyć na produkcję i tak koło się zamyka. Konsekwencje takiej sytuacji mogą być przeróżne: producenci starając się uchronić przed ciągłymi stratami finansowymi tnąc koszty, mogą oni redukować liczbę zatrudnionych pracowników, co przekłada się na jakość produktów, a to z kolei na ich popyt i mniejsze zainteresowanie nimi, co prowadzi zmiany wizerunku firmy i dalszego spadku jej popularności i przychodów.

Część sprzętowo-programowych zabezpieczeń wprowadzonych do produktu przez producentów lub dystrybutorów filmów, oprogramowania prowadzi do innych zagrożeń związanych z ochroną prywatnych danych a także wygody użytkowania produktu przez uczciwych użytkowników. Jednym z takich zabezpieczeń jest DRM (Digital Rights Menegment). Stosowane są często nie tylko do ochrony praw autorskich, ale również do bezprawnego ograniczenia praw konsumenckich, np. przez uniemożliwienie wykonywania prywatnych kopii zakupionych utworów, czy tak jak CSS (Content Scramble System) utrudnienie korzystania z utworów w określonych rejonach geograficznych lub uniemożliwienie przewinięcia reklam poprzedzających film na płytach DVD.

Jednym z najbardziej znanych wydarzeń z udziałem tego rodzaju zabezpieczeń, była sprawa płyt CD z muzyką wydawanych przez Sony, które podczas pierwszego odtworzenia instalowały w systemie Windows bez wiedzy użytkownika oprogramowanie typu rootkit, które znacząco ingerowały w system, jednocześnie obniżając jego wydajność i wywołujące błędy systemowe, a nawet wysyłając informacje dotyczące zainstalowanego oprogramowania i posiadanego systemu operacyjnego do Sony. Sprawa ta zakończyła się serią procesów, także z urzędu oraz wieloma ugodami sądowymi na niekorzyść firmy.

Inną odmianą DRM, jest niedawno wypuszczona modyfikacja stworzona przez Ubisoft, kontrolująca legalność nabytej gry. Pierwszymi produktami zaopatrzonymi w ten system były gry Assasins Creed 2 i Silent Hunter V. Zabezpieczenie te nie tylko sprawdza legalność klucza licencyjnego, ale również wymaga od użytkownika posiadania konta na serwerze Ubi.com, oraz stałego podłączenia do Internetu. Innymi słowy, konsument kupujący oryginalny produkt musi być ciągle podpięty do sieci, a nawet najmniejsze przerwanie sygnału, powodowało blokadę gry do czasu ponownego nawiązania połączenia z serwerami Ubisoftu. Zabezpieczenie te było jednak totalną klapą, przynajmniej w przypadku drugiego tytułu, gdyż crackerzy złamali je w mniej jak 24 godziny, w wyniku czego piraci mogli spokojnie i bezproblemowo grać bez konieczności stałego podłączenia do Internetu**,** podczas gdy uczciwi nabywcy borykali się z ciągłymi problemami i blokadami gry w związku z przeciążeniem serwerów ubi.com czy chwilowymi przerwami na łączu internetowym. Ostatecznie wyszło to producentowi na złe, gdyż nie dość że wydali duże ilości pieniędzy na opracowanie tej technologii to jeszcze stracili w oczach uczciwych klientów, gdyż ci woleli zaopatrzyć się w „scrackowaną" wersje gry, nie tworzących tyle problemów co oryginał, co znów doprowadziło do zmniejszenia przychodów Ubisoftu**.** Efektem tego stanu rzeczy jest fakt, że zabezpieczenie zamiast przeszkadzać piratom, przeszkadza legalnym użytkownikom.

Innym sposobem radzenia sobie z nielegalnym rozpowszechnianiem np. oprogramowania jest wprowadzenie przez koncerny zniżki na konkretne produkty lub specjalnie dostosowanych pakietów oprogramowania dla firm, instytucji państwowych, lub uczelni. Do pewnego stopnia takie rozwiązanie jest skuteczne. Jednak do tej pory w większości firmy i koncerny z branży IT i nie tylko, były zdane tylko na siebie w walce z piractwem, ew. wspierani byli przez odpowiednie stowarzyszenia zajmujące się ochrona praw autorskich branży audio-video takie jak RIAA czy MPAA. Dziś jednak zauważamy coraz większe zainteresowanie tym zjawiskiem przez rządy konkretnych krajów, które coraz częściej wprowadzają nowe przepisy i prawa dotyczące ochrony praw autorskich. Niektóre kraje, tj. jak Wielka Brytania czy Francja w krótkim czasie bardzo zaostrzyły swoje przepisy i regulacje,

wprowadzając m.in. prawo trzech ostrzeżeń w swoich krajach. Polega ono na tym, aby każdy obywatel kraju, posiadający dostęp do Internetu, był kontrolowany pod względem pobieranych z Internetu treści i jeżeli świadomie bądź nieświadomie pobiera z Internetu nielegalne kopie oprogramowania, filmów, muzyki, gier, itp. odebrał najpierw ostrzeżenie o niezgodnym z prawem postępowaniem. Jeżeli po trzecim takim ostrzeżeniu ów użytkownik dalej łamie w ten sposób prawo, zostaje pozbawiony dostępu do Internetu na określony czas i nakładana jest na niego kara pieniężna adekwatna do skali popełnionego wykroczenia. W związku z tym istnieją obawy o prywatność osób i ich wszelkich działań w Internecie.

Podsumowując, uważam iż obecna polityka prowadzona przez większość firm i koncernów w celu zredukowania zjawiska piractwa jest bardzo nieefektywna, lub też raczej źle przemyślana. Moim zdaniem większe korzyści odniesiono by, zarówno po stronie producentów jak i konsumentów, gdyby producenci zamiast podwyższać ceny w celu kompensacji strat poniesionych przez nielegalne dystrybucje, obniżyli by je nieznacznie (m.in. przez zamknięcie projektów opracowywania skomplikowanych zabezpieczeń i częściowo zmniejszenie chwilowych przychodów). Ludzie chętniej by kupowali oryginalne produkty gdyby były tańsze, nie sprawiały problemów z użytkowaniem, i były pozbawiane często frustrujących zabezpieczeń które np. uniemożliwiają wykonanie prywatnej kopii zapasowej. Na początku oczywiście dystrybutorzy i producenci musieli by się pogodzić z mniejszymi przychodami, ale z drugiej strony takie działania prawdopodobnie doprowadziły by do wzrostu liczby użytkowników kupujących legalny produkt, co w dłuższym przedziale czasu mogło by owocować zwiększeniem przychodów producentów, niż gdyby dalej zabezpieczali swoje produkty windując ceny w górę, lub też powinni skierować się ku dystrybucji typu opensource, czerpiąc zyski z reklam czy wsparcia technicznego jak np. Canonical. Takie rozwiązania były by duże lepsze dla wszystkich i w dużym stopniu ograniczyłoby piractwo i związanych z nim zagrożeń.