

# Analiza kosztów systemu ochrony treści Windows Vista

(cc) Peter Gutmann ([wersja oryginalna](#))

Tłumaczenie pochodzi ze strony: [bytowisko](#)

Ostatnia aktualizacja 30 styczeń 2007 (na podstawie wersji oryginalnej z 27.01.2007)

Uwaga do czytelników: reakcja na coś, co miało być tylko krótkim technicznym postem na listę dyskusyjną poświęconą bezpieczeństwu przeszła moje najśmielsze oczekiwania. W tej chwili jestem pogrzebany pod stosem listów dotyczących Visty, proszę więc o cierpliwość w oczekiwaniu na moją odpowiedź. Z góry też przepraszam jeżeli nie zdołam odpowiedzieć na wszystkie maile.

## Podsumowanie

Dzięki poważnym - w stosunku do Windows XP - modyfikacjom kluczowych elementów systemu, Windows Vista zapewnia ochronę tzw. "treściom kwalifikowanym" - tym mianem określa się obraz wysokiej rozdzielczości zawarty na płytach Blu-Ray i -DVD. Jak wykaże, taka ochrona odbija się w znacznym stopniu na wydajności systemu, jego stabilności, dodatkowych kosztach pomocy technicznej oraz cenach sprzętu i oprogramowania. Te niepożądane przez konsumentów objawy dotyczą jednak nie tylko na najnowszego systemu Microsoftu ale również całego przemysłu komputerowego, ponieważ skutki stosowania tak restrykcyjnych ograniczeń dotkną cały sprzęt i oprogramowanie, które kiedykolwiek ma zadziałać z Vistą, choć faktycznie nie będzie współdziałać z tym systemem (na przykład sprzęt używany z [komputerami Macintosh](#) czy systemem [Linux](#)). Celem tego dokumentu jest analiza kosztów związanych z zastosowanym przez [Microsoft](#) systemem ochrony treści oraz wpływem, jaki wywrze on na cały przemysł komputerowy.

## Podsumowanie podsumowania

Specyfikacja systemu ochrony treści Visty jest najdłuższym listem samobójczym w historii[1].

## Wstęp

Opracowanie to poświęcone jest wyłącznie kosztom zabezpieczeń Visty[2]. Wszelkie kwestie "polityczne" (chodzi przede wszystkim o sens stosowania DRM) zostały już szczegółowo omówione w innych tekstach i nie będą tutaj poruszane, chyba że okażą się istotne dla analizy kosztów. Podczas czytania niniejszego opracowania warto jednak pamiętać o jednym - jeżeli zabezpieczenia Microsoftu mają działać, muszą łamać obowiązujące prawa fizyki, co pomimo szczerych chęci posiadaczy praw autorskich wydarzyć się nie może[3]. Podczas lektury wymagań stawianych przez system ochrony treści wielokrotnie można zdać sobie sprawę z tej zasadniczej sprzeczności. Wytwórcom sprzętu nie podpowiada się szybkich i działających zawsze rozwiązań - zamiast tego sugeruje się poświęcenie większej uwagi firmowej infolinii. Specyfikacja najeżona jest stwierdzeniami w rodzaju:

Zaleca się, aby producenci kart graficznych nie ograniczali się jedynie do wymogów poniższej specyfikacji i proponowali dodatkowe sposoby na ochronę treści. Dobra wola potwierdza ich zaangażowanie w ochronę treści kwalifikowanych.

Pomimo iż pierwszy raz spotykam się z taką manierą pisania specyfikacji technicznych, staram się rozumieć Microsoft. Chodzi o to, że cel, jaki stawia sobie ich dokument jest zwyczajnie i po prostu niemożliwy do osiągnięcia. Czytelnicy powinni jednak zapamiętać tą "dobrą wolę potwierdzającą zaangażowanie w ochronę treści". Przyda się wielokrotnie podczas lektury mojego opracowania[4].

Warto zauważyć, że określenie "treści kwalifikowane" (Microsoft stosuje też ostatnio określenie "treści komercyjne") wykracza poza ramy nośników HD-DVD czy Blu-Ray, ale odnosi się również do "przekazu HD w dowolnej formie" czy wręcz nawet do materiałów, które nie są rozpowszechniane w wysokiej rozdzielczości ("ogólnie rzecz biorąc treści komercyjne, niezależnie od rozdzielczości").

Wprawdzie “treści kwalifikowane” są dziś na rynku rzadkością, ale za pięć lat trudno będzie znaleźć film, który nie będzie rozpowszechniany w wysokiej rozdzielczości. Mimo więc, że Microsoft próbuje zbagatelizować wpływ systemu ochrony treści, twierdząc że jego działanie odnosi się jedynie to “treści kwalifikowanych/komersyjnych” ma jednocześnie nadzieję, że w bliskiej przyszłości ten rodzaj nagrań stanie się powszechny. Jest to główne założenie projektantów systemu - nie ma przecież potrzeby stosowania tak restrykcyjnych zabezpieczeń skoro dane przez nie chronione nie mają być w przyszłości powszechne.

---

Przypisy:

1. Komentarz ten inspirowany jest podobnym komentarzem sir Geralda Kaufmana dotyczącym wyborczego manifestu brytyjskiej Partii Pracy z roku 1983. Dokument był tak fatalny, że zaowocował najgorszym wynikiem Partii Pracy w historii a ich przeciwnicy powielali i rozpowszechniali go na własny koszt. Być może z tych doświadczeń powinno skorzystać Apple przy promocji OS X? Zapewniam że liczący 44 strony “Output Content Protection and Windows Vista” pod każdym względem bije na głowę 37-stronicowy manifest Brytyjczyków. [↩]
2. Dokument ten używa słowa “koszt” w znaczeniu “szkoda”, “strata” czy “grzywna” a nie w znaczeniu “wydatek”, “cena”, “nakłady”. Rzetelna analiza finansowa wymagałaby pełnego audytu kosztów projektowania, rozwijania, produkcji, dystrybucji, wsparcia a także kosztów obsługi prawnej dla każdego z producentów osobno. Obawiam się, że nawet producenci mieliby tu problem z oszacowaniem swoich kosztów. [↩]
3. Zaryzykuję dziś stwierdzenie, że obejście czy złamanie systemu zabezpieczeń treści Visty zajmie niecały dzień, jeżeli tylko będzie to kwestia wadliwego sterownika czy łatwej do odnalezienia luki w bezpieczeństwie, która dotyczy tylko jednego fragmentu kodu. Jeżeli obejście systemu nie będzie wiązało się z konkretnym sterownikiem czy urządzeniem, to stawałbym na niecały tydzień. Nie znaczy to oczywiście, że nastąpi to dzień czy tydzień po premierze, ale wtedy, gdy ktoś z odpowiednią wiedzą będzie miał motywację do złamania zabezpieczenia.  
Dochodzą mnie słuchy, że mamy powtórkę z sytuacji sprzed kilku lat (do złamania posłużył odtwarzacz Xing). Podobno komuś udało się wydobyć z programu PowerDVD klucze HD-DVD i Blu-Ray, które pozwalają na odtwarzanie wszystkich(?) materiałów HD z dysku komputera w każdej rozdzielczości ([twórcy PowerDVD oficjalnie twierdzą, że nie popełnili żadnego błędu](#) i nie będą wydawać nowej, poprawionej wersji programu). Wydaje się, niemożność odtworzenie legalnie nabytego nagrania na legalnie nabytym sprzęcie okazała się wystarczającą motywacją do stworzenia cracka. [↩]
4. Przed wyświetleniem danych na ekranie system musi je kilkukrotnie powielić. Jako przykład niech posłuży ten dokument. Nim pojawi się u ciebie na ekranie musi być najpierw skopiowany z dysku serwera do jego pamięci, potem do bufora stosu TCP/IP, potem poprzez internet do bufora stosu twojego komputera, stamtąd do pamięci, następnie do pamięci podręcznej twojej przeglądarki (czyli na dysk), potem przesłany do silnika renderującego, skąd jeszcze skok do bufora ekranu i dopiero potem na ekran. Jeżeli go wydrukujesz, dane odbędą jeszcze kilka wędrówek po systemie. Vista i jego system DRM dążą do tego, żeby kopiować dane tak naprawdę ich nie kopiując. Jeżeli nie jesteś biegły w tej technologii, to ten pomysł wyda ci się zapewne szalony, ale gdyby oprzeć się na mechanice kwantowej, to można zauważyć że chroniona treść wchodzi w superstan bycia jednocześnie skopiowaną i nieskopiowaną dopóki użytkownik nie zakłóci jej funkcji falowej poprzez odtworzenie tej treści (fizycy nazywają to paradoksem [EPR](#)). W zależności od tego czy do opisu mechaniki kwantowej używasz interpretacji kopenhaskiej czy może innej, rzeczy mogą się pokiełbać bardzo albo jeszcze bardziej. Sumując: żeby działać, system ochrony treści Microsoft Vista musiałby przekraczać znane nam dziś prawa fizyki i tworzyć wielokrotne kopie danych, które jednocześnie kopiami nie są. (Ktoś zwrócił uwagę, że Microsoft próbuje zaimplementować kanał szyfrowania kwantowego aby za jego pomocą doprowadzić chronioną treść do nieustalonego, nieobserwowalnego stanu.

Następnie próbuje wykryć podejrzane stany i przerywa transmisję, gdy takowe wystąpią [na wypadek, gdyby Czytelnik miał już dość fizyki kwantowej, po ludzku: Microsoft próbuje skonstruować kwadrat o sumie kątów większej niż 360 stopni. Pamiętajcie co nieco o kwadratach ze szkoły, prawda? ;) - przyp. tłumacza]. [↩]

## Ograniczenie funkcjonalności

Windows Vista zezwala na wysyłanie sygnału zawierającego dane wysokiej jakości jedynie to tych interfejsów, które posiadają wbudowane zabezpieczenia. Obecnie najpopularniejszym interfejsem służącym do wyprowadzania sygnału HD jest . Większość nowszych kart dźwiękowych zawiera cyfrowe złącze , układy audio zintegrowane na płytach głównych oferują co najmniej standardowe, koncentryczne złącze cyfrowe (często realizowane jako optyczne). Jako że S/PDIF nie posiada mechanizmów zabezpieczających przesyłane za jego pośrednictwem dane, Vista wymaga, by podczas odtwarzania zabezpieczonych danych HD było ono wyłączone[1]. Innymi słowy, jeżeli wydałeś sporo pieniędzy na sprzęt audio wysokiej klasy posiadający łącze S/PDIF, to Microsoft nie pozwoli Ci na nim odtwarzać dźwięku dekodowanego przez Twój komputer.

Powiedzmy że kupiłeś właśnie płytę [“Dark Side of the Moon”](#) grupy [Pink Floyd](#). Kupiłeś ją w wersji [Super Audio CD](#) wydanej w 2003 roku, w trzydziestą rocznicę nagrania tego legendarnego krążka. Chcesz odtworzyć ją za pomocą Visty, niestety system uważa posiadane przez Ciebie złącze S/PDIF za nieodpowiednie dla jakości Super Audio i odcina je a ty kończysz jak słuchacz występu [Marcela Marceau](#).

Podobne ograniczenia dotyczą popularnego złącza typu “komponent” ([YPbPr](#)). Vista blokuje je podczas przesyłania danych HD, więc nie możesz podłączyć do niego telewizora czy projektora wysokiej rozdzielczości. Co jednak jeżeli kupiłeś kartę graficzną ze złączem wspierającym zabezpieczenie ? Jest spora szansa, że będziesz musiał kupić drugą kartę, taką która *naprawdę* obsługuje HDCP, ponieważ żadna z kart dostępnych do niedawna nie zapewniała prawidłowej obsługi tego zabezpieczenia, pomimo że producent twierdził coś zupełnie przeciwnego. Tak całą sprawę opisuje artykuł [“The Great HDCP Fiasco”](#):

Żadna z kart AGP czy , którą możesz dziś kupić w sklepach nie obsługuje HDCP [...] Jeżeli właśnie wydałeś 1000 dolarów na parę Radeonów X1900 XT zakładając, że będziesz mógł bez przeszkód odtwarzać filmy HD-DVD czy Blue-Ray w rozdzielczości 1920×1080, to właśnie wyrzuciłeś pieniądze w błoto [...] Jeżeli wydałeś jedyne 1500 dolarów na zestaw dwóch 512-megowych 7800GTX by odtwarzać na nich filmy HD-DVD czy Blue-Ray w rozdzielczości 1920×1080, to właśnie wyrzuciłeś pieniądze w błoto.

(oba urządzenia, o których wspomina powyższy fragment są kartami z najwyższej półki, produkowanymi przez dwie czołowe firmy w branży: [ATI](#) i [nVidie](#)). ATI zresztą doczekał się procesu sądowego na tym tle. Gdy w sierpniu 2006 roku Sony ogłosiło dostępność napędu Blue-Ray dla PC, okazało się że urządzenie to nie potrafi odtwarzać nośników Blue-Ray w standardzie HD ([“First Blu-ray disc drive won't play Blu-ray movies”](#)):

Jako że obecnie nie ma komputerów wyposażonych w układy, które wspierają HDCP, odtwarzanie materiału HD nie jest możliwe

Prawdę mówiąc nikomu jeszcze nie udało się obejrzeć filmu HD w jakości HD na którymkolwiek z systemów Windows. Dotychczasowe próby kończyły się albo brakiem sygnału na wyjściu albo komunikatem systemu ochrony treści, że zadziałało zabezpieczenie. Nie można oczywiście twierdzić, że takie odtwarzanie nie będzie możliwe w przyszłości, ale nabywcy Visty mogą spodziewać się problemów.

Podobnie jak właściciele kart graficznych, problem mają też posiadacze monitorów LCD wysokiej rozdzielczości. Na targach CEC 2007 pokazano nowy monitor Samsunga - Syncmaster 275T. Sprzęt ten wyświetla 27-calowy obraz w rozdzielczości 1920×1200 i to w czasach, gdy inni dostawcy jako

nowość proponują ekrany 24- i 25-calowe[2]. Problem polega na tym, że monitor jest z punktu widzenia Visty bezużyteczny - system żadnego z portów (DVI-D, 15-pionowy D-Sub, S-Video oraz komponent) nie uważa za bezpieczny.

Jeżeli macie jeszcze więcej pieniędzy do wydania, to zawsze możecie się szarpnąć na największy monitor LCD świata - 46-calowy SyncMaster 460PN. Wydanie na niego 4000 dolarów to wyjątkowo kiepska inwestycja, bo Vista nie będzie z nim współpracować. Co ciekawe, sprzęt ten był reklamowany przez sprzedawców jako "HDTV ready", co stanowi jaskrawy przykład tego, jak bardzo już sprane i niewiarygodne jest określenie "HD-ready".

Ze względów bezpieczeństwa chronionych przez siebie treści, Vista prawdopodobnie nie będzie obsługiwała żadnych dodatkowych funkcji urządzenia, oprócz tych, które potrafi obsłużyć sama, w sposób bezpośredni. Przykładowo, wiele kart dźwiękowych opartych na chipsecie [C-Media](#) (czyli w praktyce większość kart dostępnych na rynku) posiada wsparcie dla interfejsu firmy [Steinberg](#). Sygnał podawany na to łącze całkowicie omija systemowy mikser dźwięku i wszelkie sterowniki w celu zapewnienia większej elastyczności i zmniejszenia opóźnień przez nie generowanych. [Wsparcie ASIO jest standardem wśród nowszych kart C-Media](#). Ponieważ takie rozwiązanie omija system ochrony treści, najprawdopodobniej będzie musiało zostać wyłączone, co szczególnie zaboli audiofilów oraz profesjonalnych muzyków, którzy korzystają z ASIO jako źródła o lepszej jakości dźwięku (więcej informacji o systemie dźwiękowym Visty i zmianach, jakie w nim poczyniono w stosunku do XP znaleźć można w [poście pochodzącym z forum Creative Labs](#)).

---

Przypisy:

1. Jest , ale wyraźnie pisze na nim "nie dotykać". [[↵](#)]
2. Gdyby ktoś zechciał udostępnić mi taki fajny, 27-calowy monitor do... yyyy... testów, to obiecuję go zwrócić do roku 2012. [[↵](#)]

## Pośrednie ograniczenie funkcjonalności

Ograniczeniom wyrażonym jasno i wprost towarzyszą również przeszkody ukryte nieco głębiej. Na przykład rozmowy głosowe opierają się w pewnym stopniu na technice automatycznego usuwania efektu echa (). AEC do swojej pracy wymaga próbek sygnału audio, co jednak nie jest możliwe na Viście, stanowiłoby bowiem furtkę do chronionych "treści kwalifikowanych". System zezwala wprawdzie na bardzo ograniczone zabiegi w tym względzie, ale efekty pracy algorytmów usuwania efektu echa będą dużo gorsze.

Wymaganie wyłączenie wyjść audio i video prowadzi do zamieszania do standardowych operacji w systemie ponieważ przyjęta polityka bezpieczeństwa realizuje założenie według którego "poziom czułości" systemu zabezpieczeń jest taki, jakiego wymagają najbardziej chronione nim dane. Zatem gdy tylko pojawią się dane pochodzące z "treści kwalifikowanych", system od razu wyłącza "niebezpieczne porty" i obniża jakość sygnału. Najśmieszniejszy jest fakt, że to wyłączenie i obniżanie jakości ma charakter dynamiczny, jeżeli zatem chroniony sygnał jest przerywany lub zanika (jak na przykład wyciszająca się stopniowo muzyka), różne porty wyjściowe będą dynamicznie wyłączone i włączone a jakość sygnału będzie się raz podnosić, raz opadać. W normalnych warunkach takie objawy wskazują na konieczność przeinstalowania sterowników, w Viście jednak są na porządku dziennym; więcej nawet - wskazują że system działa jak należy.

## Pogorszona jakość nagrań

Jednocześnie z manipulacją portami na zasadzie "wszystko albo nic", Vista wymaga żeby każdy interfejs zdolny transmitować dane wysokiej jakości automatycznie pogarszał jego jakość gdy tylko pojawią się na nim chronione dane. Osiąga się to z wykorzystaniem tak zwanego "dusiela", który najpierw powoduje obniżenie jakości sygnału aby potem cyfrowo go "ulepszyć", powodując tym samym sporą stratę w jego jakości. Jeżeli na przykład używacie nowego, wysokiej klasy monitora

LCD podłączonego do złącza i pojawi się na nim chroniony przekaz, to obraz jaki ujrzycie będzie - jak to ujmuje specyfikacja - "nieco zamglony", trochę jak na 10-letnim monitorze kupionym na wyprzedazy za dwa dolary (w [przypisach](#) znajdziecie konkretne przykłady). Specyfikacja wprost zezwala na stosowanie analogowych wyjść, ale tylko dlatego, żeby nie rozwścieczyć wielu obecnych posiadaczy analogowych wyświetlaczy. W przyszłości prawdopodobnie nawet one będą wyłączone. Wydaje się, że jedynym otwarciem pobłogosławionym interfejsem jest bardzo słabej jakości gniazdo TV-out, oczywiście pod warunkiem, że nad sygnałem czuwa [system Macrovision](#).

Podobne zabiegi ze strony systemu odnoszą się również do dźwięku. Dokument Microsoftu określa jego brzmienie "po przejściach" jako "niewyraźny, z mniejszą ilością detali"[1].

Zdumiewa, że specyfikacja pozostawia w gestii producentów sprzętu rozróżnienie gamy ich produktów na podstawie celowo pogorszonej jakości sygnału. To mniej więcej tak, jak by połamać olimpijskim biegaczom nogi a potem oceniać ich na podstawie tego jak szybko są w stanie kuśtykać podpierając się kulami.

Specyfikacja udostępniona przez Microsoft stwierdza, że pogorszeniu ulegną tylko te obrazy, które składają się z więcej niż 520 000 pikseli (projektanci przewidzieli nawet specjalny kod błędu na tą okoliczność - STATUS\_GRAPHICS\_OPM\_RESOLUTION\_TOO\_HIGH). Stanowi to z grubsza odpowiednik rozdzielczości 800×600, co oznacza że efekt ten dotknąć może każdy wyświetlacz, jaki kiedykolwiek zostanie podłączony do komputera wyposażonego w ten system. Absolutnym, podawanym przez producenta minimum, jakie brać można pod uwagę przy instalacji Visty jest właśnie rozdzielczość 800×600 (oraz Pentium II 800 MHz i 512, co jest założeniem wysoce optymistycznym). Taki sprzęt uniemożliwia jednak skorzystanie z interfejsu Aero, co właściwie stawia pod znakiem zapytania sens przesiadki z XP (które zresztą na procesorze o takcie 800 MHz też nie czuje się za dobrze). Minimalne wymagania, które musi spełnić karta graficzna w celu uruchomienia Aero to "obsługa 9 i technologii Pixler Shader 2.0, 128 MB RAM własnej pamięci, rozdzielczość minimum 1024×768x32". Aero Glass stawia jeszcze wyższe wymagania. Minimalna rozdzielczość, z jaką natywnie pracują dzisiejsze monitory LCD to 1024×768 - dobrze wyglądające 800×600 wymaga zastosowania monitora CRT. W praktyce zatem cały sprzęt dostępny dziś na rynku znajduje się powyżej granicy 520 000 pikseli, poza którą Vista może zacząć kombinować z jakością sygnału.

(Do tej pory systemy operacyjne zwracały błędy na przykład przy problemach z odczytem danych czy przy uszkodzeniu pakietu, ale Vista idzie o krok dalej - jest pierwszym na świecie systemem, który przewiduje kod błędu "rozdzielczość ekranu przekroczone")

Poza oczywiście słabszą jakością nagrań, system zabezpieczeń stosowany w Viście może zaowocować całkiem poważnymi konsekwencjami wszędzie tam, gdzie jakość sygnału podawanego do urządzenia jest sprawą kluczową. Za przykład może posłużyć analiza zdjęć medycznych, bazująca na materiale, który nie akceptuje żadnych zakłóceń wprowadzanych na przykład przez formaty stratnej kompresji. Artefakty wywołane przez zakłócenia mogą prowadzić do błędnej diagnozy a nawet do stanów zagrożenia życia. Nie jest trudno wyobrazić sobie pracownika placówki medycznej obsługującego peceta używanego do analizy obrazów, który jednocześnie słucha na nim muzyki (napędy w służbowych komputerach służą jak wiadomo głównie do odtwarzania płyt lub zbiorów). Płyta CD nie jest rzecz jasna nośnikiem danych HD, ale przykład ten miał uzmysłowić jak częstą praktyką jest odtwarzanie mediów podczas pracy. Zamiast nagrań audio można rzecz jasna odtwarzać film (przesłany przez znajomego czy pobrany z YouTube), który bez wiedzy użytkownika może okazać się chroniony przez system. Jeżeli takie dane pojawią się na nieodpowiednim interfejsie, Vista natychmiast pogorszy jakość sygnału przesyłanego do monitora, co wpłynie oczywiście na jakość wyświetlanych przez to urządzenie zdjęć. Najgorsze jest to, że nie można tego działania w żaden sposób zniwelować - Windows bez ostrzeżenia obniży jakość sygnału kierując się nieznanymi nikomu - poza systemem ochrony treści - przesłankami[2][3]. Microsoft twierdzi, że to pogorszenie obrazu dotyczyć będzie jedynie tych partii obrazu, w których znajdzie się chroniona treść, ale jako że nie ma w tej chwili na rynku urządzeń, które wspierałyby taką funkcję trudno jest powiedzieć jak to będzie w praktyce funkcjonowało (w tej chwili na przykład system po prostu blokuje wyświetlanie "treści kwalifikowanych" zamiast pogarszać ich jakość).

(Obsesja przemysłu rozrywkowego na tle jakości obrazu jest o tyle śmieszna, że wiele badań wskazuje na fakt, że dla użytkownika najbardziej liczy się rozmiar ekranu, nie zaś jakość przekazu. Oczywiście gdy zaprowadzimy klienta do sklepu i postawimy go przed najnowszym ekranem plazmowym, to początkowo będzie on zachwycony faktem, że może policzyć wszystkie włosy na brodzie Gandalfa. Niestety, gdy Gandalf zaczyna walczyć z Balrogiem, wszelkie detale przestają mieć znaczenie i jedynym wyróżnikiem zostaje wielkość obrazu. W swojej książce “Media i ludzie” odnoszą się do tego faktu profesorowie Byron Reeves i Clifford Nass. W jednym z eksperymentów pokazali oni publiczności film, wyświetlając go na najlepszym dostępnym im sprzęcie, po czym powtórzyli seans używając tym razem piątej kopii zrobionej na mamej taśmie i wyświetlonej za pomocą przeciętłego sprzętu. Uczestnicy eksperymentu nie zauważyli żadnej różnicy w jakości! Podobne obserwacje można przeprowadzić samemu: wystarczy podpiąć do komputera dwa monitory - LCD i CRT. Spójrzcie na ekran CRT a po chwili na LCD. Po dwóch-trzech minutach powróćcie wzrokiem do CRT i oceńcie sami. Czy widzicie jakąś różnicę?

Jest dokładnie odwrotnie - liczy się jedynie wielkość ekranu. W praktyce zatem pogorszony obraz wyświetlony na dużym monitorze VGA (czy jakimkolwiek innym urządzeniu posługującym się analogowym złączem) będzie oceniony wyżej niż obraz nie pogorszony, wyświetlony na mniejszym monitorze LCD (o ile znajdzie się monitor działający z Vistą). Rzecz jasna przekonanie do tego szerokim mas konsumentów to już inna sprawa.)

---

Przypisy:

1. Czytelnicy często pytają w jaki sposób dostawcy treści nie tak bogaci jak studia filmowe podoleją kosztom związanym z przygotowaniem materiału HD. Jedna z osób, która współpracuje ze mną przy tworzeniu tego dokumentu donosi, że “spotykałem się z mniejszymi producentami, zarówno takimi, którzy żyją z utrwalania wesel czy innych uroczystości oraz takimi, którzy mają już na swoim koncie prawdziwe filmy. Wszyscy oni napotykali kolejne problemy w rodzaju montażowni, kamer, formatów zapisu, itp. Decyzje, które podejmowali oparte były raczej na dostępności określonego sprzętu niż na szacunku kosztów”. Podobno duże wytwórnie nie narzekają na taki obrót sprawy, bo ta sytuacja zniechęca innowacyjnych, kreatywnych i dynamicznych debiutantów. [↵]
2. Philip Dorrell prezentuje [fajny komiks, który dobrze ilustruje ten problem](#) [↵]
3. Karl Siegmund opisał interesujące zagrożenie, które może mieć miejsce gdy Vista zarządza systemem nadzoru audio/video. Skoro można przekonać system, że ten przekazuje dane chronione, to można też całkowicie go oślepić, bo centrum monitoringu nie będzie raczej używało nagrywarek i monitorów obsługujących DRM. Już widzę tą kwestię z “Ocean’s Fifteen” lub “Mission Impossible 6”: “W porządku, ich system nadzoru pracuje na Viście, możemy go wyłączyć jeśli Windows uzna, że transmituje filmy” [↵]

## Eliminacja otwartych sterowników

W celu przeciwdziałania tworzeniu emulatorów sprzętu akceptowanego przez Vistę, Microsoft wprowadza pojęcie , który to proces ma za zadanie tworzenie cyfrowego “odcisku palca” jednoznacznie identyfikującego każde urządzenie. Operację tą wykonuje na sprzęcie jego sterownik (niech będzie to na przykład renderowanie obiektu na karcie 3D) - a jej wynik jest unikalny dla każdego modelu kart każdego producenta.

Aby HFS mógł funkcjonować, szczegóły budowy urządzenia muszą być utrzymywane w tajemnicy. Oczywiście każdy, kto zna je na tyle dogłębnie aby napisać własny sterownik (na przykład dla systemu takiego, jak Linux) będzie miał wiedzę wystarczającą również do oszukania HFS. Jedynym zatem sposobem na ochronę skuteczności HFS będzie utrzymywanie budowy urządzeń w tajemnicy i ujawnianie ich tylko w takich granicach, jakie są niezbędne na przykład na potrzeby testów porównawczych.

To “zamykanie” otwartej przecież architektury PC jest bardzo niepokojącym trendem. Ćwierć wieku

temu [IBM](#) podjął wielkopomną decyzję o otwarciu swojej konstrukcji i opublikował wszelkie dotyczące jej szczegóły, czym otworzył pole dla konkurencji w ramach wolnego rynku. Wielu małych producentów, którzy w zgodzie z duchem tamtych czasów zaczynali swoją działalność w garażu, miało dzięki temu szansę na rozwój. Ta otwartość okazała się podstawowym atutem PC, to ona stworzyła dzisiejszy rynek wytwórców sprzętu, to ona wreszcie wprowadziła komputery pod strzechy, dzięki czemu w każdym domu stoi dziś nawet kilka takich maszyn. Ostatnie posunięcia Microsoftu grożą powrotem do sytuacji sprzed 25 lat, kiedy tylko wybrani mogli produkować sprzęt dla danej platformy.

## **Eliminacja ujednoczonych sterowników**

Istnienie HFS pociąga za sobą jeszcze inne koszty. Większość producentów od jakiegoś już czasu wypuszcza ujednoczone sterowniki do swoich urządzeń. Jako że HFS wymaga, żeby oprogramowanie rozpoznawało nie tylko każdy typ urządzenia (na przykład układ graficzny) ale również każdy wariant tego urządzenia (na przykład układ taktowany określoną częstotliwością zegara) nie będzie już możliwe wydawanie sterowników, które pasują do wszystkich urządzeń pewnej klasy, jak dzisiejsze oprogramowanie z serii Catalyst/Detonator/ForceWare. Każda najmniejsza modyfikacja na poziomie sprzętu będzie wymagała osobnego sterownika, tak aby HFS mógł działać w pełni skutecznie. Jest to powód do zmartwienia dla producentów sprzętu, nie dla użytkowników - z ich punktu widzenia nadal mają do czynienia z pojedynczym pakietem, którego objętość jednak wzrośnie. Taki model sterowników oznacza jednak wydłużony czas przygotowywania oprogramowania i zwiększone koszty.

Jeżeli układ graficzny jest zintegrowany z płytą główną i nie ma do niego łatwego dostępu, nie jest wymagane szyfrowanie transmisji na szynie systemowej (patrz [“Zwiększone zapotrzebowanie na moc procesora”](#)). Ponieważ wymaganie szyfrowania jest bardzo uciążliwe z punktu widzenia programowania sterownika, okazać się nagle może, że karty graficzne wbudowane bezpośrednio w płytę nagle zyskają na popularności. Powstaje jednak problem rozróżnienia obu typów urządzeń: z punktu widzenia systemu zintegrowany układ graficzny nie różni się niczym od tego znajdującego się na karcie zamontowanej w specjalizowanym złączu płyty głównej - oba wpięte są po prostu do magistrali AGP/PCIe. Rozwiązanie narzuca się samo: trzeba świadomie doprowadzić do niekompatybilności obu układów, co będzie skutkowało zwiększeniem stopnia skomplikowania sterowników i przy okazji kosztów rzecz jasna.

Inne problemy związane są ze sterownikami urządzeń audio. System nie jest w stanie odróżnić złącza HDMI od S/PDIF, co było świadomą decyzją projektową mającą na celu uproszczenie sterowników. Jeżeli jednak Vista ma wyłączać interfejsy, oprogramowanie sterujące pracą HDMI musi stać się niekompatybilne z oprogramowaniem zarządzającym pracą S/PDIF, co będzie działaniem, które staje w sprzeczności z założeniami twórców obu złącz.

## **Ataki Denial-of-Service poprzez unieważnienie sterownika lub urządzenia**

Kiedy tylko w danym sterowniku lub urządzeniu zostanie odkryta luka umożliwiająca nieautoryzowany dostęp do chronionej zawartości, sterownikowi takiemu zostanie cofnięty cyfrowy certyfikat wystawiany przez Microsoft. Nie bardzo wiadomo co następuje potem, specyfikacja posługuje się określeniami w stylu “dany sterownik będzie musiał zostać wycofany a na jego miejsce wprowadzona zostanie poprawiona wersja”, choć prawdopodobnie system zezwoli na bardzo ograniczoną funkcjonalność w rodzaju rozdzielczości VGA 640×480, choćby po to, by mógł wystartować.

Oznacza to mniej więcej tyle, że po doniesieniu o luce w zabezpieczeniach powodowanej przez urządzenie lub jego sterownik, wsparcie dla tego produktu zostanie zawieszona - w skali całego świata - dopóki nie pojawi się poprawka[1]. Szczegóły są dość niejasne, ale wydaje się że jeżeli problem leży po stronie urządzenia, to jego funkcjonalność zostanie drastycznie ograniczona. Jeżeli jest to starszy sprzęt, którego rozwojem producent nie jest już zainteresowany (pamiętajmy, że obecnie sprzęt przechodzi w status “przestarzały” w ciągu roku czy dwóch, w praktyce gdy tylko

pojawi się jego następcą) to wszystkie te urządzenia z dnia na dzień przestaną funkcjonować.

Za przykład może tu posłużyć karta graficzna Riva TNT2, która wciąż często znajduje się w komputerach używanych w biurach, bo czego więcej potrzeba do uruchomienia Worda, Excela czy Outlooka (w zasadzie każdej aplikacji, która nie jest grą)? Sterowniki do tych kart nie były aktualizowane od dawna z tego jednego powodu - nowe oprogramowanie nie jest potrzebne, bo karta i tak nie udźwignie wymagań współczesnych gier. Jeżeli więc w przypadku TNT2 okazałoby się, że istnieje niebezpieczeństwo “wycieku” treści kwalifikowanych, to nie wydaje się żeby nVidia była zainteresowana modyfikacją pokrytych kurzem sterowników.

Wizja unieważnienia sterowników jest realnym niebezpieczeństwem, jakie grozi dostawcom sprzętu[2]. Szczegóły konstrukcji tego “młotka” są ukryte głęboko w paragrafach umów licencyjnych, obito mi się jednak o uszy, że oprócz ograniczenia funkcjonalności konkretnego modelu może chodzić o wielomilionowe odszkodowania oraz embargo na dostarczanie nowych urządzeń w przyszłości.

Unieważnienie sterownika pociągać może za sobą koszty, z których istnienia nie zdajemy sobie dziś sprawy. Antypiracki komponent Windows - (w przypadku Visty jest to [Software Protection System](#)) - jest bardzo silnie związany z zainstalowanym w komputerze sprzętem. Microsoft zezwala na zmiany w posiadanym sprzęcie w z góry ograniczonym zakresie - po wyczerpaniu tego limitu będziesz musiał odnowić licencję (do dziś nie wiadomo dokładnie co można a czego nie można wymieniać aby nie ryzykować kolejnych wydatków). Jeżeli więc nagle jedno z urządzeń zostanie wyłączone (nawet tymczasowo, w oczekiwaniu na nową wersję oprogramowania) a w jego miejsce użytkownik zainstaluje inne urządzenie, okazać się może, że WGA uzna komputer za nowy i zablokuje działanie całego systemu. Stanie się to na pewno wtedy, gdy trzeba będzie wymienić jeden z podstawowych elementów maszyny, jak płytę główną. Wycofanie zatem sterownika jakiegokolwiek urządzenia zintegrowanego z płytą (obecnie praktycznie każda ma wbudowany układ audio, wiele z nich również układ wideo) może mieć bardzo niemiłe konsekwencje.

Inną konsekwencją podejścia polegającego na “poprawkach” unieważniających sterowniki jest zniechęcenie użytkownika do poprawek w ogóle. Przez pojęcie “poprawki” rozumiemy z reguły działanie mające na celu poprawienie komfortu czy bezpieczeństwa pracy z komputerem. O ile jednak działanie oprogramowania typu “malware” jest dla użytkownika niewidoczne, o tyle wyłączenie sterownika jest zauważalne od razu, co może doprowadzać do wyłączania funkcji Windows Update w ogóle.

Nie wiadomo co się wydarzy, gdy unieważnione zostaną sterowniki płyty głównej zawierającej nieużywane układy audio i oprócz nich kartę dźwiękową. Windows nie jest w stanie stwierdzić czy jakieś urządzenie jest czy nie jest podłączone do wyjść audio płyty głównej, wie tylko że użytkownik używa karty M-Audio Revolution 7.1 Surround Sound, więc prawdopodobnie będzie musiał też unieważnić sterowniki płyty głównej, mimo że użytkownik z nich nie korzysta. Problem jest poważny, bo praktycznie wszystkie płyty główne mają wbudowane układy dźwiękowe.

Zagrożenie atakami , które dotyka urządzenia wyposażone w złącza HDMI zdążyło się już zmaterializować w postaci tak zwanych “wzmacniaczy HDMI”. Jest to sprzęt, który na wejściu pobiera sygnał HDMI aby wyprowadzić go na wyjściu w postaci wzmocnionego DVI. Po drodze oczywiście znika zabezpieczenie HDCP. Dokładnie takie “lekarstwo” [zostało zarekomendowane przez firmę Westinghouse](#) (duży amerykański producent sprzętu TV) w przypadku problemów ich sprzętu 1080p z konsolą Playstation 3. Zalecili klientom “zakup przejściówki z HDMI na DVI aby obejść HDCP”. W odniesieniu do zabezpieczeń przed kopiowaniem producenci sprzętu doszli zatem do takich samych wniosków, do jakich doszedł komputer w [“Grach wojennych”](#) w odniesieniu do wojny termonuklearnej: Dziwna gra. Wygrywa jedynie ten, kto w nią nie gra.

Wzmacniacze są urządzeniami stosunkowo prostymi w konstrukcji, opartymi na powszechnie dostępnych układach HDMI. Poza tymi dostępnymi w handlu, istnieją też modele skonstruowane przez hackerów, oparte na pokazowych egzemplarzach układów otrzymanych od ich producentów. Jeżeli ma się odpowiednie “plecy”, można nawet uzyskać dostęp do kart tworzonych dla developerów, które od razu mają wbudowaną opisywaną wyżej funkcjonalność. Nie poruszam tu

nawet tematu odtwarzaczy HD z interfejsami (SMPTE 292M). HD-SDI to pozbawione zabezpieczeń złącze cyfrowe używane przede wszystkim w studiach telewizyjnych, choć dostępne jest też poza w formie “ulepszeń”, które pozwalają uzyskać obraz wyższej niż w przypadku HDMI jakości, w dodatku nie skażony HDCP.

Załóżmy teraz, że producent takiego “wzmacniacza” kupuje tonę układów HDMI (a kupować będzie olbrzymie ilości, bo nikt mu już takich układów nie sprzeda po wypuszczeniu pierwszej serii “wzmacniaczy”). Sterownik takiego “bandyckiego” urządzenia można unieważnić... a wraz z nim setki tysięcy innych urządzeń, które są oparte na takim samym układzie HDMI. Serwis Egadget opublikował [scenariusz opisujący taką historię](#).

(Ostateczny efekt wycieku klucza zależy od tego, w jaki sposób używa go atakujący. Klucze stosowane przez napędy HD-DVD/Blue-Ray działają w ten sposób, że klucz przypisany do urządzenia odszyfrowuje klucz przypisany do danego tytułu a ten z kolei odszyfrowuje zawartość nośnika. Pozwala to na unieważnienie klucza bez obawy o zablokowanie płyty również na innych urządzeniach, ponieważ klucze w nich zawarte nadal będą mogły posłużyć do odszyfrowania tytułu i nośnika (ten opis jest nieco uproszczony, więcej na ten temat w specyfikacji AAC3).

Klucz urządzenia jest przypisany do konkretnego odtwarzacza/dostawcy ale już klucz tytułu jest unikalny tylko dla zawartości płyty. Zorientowaliście się już do czego zmierzam? Publikując klucz urządzenia atakujący spowoduje prawdziwe piekło wśród właścicieli urządzeń, które go zawierają, bo klucze zostaną unieważnione. Z drugiej strony, ujawnienie klucza tytułu grozi możliwością wydania wersji odkodowanej ponieważ nie sposób stwierdzić jakiego urządzenia użyto dla złamania klucza tytułu. Co więcej, w związku z tym że nie można “odnowić” klucza (zaszyfrowana zawartość + klucz = odszyfrowana zawartość), to w tym momencie treści chronione przez ujawniony klucz są już ochrony pozbawione.

---

Przypisy:

1. Nie bardzo wiadomo w jakim zakresie urządzenie zostanie “okaleczone” po cofnięciu uprawnień (czyli w chwili, gdy wektor wyboru klucza urządzenia pojawi się na liście unieważnionych). Wymagania HDCP są w tej kwestii jasne - z chwilą unieważnienia, urządzenie nie otrzyma żadnych danych. Sprawa się komplikuje, gdy dane urządzenie działa w środowisku mieszanym (czyli nie jest samodzielne). Niektóre dokumenty sugerują, że Windows zachowa się tak, jak zachowuje się HDCP (“Vista wycofa certyfikat sterownikom nie spełniającym warunków stawianych przez system ochrony treści. Jeżeli ten sam sterownik obsługiwać będzie kilka produktów tego samego producenta, wszystkie te produkty zostaną wyłączone.”), podczas gdy inne źródła twierdzą, że wadliwy sterownik nie będzie po prostu otrzymywał danych HD. Jak będzie naprawdę, okaże się w praktyce. [↵]
2. Nasuwa się tu porównanie ze starą piłą i powiedzeniem, że gdyby Lucas Electric zajmował się produkcją broni, nie byłoby czym wojować. [↵]

## Ograniczona stabilność systemu

Sterowniki muszą być bardziej skomplikowane. Producent musi zaangażować dodatkowe środki w opracowanie oprogramowania zdolnego wyizolować i chronić wybrane fragmenty kodu. - ATI

System ochrony treści, w jaki wyposażono Windows Vista wymaga by urządzenia (sterowniki systemowe i te zaszyte w sprzęcie) reagowały na wszelkie nietypowe sytuacje ustawieniem tak zwanych “bitów spustowych” (ang. “tilt bits”). Na przykład, gdy pojawią się zaburzenia napięcia czy zakłócenia na szynie systemowej, gdy jakaś funkcja zwróci niespodziewany wynik, gdy jeden z rejestrów będzie zawierał nie takie dane, jakie zawierać powinien, gdy generalnie coś pójdzie “nie tak” - wtedy sterownik powinien ustawić “bit spustowy”. Problem w tym, że takie zdarzenia nie są wcale rzadkością w dzisiejszych komputerach. Na przykład podłączenie urządzenia zasilanego z

jednej z szyn systemowych może skutkować niewielką i krótkotrwałą zmianą napięcia na całej szynie, niedostatecznie precyzyjne w zarządzaniu stanem urządzenia mogą okazać się też jego sterowniki. Do tej pory nie stanowiło to problemu - system wykazywał się po prostu pewną elastycznością. W skrócie - niewielkie zakłócenia są typowe. Co więcej, stopień tych zakłóceń może różnić się w zależności od użytego sprzętu - niektóre maszyny mogą doświadczać większych odchyień od normy, inne zaś mniejszych. Staje się to oczywiste gdy mamy okazję doświadczyć krótkiego zaniku napięcia, które dotyka naraz wielu komputerów: niektóre się wyłączają, inne zawieszają, jeszcze innym nic się nie stanie.

Wraz z wynalazkiem "bitów spustowych" cała dotychczasowa tolerancja dla różnorodnych zakłóceń znika. Każda niewielka niezgodność zostaje natychmiast wychwycona, może być bowiem oznaką próby włamania. Jak na ustawienie tych bitów reaguje system? Bardzo prosto i skutecznie - restartując cały podsystem graficzny.

Takie "wynalazki" mają też reperkusje w związku z bezpieczeństwem systemu, w szczególności z wrażliwością na ataki DoS. Można się tylko cieszyć, że autorzy programów typu malware mają na względzie korzyści finansowe a nie bezmyślną destrukcję. Vista udostępnia wygodne w użyciu "spusty", które można nacisnąć, gdy chce się komuś zaszkodzić. Zagrożenia dla bezpieczeństwa narodowego wydają się w tym świetle oczywiste - niewielki, sprytnie ukryty kawałek kodu mógłby całkowicie zablokować maszynę a z definicji okryty mgłą tajemnicy system ochrony treści mógłby uniemożliwić ustalenie dlaczego nagle wszystko oszalało. Ten sam system udostępnia takim programistom tarczę w postaci .

Nawet jeżeli zapomnimy na chwilę o złośliwym oprogramowaniu, to łatwo sobie wyobrazić obcego agenta, który właśnie dostaje do ręki potężne narzędzie, pozwalające mu sparaliżować sporą część infrastruktury przeciwnika. Rządy na całym świecie są już teraz zaniepokojone skalą, w jakiej system produkowany w USA kontroluje ich komputery [polski ani trochę - przyp. tłumacza] i zapewne nie będą szczęśliwe wiedząc, że jego najnowsza odsłona podniosła zdalny detonator do rangi funkcji systemowej. Tak jak w przypadku historii z analizą zdjęć medycznych - nie wiadomo w którym momencie system ochrony treści zdecyduje się wkroczyć, co zmienia pecety z zainstalowaną Vistą w tykające bomby zegarowe.

Scenariuszy, w których "bity spustowe" nagle "odpalą" może być wiele. Wyobraźmy sobie statek wojenny operujący w strefie działań wojennych, którego podstawowe funkcje kontrolują komputery sterowane przez Vistę. Zakłócenia wychwycone przez system spowodować może na przykład nieodległa detonacja - detonacja, która nie wyrządziła statkowi żadnej szkody, poza pobudzeniem systemu operacyjnego do działania. Podobna sytuacja miała już miejsce: we wrześniu 1997 roku Windows NT sparaliżował funkcjonowanie krążownika rakietowego USS Yorktown ("NT Leaves Navy "Smart Ship" dead in the water", Government Computer News z 13.07.1998 r.). Teraz szansę na powtórzenie tego wyczynu ma Windows Vista - i to nie dlatego, że coś poszło nie tak, tylko dlatego, że system zadziałał prawidłowo.<sup>[1]</sup>

---

#### Przypisy:

1. Oczami wyobraźni widzę już pozwy sądowe, które zostaną wniesione, jeżeli urzeczywistni się wersja przewidująca całkowite blokowanie urządzeń ([przypis](#)). Być może Microsoft i dostawcy treści będą kupować zwracać właścicielom zablokowanych urządzeń koszty poniesione na zakup sprzętu. Ta sprawa, dopóki nie zostanie ostatecznie rozwiązana, odetnie systemowi Microsoftu dostęp do zastosowań, w których pewna niestabilność jest codziennością.

Niektórzy twierdzą, że nie wyobrażają sobie, żeby zdecydowano się na taki ruch, ponieważ negatywny oddźwięk wśród użytkowników byłby olbrzymi, tyle że dostawcy treści będą równie zdesperowani. Prawdziwym dowodem na to, jak dalece Microsoft jest "zaangażowany w sprawę ochrony prawa autorskich" okazało się tempo, w jakim wydano poprawkę zapobiegającą łamaniu zabezpieczeń . Najgroźniejszy nawet robak internetowy nie spowodował takiego pośpiechu w Redmond (zob. ["Quickest Patch \\*Ever\\*"](#)). Wydaje się

zatem, że firma traktuje sprawę śmiertelnie poważnie, skoro priorytet takich łatek jest wyższy niż poprawki związane z bezpieczeństwem systemu. Każdy, kto czytał "Sierpniowe salwy" może skojarzyć całą sytuację z sytuacją, jaka panowała w Europie przed wybuchem pierwszej wojny światowej, kiedy to siedzących w okopach żołnierzy - mimo pełnej świadomości, że to, co nastąpi będzie katastrofą - nie można było już wycofać. W przypadku unieważnienia sterownika stroną przegrywającą jest zawsze Microsoft. Prawnicy tej firmy nie byli chyba do końca przytomni, gdy akceptowali to założenie - pierwsze wycofanie uprawnień, które dotknie szpital, system kontroli lotów czy jakiś podobny system spowoduje, że do końca życia nie wyjdą z sali sądowej. (Kilka osób stwierdziło, że przyklepanie tego przez prawników zapewnia im pracę do końca życia. Nie wydaje mi się. Po pierwsze, obowiązkiem prawnika jest obrona interesów klienta, więc świadome wprowadzanie go na minę raczej spowoduje problemy w karierze niż jej dalszy rozwój. Po drugie, Microsoft ma własny dział prawny, który i tak ma co robić. Nie chcieliby sobie raczej dodawać zajęć. [↔])

## Zwiększone ceny sprzętu

Urządzenie nie może zostać skierowane na rynek zanim nie spełni wymogów specyfikacji... prawdopodobne częstsze wymiany sprzętu - ATI

Oznacza to zwiększenie kosztów projektowania płyt głównych, wydłuża proces wprowadzenia produktu na rynek, zmniejsza elastyczność dostawców. Koszty te ponoszą nabywcy sprzętu, co może opóźnić proces wprowadzania na rynek nowych rozwiązań - ATI

Przed producentami sprzętu Vista stawia wiele wymagań dotyczących jakości ich produktów. Tak naprawdę jednak to nie są wymagania Microsoftu, tylko przemysłu rozrywkowego. Zakres, w jakim sprawuje on kontrolę nad procesem projektowania urządzeń jest naprawdę zdumiewająco szeroki. Ekspert d/s bezpieczeństwa, Ed Felten, [omawiał go już ponad rok temu na swojej stronie](#):

Przedstawicielom Hollywood (oraz innym posiadaczom praw autorskich) trzeba przedstawić dowody na to, że zastosowane zabezpieczenia naprawdę działają. Takie analizy na piśmie są wymagane od co najmniej trzech największych wytwórni Hollywood.

Tak więc, jeżeli projektujesz nowy system bezpieczeństwa, to nie możesz zamaryć o jego wsparciu przez Windows, jeżeli wcześniej nie wypowiedzą się w tej kwestii tacy specjaliści od zabezpieczeń jak [Disney](#), [MGM](#) czy [20th Century Fox](#). Zaskakujące, że takie kwiatki można znaleźć w dokumencie technicznym Microsoftu, bo oznacza to że studia filmowe mogą kształtować stan zabezpieczeń systemu komputerowego.

Za przykład takiej "zasady jakości" niech posłuży wytyczna, która zezwala się na jedynie określone sposoby projektowania urządzeń, co ma na celu utrudnienie osobom trzecim dostępu do elementów elektronicznych. Prawdopodobnie po raz pierwszy w historii projektowania układów elektronicznych nie jest już podporządkowane wypracowanym przez lata dobrym zwyczajom projektowym, fizycznym ograniczeniom wydajności w odprowadzaniu ciepła ale życzeniom przemysłu wcale nie komputerowego. Pomijając już ból głowy projektantów, takie założenie naraza też na dodatkowe koszty producentów tych urządzeń, koszty które nie są związane tylko i wyłącznie z produkcją nieoptymalnie zaprojektowanych układów. Producenci kart graficznych na przykład przygotowują tylko jeden projekt (który w dodatku nie odbiega zbytnio od modeli referencyjnych - [na tym zdjęciu widać że pięć różnych kart może różnić się jedynie logiem producenta i zastosowanym wentylatorem](#)), służący potem jako baza dla wszystkich produktów z danej serii. Widać to gołym okiem na tanich kartach graficznych, które w celu ograniczenia wydajności często mają po prostu przerwane niektóre ścieżki, co potem łatwo naprawić za pomocą ołówka.

Przykład zubożonej karty wyższej klasy, która dzięki temu może być sprzedawana taniej można

znaleźć [choćby na tej stronie](#). Zwróćcie uwagę na duży, czerwony i prostokątny obszar w lewej części karty - jest to miejsce po elemencie usuniętym z płytki w celu zmniejszenia kosztów urządzenia. Ślady po podobnym zabiegu widać na [zdjęciu tej karty](#). I przeciwnie, [to zdjęcie](#) pokazuje kartę “z górnej półki” zawierającą dodatkowe podzespoły. Układ znajdujący się na lewo od układu chłodzącego zajmuje się kodowaniem strumienia wideo - jak widać można go usunąć by zaoferować tańszą wersję całości. Podobne zabiegi stosuje przemysł motoryzacyjny - model każdego samochodu ma swoją wersję podstawową, którą można następnie wzbogacać o dodatkowe opcje, dobierane wedle uznania.

Bywa i tak, że dodanie kilku obwodów nie jest podyktowane chęcią rozróżnienia modeli na rynku, ale jest niezbędne do prawidłowego działania urządzenia. Większość najnowszych kart graficznych posiada podwójne wyjścia video, a te najdroższe mają nawet podwójne wyjścia DVI. Niestety, wiele kart posiada jedynie jedną linię TMDS, konieczną do prawidłowego działania złącza DVI. Drugie złącze obsługiwane jest za pomocą portu DVO pracującego wspólnie z zewnętrznym przekaźnikiem. Niektóre wyświetlacze HD potrzebują jednak wielu linii DVI/TMDS, bowiem pojedyncze połączenie nie zapewnia odpowiedniej przepustowości koniecznej do przesyłania obrazu wysokiej rozdzielczości. Można to zobaczyć na własne oczy na [zdjęciu karty, która posiada dwie linie TMDS](#) a która została zaprojektowana specjalnie do obsługi 30-calowego monitora Cinema Display firmy Apple. Teraz uwaga: z punktu widzenia systemu zabezpieczeń Visty pojęcie “zewnętrzny przekaźnik TMDS” nie istnieje, jako że taki układ ma bezpośredni dostęp do sygnału video wysokiej rozdzielczości i nie spełnia “wymagań jakości” stawianych przez projektantów Microsoftu. Zabawne, bo to z reguły właśnie duże wyświetlacze LCD są reklamowane jako idealne do oglądania nagrań wysokiej rozdzielczości.

Jest to pułapka, z której nie ma ucieczki. Teoretycznie można ratować się urządzeniem przetwarzającym sygnały DVI na HDMI (z HDCP) (w oparciu o układy Silicon Image Sil139x lub Sil193x szeroko stosowane w kartach graficznych), HDMI nie dysponuje jednak wystarczającym pasmem przesyłowym by transportować dane w takiej rozdzielczości. Nawet bez interwencji systemu ochrony treści, przesyłanie danych via HDMI samo w sobie spowoduje spadek jakości sygnału a karty graficzne, które będą zawierały port HDMI będą droższe - czyli klient będzie płacił więcej za sprzęt powodujący utratę jakości.

System ochrony treści stosowany w Viście zrywa zatem ze tym zwyczajem projektowania uniwersalnych układów i zabrania stosowania dodatkowych opcji. Każde urządzenie musi być “szyte na miarę”, musi być oddzielnie projektowane aby spełnić wymagania redukcji niepotrzebnych elementów i ścieżek, z których można by było skorzystać w celu uzyskania dostępu do sygnału.

Te obostrzenia nie dotyczą oczywiście tylko konstrukcji samej karty, ale również procesu projektowania poszczególnych układów scalonych. Nie można tak po prostu dodać układu DVI - musi być on zintegrowany z układem graficznym. Producenci sprzętu są zatem zmuszeni do projektowania wielkich, skomplikowanych, “wszystkomogących” jednostek graficznych, mimo że nabywca nie jest zainteresowany dodatkowymi opcjami.

Dalsze przykłady wpływu firm trzecich na proces projektowy producentów sprzętu można odnaleźć w dokumencie, który opisuje, co się dzieje ze sprzętem, który udało się w jakiś sposób “przechytryć”, choć wcześniej został uznany za spełniający warunki “zasad jakości”:

Dostawca powinien niezwłocznie przeprojektować produkt dotknięty wadą [...] jeżeli takie działanie nie jest możliwe lub jest niepraktyczne, powinien wstrzymać produkcję i dystrybucję tego urządzenia.

Wygląda na to, że choćbyś nie wiadomo jak się starał, to i tak nic ci to nie pomoże w sytuacji, gdy twój wyrób zostanie “złamany”. Kilka lat temu mój przyjaciel pracował w firmie, która przygotowywała system IT dla pewnego klienta ze sfer rządowych. Kiedy zapadła decyzja o wycofaniu się z kontraktu, wszyscy upoważnieni przedstawiciele klienta udali się nagle na zwolnienia lekarskie - wszystko po to, aby nie musieć podpisywać się pod tym dokumentem. Wyobrażam sobie dzień, w którym plaga dotknie pracowników ATI, nVidii, Intelu, VIA czy SiS - będzie to dzień, w którym trzeba będzie się podpisać pod dokumentem dającym prawo wtrącania się Hollywood w

proces produkcji, dystrybucji i sprzedaży ich urządzeń.

## **Zwiększenie kosztów związane z licencjonowaniem własności intelektualnej firm trzecich**

W przeciągu ostatnich sześciu-ośmiu miesięcy ponieśliśmy więcej kosztów związanych z prawami autorskimi, niż kiedykolwiek wcześniej. Każda umowa wprowadza nowe precedensy, każdy z nich opiera się na swoim poprzedniku - ATI

Ochrona jakże cennych "treści kwalifikowanych" wymaga stosowania wielu dodatkowych technologii. Pech chce, że wiele z nich jest chroniona prawem autorskim i wymaga zawierania nowych umów licencyjnych. Na przykład HDCP dla HDMI to zastrzeżone rozwiązanie [Intel](#), więc każdy producent projektując urządzenie zdolne przesyłać "bezpieczny" sygnał przez to złącze musi zapłacić opłatę licencyjną. Inny przykład: algorytm -128 nie jest dość wydajny by zapewnić płynne szyfrowanie danych w takich ilościach, więc znów trzeba zapłacić Intelowi, tym razem za prawa do stosowania szyfru kaskadowego, transformacji opartej na AES-128, która zapewnia podobny poziom bezpieczeństwa przy zmniejszonym zapotrzebowaniu na moc obliczeniową.

Licencjonowane są zresztą nie tylko rozwiązania sprzętowe. W celu zademonstrowania swojej gotowości do ochrony praw autorskich, Microsoft wprowadził do specyfikacji zalecenie, które zobowiązuje dostawców sprzętu do zaopatrywania swoich sterowników z rozwiązania znane dotychczas tylko autorom wirusów - chodzi o techniki ukrywania kodu. Te zabiegi mają na celu utrudnienie procesu "inżynierii wstecznej" oraz uniemożliwienie zakłócania pracy sterownika. Twórcy odpowiednich narzędzi - jak Cloakware czy Arxan - wyczuli znakomitą okazję do zarobienia pieniędzy i oferują na swoich stronach rozwiązania skierowane do producentów sterowników. Ci ostatni niezbyt się cieszą na myśl, że oprócz niełatwego przecież zadania napisania oprogramowania prawidłowo i niezawodnie obsługującego sprzęt muszą się jeszcze borykać z "ubogaceniem" go o obce im do tej pory technologie "wirusopodobne".

Zasady narzucone przez Microsoft komplikują również proces wsparcia technicznego. Sterowniki nie mogą być wyposażone w żadne mechanizmy ułatwiające proces debuggowania. Użytkownikom XP zapewne nie raz zdarzyło się widzieć komunikat systemowy oznajmiający, że jakaś aplikacja niespodziewanie zakończyła pracę. Komunikatowi temu towarzyszyła propozycja przesłania danych uzyskanych w procesie automatycznego debuggingu - wszystko po to aby ułatwić i przyspieszyć opracowanie stosownej poprawki. Niektórzy dostawcy sprzętu opracowali zresztą swoje własne narzędzia zgłaszające takie błędy (np. VPU Recover firmy ATI). W związku z tym, że taka właściwość sterownika może doprowadzić do "wycieku" chronionych treści, lub do ujawnienia istotnych danych dotyczących jego pracy, w przypadku urządzeń audio/video nie może być ona stosowana, co oczywiście stawia ich producentów w gorszej sytuacji. Jeden z menedżerów firmy ATI określił nawet koszty związane z utrudnieniem procesu usprawniania oprogramowania jako potencjalnie najwyższe spośród wszystkich wprowadzanych wymogami specyfikacji.

## **Zwiększone zapotrzebowanie na moc procesora**

Ponieważ szyfrowanie danych pochłania dodatkowe cykle procesora, dostawca OEM może być zmuszony do zwiększenia wymagań dotyczących klasy . Ten koszt ostatecznie ponosi nabywca multimedialnego peceta - ATI

Windows Vista wprowadza wymóg szyfrowania całej transmisji na szynie systemowej (przykładowo, dane przesyłane do układów graficznych muszą być szyfrowane algorytmem AES-128). Mało tego, szyfrowana musi być również komunikacja pomiędzy programami. Integralność i autentyczność komunikatów wymienianych pomiędzy aplikacjami działającymi w przestrzeni użytkownika i przestrzeni jądra jest zapewniana przez , co odbija się na prędkości tych połączeń. Procedura nawiązywania połączenia wygląda następująco:

sterownik -> aplikacja: certyfikat + jednorazowy znacznik

```
aplikacja -> sterownik: RSA-OAEP-SHA512( znacznik || klucz || nrsekw1 || nrsekw2 )
```

W tym kroku sterownik wysyła swój certyfikat do aplikacji zgłaszającej żądanie połączenia za pomocą procedury `DxgkDdiOPMGetCertificate()` i dołącza jednorazowy identyfikator wywołując procedurę `DxgkDdiOPMGetRandomNumber()`. Jest to certyfikat (stosowany w XP) lub (stosowany w Viście). Istnieje też trzeci typ certyfikatu, którego używają sterowniki posiadające dostęp do UAB (User-Accessible Bus). Certyfikat wymieniany między sterownikiem i aplikacją zawiera klucz RSA o długości 2048 bitów, który używany jest do zaszyfrowania 40-bitowego znacznika, 12-bitowy klucz sesji oraz dwa losowe, 32-bitowe numery sekwencyjne. Pierwszy z nich używany jest do przesyłania wiadomości statusu z wykorzystaniem `DxgkDdiOPMGetInformation()` a drugi do wysyłania komend poprzez `DxgkDdiOPMConfigureProtectedOutput()`.

Gdy klucze zostaną już wymienione, każdą z funkcji wywołuje się poprzez:

```
in = OMAC( znacznik || nrsekw || dane )  
out = OMAC( znacznik || nrsekw || dane )
```

(Użyłem konwencjonalnego zapisu “bity w szeregu”, choć w rzeczywistości poszczególne wartości są polami struktury). To rozwiązanie bardzo podobne, jak to, które zastosowano w czy (w praktyce pominięto niektóre kroki, jak negocjacja szyfru, bo w tym przypadku szyfry są z góry ustalone). Odkrycie, że oto aplikacje działające w pamięci komputera porozumiewają się poprzez coś w rodzaju SSL jest naprawdę dziwnym uczuciem.

Od dawna wiadomo że procesorowe szyfrowanie łączności jest jednym z najgorszych rozwiązań, jakie można zastosować w celu zapewnienia bezpieczeństwa danych. Już dwadzieścia lat temu inżynierowie IBM stwierdzili że szyfrowane szyny systemowe są po prostu niepraktyczne (odpowiednie opracowanie można znaleźć w pochodzących z 1987 roku materiałach sympozjum poświęconego bezpieczeństwu i prywatności - IEEE Symposium on Security and Privacy).

W celu utrudnienia życia włamywaczom każdy sterownik musi co 30ms (dla wyjść cyfrowych, dla analogowych co 150 ms) wysyłać sygnał kontrolny do nadzorowanego przez siebie sprzętu. Oznacza to, że nawet wtedy, gdy w systemie nie dzieje się absolutnie nic, cała gromada sterowników musi się uaktywniać trzydzieści razy na sekundę tylko po to, żeby upewnić się... że nic się nie dzieje (Leo Laporte w podkaście Stevena Gibsona [“Security Now”](#) nazywa Viście “paranoicznym systemem operacyjnym”. Są jeszcze dodatkowe wymagania, uzależnione od sprzętu. Vista sprawdza na przykład “bity spustowe” karty graficznej co każdą przesłaną ramkę obrazu. Docierają do mnie informacje o problemach w odtwarzaniu obrazu i dźwięku nawet na bardzo wydajnych systemach.[1] Z czasem okaże się, czy problem ten spowodowany jest przez niedopracowane sterowniki, czy też jednak jest efektem działania systemu ochrony treści. Stopień skomplikowania procesu obsługi mediów w nowym systemie Microsoftu łatwo sobie uzmysłowić zapoznając się z diagramem przedstawiającym. Składa się na niego jedenaście elementów, z czego tylko dwa (sterowniki audio i video) służą do przedstawiania treści. Przeznaczeniem pozostałych dziewięciu jest ochrona danych.

Zintegrowane z płytami głównymi karty graficzne stwarzają dodatkowy problem - odtwarzany materiał przechowują przecież w pamięci systemowej, skąd mogą być przeniesione do pliku wymiany. W celu ich ochrony Vista oznacza strony pamięci przechowujące dane audio/video za pomocą specjalnego bitu, który zmusza system do zaszyfrowania ich przed przeniesieniem na dysk i powtórne odszyfrowania przy wczytaniu do pamięci. Vista traktuje w ten szczególny sposób jedynie dane będące obiektem zainteresowania systemu ochrony treści - bez żadnych problemów przeniesie do pliku wymiany na przykład nieszyfrowane PIN-y Waszych kart kredytowych. Wygląda na to, że dla Microsoftu ramka filmu HD ma większe znaczenie niż poufne dane użytkownika.[2]

Co jeszcze przynosi realizowana przez Microsoft strategię całkowitego odcięcia użytkownika od chronionych danych? Na przykład to, że dekompresja filmów przez procesor nie jest już możliwa, żaden bowiem sprzęt nie poradzi sobie jednocześnie z dekompresją i szyfrowaniem. Zadanie to zostanie więc przerzucone na układ graficzny, który będzie musiał umieć się uporać przynajmniej z , kompensacją ruchu w oraz microsoftowym kodekiem VC-1. Czasy tanich kart graficznych bez

dekodera video mamy już za sobą.

Nieemożność dekodowania strumienia wideo na drodze programowej oznacza również, że żaden algorytm kompresji nie obsługiwany przez dekodery sprzętowe nie będzie miał racji bytu. Gdyby na przykład [Ogg](#) został kiedyś jakimś cudem użyty jako format przesyłania danych HD, to powinien używać kodeka w rodzaju Windows Media VC-1, bo inaczej nie ma szans w nowym systemie Microsoftu i na sprzęcie "Vista Ready". Problem ma również cyfrowe kino wysokiej jakości (D-Cinema), które bazuje na Motion 2000, ponieważ MPEG i jego odpowiedniki nie zapewniają odpowiedniego poziomu jakości obrazu. Jako że JPEG2000 używa kompresji bazującej na teorii falek (wavelet-based compression) a nie - tak jak MPEG - na , to na kartach nie obsługujących tego algorytmu nie będzie możliwe odtworzenie filmów w tym standardzie. Pamiętajmy, że *wszystkie* filmy D-Cinema będą "treściami kwalifikowanymi" - czyli że na Viście nie będzie można ich odtworzyć dopóty, dopóki w nieokreślonym momencie w przyszłości nie pojawią się karty graficzne wspierające takie operacje. Porównajmy to z sytuacją z filmami MPEG, gdzie właśnie kodeki programowe, jak XingMPEG, w praktyce otworzyły i zbudowały rynek dla "video na PC". Dziś taka historia nie ma prawa się powtórzyć - a to wszystko dzięki systemie ochrony treści Microsoft Vista.

Topowe rozwiązania audio i video skierowane są głównie do graczy, tylko oni bowiem są w stanie wydać spore sumy za cenę uzyskania najmniejszego przyrostu wydajności, kupując na przykład za 250 dolarów kartę sieciową "Killer " firmy Bigfoot Networks z nadzieją, że ta zmniejszy o kilka milisekund opóźnienia przy grze on-line. To właśnie gracze kupują kosztujące od 500 do 1000 dolarów karty graficzne i dźwiękowe - a firmy je produkujące na każdym takim urządzeniu zarabiają więcej, niż na kilkudziesięciu tanich urządzeniach wbudowanych w płyty główne. Ciekaw jestem, jak ci ludzie zareagują, gdy uzmysłowią sobie co Vista wyrabia w tle z ich cackami i jak to się odbija na wydajności tego sprzętu.

---

Przypisy:

1. Informacje, które do mnie dotarły wskazują, że naprawdę stabilne sterowniki firm trzecich pojawią się dopiero w połowie 2007 roku. Dostawcy są zdesperowani, by mieć je gotowe w chwili premiery Visty, choć nie udało im to w chwili skierowania nośników do tłoczenia, więc to oprogramowanie trzeba będzie pobierać z internetu. Wtedy sterowniki te określano mianem "w najlepszym razie wersji beta", więc na pewno usłyszymy o tym opóźnieniu po premierze nowego systemu Microsoftu. [[↔](#)]
2. Takie szyfrowanie wspierały będą wersje Enterprise i Ultimate ale z tego dobrodziejstwa nie będzie miał szansy skorzystać przeciętny użytkownik. W dodatku jest to szyfrowanie typu "wszystko albo nic", któremu podlegają wszystkie pliki systemowe i użytkownika, gdy tymczasem najważniejszy jest plik wymiany, tam bowiem trafiają naprawdę cenne dane. Właściwym rozwiązaniem problemu jest tu technika stosowana w OpenBSD, który podczas startu generuje losowy klucz, którym następnie szyfruje wszystkie dane trafiające do partycji wymiany. [[↔](#)]

## Zwiększony stopień skompilowania urządzeń

Specyfikacja wymaga od nas szyfrowania danych. Ten wymóg oznacza konieczność wprowadzenia dodatkowej logiki odpowiedzialnej tylko za ten fragment działania urządzenia i zwiększa koszty układu. Koszty te przenoszone są na naszych klientów - ATI

Jak już wspominałem wyżej, karty graficzne w Windows Vista muszą obsługiwać szyfrowanie transmisji algorytmem AES-128. Operacja ta musi przebiegać na poziomie procesora graficznego, co w praktyce oznacza wyrzucenie jednego albo dwóch potoków i przeznaczenie wolnego miejsca na "maszynę szyfrującą".

Uzyskanie klucza AES wymaga kolejnego "kryptograficznego narzutu", w tym przypadku obsługi posługującego się kluczem o długości 2048 bitów algorytmu Diffiego-Hellmana, który jest potem - z

użyciem haszowania Davisa-Meyera - konwertowany do stosowanego przez AES klucza 128-bitowego. W urządzeniach programowalnych można to uzyskać metodą trudniejszą - na przykład posługując się jednostką przetwarzającą shadery, lub łatwiejszą - wyrzucając kolejne potoki i wbudowując w to miejsce logikę obsługującą kryptografię z wykorzystaniem klucza publicznego.

Nie trzeba chyba nikogo przekonywać jak na ostateczny koszt urządzenia wpłynie konieczność przygotowania, przetestowania i zintegrowania elementów kryptograficznych w kartach audio/video. Nie trzeba też chyba wielkiej wyobraźni, żeby uzmysłowić sobie jak odbije się to na wydajności tych urządzeń - a to wszystko po to, żeby system ochrony treści mógł sprawnie działać.

Koszty, jakie system ponosi w związku z obsługą zabezpieczeń "treści kwalifikowanych" są jeszcze lepiej widoczne w przypadku urządzeń przenośnych. Jak stwierdza serwis CNET przy okazji [testu takiego sprzętu](#): "DRM nie tylko spowalnia odtwarzacz, ale zwyczajnie wysysa z niego życie". Jak wykazały testy moc zużywana na obsługę DRM skraca życie baterii o około 25%. Zabezpieczenia tego typu odbijają się też negatywnie na prędkości działania gier. Gra "[Flatout 2](#)" w wersji z zabezpieczeniami [działa o 15% wolniej niż ta sama gra pozbawiona DRM](#).

## Uwagi końcowe

Nawet najlepiej przebiegająca współpraca na nic się nie zda, jeżeli nie podporządkujemy jej potrzebom konsumentów. Microsoft uważa, że doznania użytkowników są kluczowym elementem dla dobrego przyjęcia tych rozwiązań przez rynek" - Microsoft

Przemysł PC jest zdeterminowany aby zapewnić tej platformie właściwy system ochrony treści. Nie ma jednak niczego za darmo - w tym przypadku koszty poniosą konsumenci-ATI

Po zapoznaniu się z powyższym tekstem na usta ciśnie się jedno pytanie: "Dlaczego Microsoft z własnej woli pakuje się w takie kłopoty?" Zapytajcie kogokolwiek, co oznacza dla niej/dla niego pojęcie "odtwarzacz HD". Usłyszycie "nagrywarka DVD" lub "odtwarzacz DVD" ale w żadnym wypadku nie "komputer osobisty". Skąd więc takie parcie na zrobienie z PC czegoś, czym nie jest?

W lipcu 2006 roku Cory Doctorow opublikował [analizę ograniczającego konkurencję a stosowanego przez Apple w iTunes systemu zabezpieczeń przed kopiowaniem](#). Jedyńm powodem, który przychodzi mi na myśl a który spowodowałby, że Microsoft zdecyduje się na narażenie swoich programistów, producentów sprzętu, twórców oprogramowania i w końcu również użytkowników na takie problemy jest przejęcie kanału dystrybucji cyfrowych mediów wysokiej jakości. Tak samo, jak [Apple](#) uzyskał monopolistyczną pozycję na rynku sprzedaży muzyki (pamiętacie [Motorolę ROKR](#), która była tak okaleczona przez Apple, że właściwie już w dniu premiery niezdatna do użytku?), tak Microsoft stara się o zmonopolizowanie obrotu mediami następnej generacji. Pierwsze objawy "zamykania" cyfrowych mediów przez Windows są już widoczne. Osoby, które przesiadły się na nowy system Microsoftu zaczynają zdawać sobie sprawę, że ich legalnie nabyte nośniki [nie będą pod nim odtwarzane](#) (przytoczony tu przykład jest szczerze mówiąc przerażający, bo nagranie zawarte na nośniku odtwarzać można jedynie przez pewien okres, więc co jakiś czas trzeba je ponownie kupować; w dodatku w związku z tym, że nie można wykonać kopii praw do niego, to w wypadku awarii dysku trzeba je kupić raz jeszcze). Wydaje się zatem jasne, dlaczego Microsoft decyduje się przejść piekło żeby wdrożyć zaprojektowany przez siebie system - jego sukces oznacza licencję na drukowanie pieniędzy.

Firma z Redmond będzie miała nie tylko możliwość dobierania sobie konkurentów na tym rynku, ale też zyska instrument wpływu na dostawców treści, tak samo jak Apple szantażuje swoich dostawców - "albo gracie naszymi kartami, albo w ogóle nie siadacie do stołu". Rezultatem będzie monopol o takiej skali, że dzisiejsza dominacja Windows jest przy nim doprawdy nic nie znaczącym zjawiskiem[1].

Wielce "upierdliwa" natura windowsowego systemu ochrony treści będzie skłaniała użytkowników do usuwania lub obchodzenia zabezpieczeń tylko po to, żeby móc skorzystać z legalnie zakupionego

nośnika. Widać to wyraźnie w [sekcji "Cytaty"](#) i w przypisach tego opracowania, gdzie użytkownicy są zmuszani do przełamywania zabezpieczeń mimo że nie są piratami - chcą tylko obejrzeć kupiony przez siebie film. Windows Vista stać się więc może największą zachętą do piractwa, jaka do tej pory istniała. Vista otwiera potężny rynek dla producentów przeróżnych dodatków, które będą służyły do unieszkodliwiania zabezpieczeń - tak samo, jak istniejące obecnie odtwarzacze DVD nie przejmujące się regionami DVD. Być może Hollywood powinien wziąć pod uwagę radę, którą słycać w jednej z najbardziej znanych jego produkcji: The more you tighten your grip, the more systems will slip through your fingers (Im bardziej zaciskasz dłoń, tym więcej systemów ucieka Ci między palcami - [księżniczka Leia](#), [Gwiezdne Wojny, Epizod IV](#)).

Podsumowując: system ochrony treści Windows Vista wydaje się być niezwykle krótkowzrocznym tworem, skoncentrowanym wyłącznie na zapewnieniu ochrony określonym danym, zaprojektowanym bez zwracania uwagi na problemy, które powoduje. To trochę jak pecetowa wersja (zarzuconego na szczęście) pomysłu dołączania do europejskich banknotów o dużych nominałach transponderów. Miało to ograniczyć fałszerstwa a groziło paradoksem - największy pożytek z tej technologii mieliby złodzieje, którzy mogliby zdalnie typować miejsca kradzieży.

Zmarnotrawiono olbrzymie zasoby ludzkie i finansowe w niewłaściwym celu. Microsoft twierdzi na przykład, że Vista będzie ich najbezpieczniejszym systemem, ale czy przypadkiem nie twierdzą tak przy każdej premierze, od kiedy bezpieczeństwo systemu stało się istotnym czynnikiem wpływającym na wybór klientów? Kto wierzy, że Vista nie stanie się następnym nosicielem dla "złośliwego oprogramowania" chwilę po tym, jak stanie się publicznie dostępna? Co jednak, gdyby energię włożoną w rozwój zabezpieczeń filmów i muzyki włożono w zabezpieczenia przeciwko programom malware i spyware? Zamiast oddzielnej warstwy zabezpieczeń dla "treści kwalifikowanych" mielibyśmy taką warstwę chroniącą nasze poufne dane. Zamiast specjalnych technik zabraniających użytkownikom debuggowania oprogramowania mielibyśmy inne techniki, tym razem powstrzymujące inne oprogramowanie przed ukrytym "podczepianiem" się pod system operacyjny. Tą listę można rozwijać dalej, wiele bowiem zrobiono dla DRM, czego nie udało się zrobić dla bezpieczeństwa użytkownika. Marnotrawstwo. Zwyczajne marnotrawstwo.

Najgorsze jest jednak to, że nie ma dokąd uciekać. Producenci sprzętu będą musieli wypić to gorzkie piwo, bowiem jak twierdzi specyfikacja "Nie zmuszamy nikogo do podpisywania licencji zobowiązującej do ochrony treści kwalifikowanych. Trzeba jednak pamiętać, że sterownik bez certyfikatu nie będzie otrzymywał od systemu operacyjnego żadnych danych o wysokiej jakości".<sup>[2]</sup> Będąc producentem sprzętu możesz oczywiście wybrać niezależność od Microsoftu, ale pod warunkiem, że nie będzie Ci przeszkadzał fakt, że Twoje urządzenie odtwarza obraz czy dźwięk o gorszej jakości niż konkurencja.

Premierę Visty odczują też użytkownicy innych systemów operacyjnych. Nieważne czy używacie Windows XP, Windows 95, Linuksa, FreeBSD, OS X czy Solarisa - ceny urządzeń pójdą w górę a same urządzenia staną się mniej stabilne, trudniejsze do zaprogramowania, mniej odporne na ataki, mniej kompatybilne. Windows dominuje na rynku, więc producenci nie będą tworzyć dwóch wersji tego samego sprzętu a użytkownicy innych systemów w ten czy inny sposób zapłacą za system ochrony treści Windows pomimo tego, że go nie użyją.

Mam ofertę dla Microsoftu: jeżeli my, konsumenci, obiecamy że nigdy, przenigdy nie kupimy jakiegokolwiek zabezpieczonego nośnika HD, to wy wycofacie się ze swoich pomysłów na utrudnianie nam życia? Prosimy?

---

Przypisy:

1. Odtwarzanie nagrań audio i wideo to nie jedyne dziedziny, w których Vista popada w paranoję. Artykuł serwisu Gamasutra "[Vista Casts A Pall On PC Gaming](#)" analizuje nową "cechę" Visty, która pozwala na kontrolę gier, jakie można uruchamiać na danej maszynie. Każdy producent gier, którego nie stać na bardzo kosztowny rating musi się pogodzić z tym, że jego produkt będzie traktowany jako "nie sklasyfikowany", co jest odpowiednikiem

oznaczenia “tylko dla dorosłych” w świecie filmu (wielokrotnie nagradzany [“Nocny kowboj”](#) miał kiedyś takie oznaczenie). Oczywiście każdy rodzic od razu zablokuje możliwość uruchamiania gier tak oznaczonych, więc mali, niezależni wydawcy, którzy ze względów finansowych nie mogą sobie pozwolić na wystąpienie o rating będą z góry skreśleni. To kolejna “cecha” Visty, która w przyszłości może poważnie zaangażować prawników Microsoftu. [↵]

2. Jeżeli kiedykolwiek chciałbym odtworzyć materiał HD, poczekałbym kilka lat i kupił za pięćdziesiąt dolarów wyprodukowany w Chinach odtwarzacz a nie wydawał 1000 dolarów za komputer z Vistą na pokładzie. Jest coś dziwnego w tym, że najbliżsi dostawcy rozumiejący potrzeby klientów znajdują się aż w Chinach. Rozwiązaniem problemu “treści kwalifikowanych” (dokonanym drogą *reductio ad absurdum*, ale zawsze), jest propozycja jednego z czytelników serwisu Slashdot, który wnosi o dodanie do systemu obsługi “czarnej skrzynki”, która na wejściu przyjmuje zaszyfrowany materiał HD a na wyjściu podaje zaszyfrowany (czy w inny sposób zabezpieczony) odkodowany materiał HD. Innymi słowy: należy przenieść cały sprzęt, sterowniki i inne oprogramowanie do urządzenia, które będzie montowane jedynie w komputerach typu “media PC”, gdzie będzie prawdopodobnie miało rację bytu. Porównajmy teraz tą “przystawkę” do chińskiego odtwarzacza za 50 dolarów. Po co ktokolwiek miałby ją kupować (za cenę zapewne większą niż 50 dolarów) do swojego i tak drogiego komputera, skoro może kupić odtwarzacz potrafiący to samo a nawet więcej? [↵]

## Podziękowania

Dokument ten powstał dzięki pomocy wielu osób, wiele z nich prosiło o anonimowość. Miejscami uprościłem lub zmieniłem treść fragmentów dokumentów, w których posiadanie wszedłem, a które nie mogą być upublicznione. Ponieważ nie zawsze miałem możliwość dotarcia do źródeł i zweryfikowania szczegółów, moje opracowanie może zawierać pewne nieścisłości, o których zapewne wkrótce się dowiem. Bez wątpienia pierwszy zauważył je Microsoft, który nie chce oczywiście, żeby pogląd “Vista jest systemem wadliwie zaprojektowanym już u samych podstaw” mógł się upowszechnić.

Byłbym wdzięczny za kontakt zarówno z pracownikami Microsoftu zaangażowanymi w opracowanie systemu ochrony treści, jak i producentami urządzeń, których ten system dotyczy. Od swoich źródeł w Microsoftzie wiem, że wielu pracownikom tej firmy naprawdę zależy na jak najlepszej jakości podsystemu audio/video. Są oni sfrustrowani posunięciami swojego pracodawcy, które nakazują im poświęcanie czasu na rozwijanie zabezpieczeń treści, mimo że i bez tego ich zadanie jest wystarczająco skomplikowane. Jestem otwarty na wszelkie uwagi, zobowiązuję się też do zachowania w tajemnicy źródeł informacji. Jeżeli obawiacie się zdemaskowania, załóżcie konto pocztowe na serwerach w rodzaju Yahoo i Gmail. Jeżeli boicie się identyfikacji na podstawie numeru IP maszyny, z której łączycie się z serwerem pocztowym, skorzystajcie z kafejki internetowej. Zainteresowani mogą pobrać moj klucz (z mojej strony domowej).

(W razie gdyby powyższe wskazówki nie były dość oczywiste - jeżeli pracujecie dla nVidii, ATI, VIA, SiS, Intela, ..., byłbym *naprawdę* wdzięczny za informacje o tym, jak Vista wpływa na Waszą działalność)

## Źródła

Ponieważ dokument ten powstał jako rozwinięcie pewnej dyskusji prowadzonej za pomocą poczty elektronicznej, niektóre ze źródeł nie mogą być upublicznione. Najlepsze ogólnodostępne źródła, jakie znam to:

- [“Output Content Protection and Windows Vista”](#),
- [“Windows Longhorn Output Content Protection”](#),
- [“How to Implement Windows Vista Content Output Protection”](#),
- [“Protected Media Path and Driver Interoperability Requirements”](#),

(Proszę pamiętać, że od czasu opublikowania tych informacji zmieniły się wymagania kryptograficzne. -1 zostało zastąpione przez SHA-256 i SHA-512 a klucze publiczne mają teraz długość 2048 bitów, zamiast połączenia kluczy 512- i 2048-bitowych, o których mowa w prezentacjach).

Doskonałą analizą jest dokument pochodzący od ATI pod tytułem [“Digital Media Content Protection”](#). Wskazuje on na problemy związane z implementacją systemu ochrony treści i wciąż wspomina o zwiększonych kosztach, zmniejszonej wydajności a zwrot “koszty przeniesione na konsumentów” przewija się przez całą prezentację jak mantra.

Dodatkowo, w sieci dostępnych jest kilka analiz podobnych do mojej, które nie są jednak aż tak szczegółowe. Przykładem może być jeden z “okładkowych” tekstów PC World’a [“Will your PC run Windows Vista?”](#), który zajmuje się systemem ochrony treści w rozdziale “Multimedia in chains”. Reakcje uczestników WinHEC na przedstawione przez Microsoft propozycje dostępne są na stronach EE Times ([“Longhorn: tough trail to PC digital media”](#), choć trzeba być subskrybentem, żeby móc ten tekst przeczytać (można poszukać w systemach gromadzących kopie stron internetowych). również przygotowała tekst dotyczący unieważniania sterowników: [“Protected Media Path, Component Revocation, Windows Driver Lockdown”](#).

## Użycie, modyfikacja i rozpowszechnianie

Dokument ten objęty jest licencją [Creative Commons Uznanie Autorstwa 2.5](#). Oznacza to, że możesz go kopiować, rozpowszechniać, wyświetlać oraz tworzyć utwory zależne pod warunkiem, że zamieścisz informację o autorze oryginału i link do tego opracowania ( podany jest na początku mojego tekstu).

[polskie tłumaczenie objęte jest identyczną licencją - przyp. tłumacza]

## Dodatki i przypisy

Ta bardziej “formalna” część tego pracowania kończy się właśnie tutaj. Następne sekcje zawierają różne nieformalne komentarze, przemyślenia oraz inne drobiazgi. Prawdopodobnie niewarte tłumaczenia, jeżeli ktoś się za nie zabrał.

[od tłumacza: nie ma mowy, pozostała część jest równie ciekawa; polecam ją wszystkim sceptykom]

## Mini-FAQ

Lektura tego dokumentu powoduje różne reakcje. Poniżej odpowiadam na najczęstsze zarzuty.

1. Kolejne walenie na ośle w Microsoft...

Nie, to walenie w złą technologię. Jeżeli tego samego dopuściłby się [Linus Torvalds](#), [Steve Jobs](#), [Alan Cox](#) czy [Theo de Raadt](#), zrobiłbym to samo. Jeżeli o mnie chodzi, komputerów używam jak narzędzi - chcę wykonać pewną pracę za ich pomocą, nie zaś angażować się w pseudo-religijne potyczki. Mój sprzeciw budzi określone postępowanie, nie zaś osoba w ten sposób postępująca. Dla informacji: używam w tej chwili systemu Windows na.... [liczę]... siedmiu moich komputerach, reszta napędzana jest przez Linuksa, FreeBSD i OpenSolaris. Kiepski ze mnie krytyk Microsoftu jako takiego, skoro używam ich systemu.

2. Tekst został napisany pod z góry założoną tezę

Być może, ale w takim razie niech ktoś inny zapozna się z dokumentami, do których linkuję w [sekcji “Zródła”](#) i po tej lekturze napisze pozytywną recenzję. Ktoś musiał powiedzieć to głośno - padło na mnie. Sądzę jednak, że każdy kto dysponuje odpowiednią wiedzą, doszedłby do podobnych wniosków.

3. Jeden wielki

Komentarze takie jak ten powstają z trzech powodów powodów (1)szybkiego przebieżenia wzrokiem po tekście, nie wgłębiając się w szczegóły, (2)założenia z góry, że dokument jest niewiarygodny,

często bez zaliczenia nawet punktu 1, (3)z czystej przekory. Weźmy za przykład komentarz jednego z użytkowników serwisu [Digg](#) - dotyczy on uwagi, że procesory nie radzą sobie z jednoczesną dekompresją strumienia wideo i zaszyfrowaniem go:

Przepraszam, skąd to wzięłeś? Doskonale wiesz, że nie masz na to żadnych dowodów i najprawdopodobniej się mylisz? Cały następny paragraf opiera się na tym założeniu, wyciągniętym wprost z kapelusza. [...] Nie jestem fanem DRM, ale scenariusze przez ciebie kreślone i zgłaszane postulaty to kompletna bzdura.

No to zajrzyjmy do pierwszego z brzegu źródła, żeby przekonać się, że twierdzenie to pochodzi od Microsoftu:

Problem ze stosowaniem AES jest taki, że każdy bajt danych wymaga około 20 cykli procesora. Jest to do przyjęcia w przypadku materiału skompresowanego lub skompresowanego częściowo, ale nieskompresowanemu materiałowi HD nie poradzi nawet współczesny procesor.

i dalej:

W przypadku materiału o wysokiej rozdzielczości płynne odtwarzanie zaszyfrowanego za pomocą AES i nieskompresowanego filmu będzie zależało od rozdzielczości obrazu i mocy procesora. Nie wydaje się, żeby układy dostępne w 2006 roku były w stanie zapewnić płynność odtwarzania.

Jeżeli nie wierzycie tym słowom, zajrzyjcie do dokumentów firmy i przekonajcie się na własne oczy. Jeżeli nadal uważacie to opracowanie za FUD, to przynajmniej będziecie wiedzieli, że nie ja to wymyśliłem.

#### 4. Microsoft działa pod przymusem przemysłu filmowego i muzycznego

“My tylko wykonujemy rozkazy” już dawno temu było kiepską wymówką, dziś ma się jeszcze gorzej. Dziwi mnie fakt, że o ile łatwo jest wieszać przysłowiowe psy na przemyśle, który na kozły ofiame pozwów sądowych wybiera sobie 12-letnie dzieci i 80-letnie babcie, o tyle nikt nie ma pretensji do Microsoftu. Wydawcom bardzo zależy na dotarciu ze swoim towarem na ekrany komputerów osobistych i Microsoft mógłby z łatwością odpowiedzieć “Mamy swoją wizję Visty, skoro się nie podoba, żegnamy. Nie mamy zamiaru psuć interesu sobie i naszym partnerom tylko po to, żeby robić wam dobrze”. Innymi słowy: mogli jasno powiedzieć Hollywood kto przy tym stole rozdaje karty.

Opiszę historię, jaka ma wydarzyła się, gdy to wydawcy próbowali rozdać talię. Około 10-15 lat temu firmy wydawnicze zakomunikowały nowozelandzkim stacjom telewizyjnym, że odtąd za każde odtworzenie teledysku należy się zapłata. Stacje oczywiście się nie zgodziły, argumentując że i tak za darmo reklamują ich produkt i jeżeli tak im to przeszkadza, to proszę bardzo - wstrzymujemy emisję teledysków. I wiecie co zrobili? Przestali je pokazywać, naprawdę.

Po kilku tygodniach wydawcy zdali sobie sprawę jak bardzo potrzebują kanałów telewizyjnych do promocji swojej muzyki. Jedna z takich firm wykupiła cały blok reklamowy w porze największej oglądalności (za bająką sumę zresztą) tylko po to żeby zaprezentować jeden(!) nowy teledysk.

Wkrótce potem teledyski wróciły do telewizji. Szczegółów porozumienia nigdy nie zdradzono, ale wyobrażam sobie, że widok kilku szefów największych firm muzycznych błagających na kolanach o zmiłowanie i odpuszczenie grzechów musiał być bardzo pocieszny.

Tak samo jest z Microsoftem. Przemysł rozrywkowy po prostu potrzebuje go bardziej, niż Microsoft przemysłu rozrywkowego. Twierdzenie, że tylko wykonują rozkazy, to przerzucenie odpowiedzialności - gdyby Microsoft nie zechciał przystać na ich warunki, to wydawcy musieliby wywiesić białą flagę. Nie można zrezygnować z 95% rynku, dokładnie tak, jak firmy muzyczne nie mogą sobie pozwolić na rezygnację z darmowej promocji w telewizji.

#### 5. Zagrożenia są przejawskrawione

Zawodowo zajmuje się bezpieczeństwem sytemów komputerowych. Moim zadaniem jest ocena bezpieczeństwa technologii komputerowych a tym przecież zajmuję się w tym opracowaniu. Gdybym pracował w marketingu, moim obowiązkiem byłoby zachwalanie systemu ochrony treści “zaszytego” w Viście. Niestety, nie pracuję w marketingu, dlatego też czytacie o zagrożeniach, jakie niesie za sobą ta technologia.

Jeżeli pójdziecie do prawnika i spytacie “Chcę zrobić X, jakie jest potencjalne ryzyko z prawnego punktu widzenia?”, dowiedcie się. Jeżeli udacie się do specjalisty do spraw bezpieczeństwa, dowiedcie się jakie zagrożenia dla bezpieczeństwa niesie to, co chcecie zrobić. Celem tej analizy jest poinformowanie potencjalnych nabywców Visty o zagrożeniach, jakie może nieść korzystanie z tego systemu - oni sami zdecydują, czy warto ryzykować. Niektóre z tych zagrożeń mogą wydawać się nie dość wyraźne, ale to wy zadecydujecie, czy ta wizja wam przeszkadza.

6. Wkurzasz się, bo nie będziesz już mógł sobie kraść filmów/muzyki w Viście

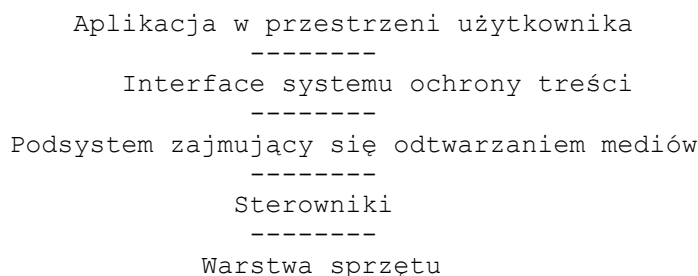
Serio, dostałem takiego maila. Jest na tyle śmieszny, że aż musiałem go tu zamieścić.

## Pytania bez odpowiedzi

Jest wiele otwartych pytań dotyczących systemu ochrony treści Visty, na które nie jesteśmy teraz w stanie odpowiedzieć. Takie odpowiedzi pojawią się być może za kilka miesięcy. To wtedy system zyska sensowną bazę użytkowników, którzy będą się mogli podzielić swoimi odczuciami. Dziś nikt nie jest do końca pewien jak działają niektóre elementy.

Pytanie 1.

Jak łatwo można obejść zabezpieczenia Visty? Przyjrzyjmy się diagramom widocznym w dokumentach źródłowych:



Ze specyfikacji wynika, że programy działające w przestrzeni użytkownika muszą odwołać się do interfejsu systemu ochrony treści w celu odtworzenia dowolnego pliku (jeden z dokumentów porównuje nawet aplikację do pilota służącego do obsługi systemu ochrony treści i podsystemu zajmującego się odtwarzaniem mediów). Pytanie brzmi: czy aplikacja może ominąć ten poziom “pośrednictwa” i odwołać się do procedur niższego poziomu? [Odpowiedzi](#), które można znaleźć na [forum Microsoftu](#) wskazują na to, że nawet używając nie-microsoftowych odtwarzaczy, jak programy nVidii czy [Cyberlinka](#) odtwarzanie czegokolwiek będzie niemożliwe, gdy (w tym przypadku) wygaśnie licencja na wersję trial Vista Media Center.

Pytanie 2.

Jak ta cała sytuacja odnosi się do użytkowników, którzy chcą przygotować własny materiał HD, zabezpieczony bądź nie? Jeżeli podstawową funkcją systemu ochrony treści jest zapewnienie, że dane wysokiej jakości nigdy nie opuszczą systemu, jak można przygotować własny materiał? Zważywszy na fakt, że Vista jest systemem wielozadaniowym, to gdy podczas przygotowywania takiego materiału gdzie indziej w systemie pojawi się inny materiał, którym zainteresuje się system ochrony treści, to czy materiał użytkownika nie ulegnie pogorszeniu w chwili, gdy zadziałają zabezpieczenia? Jak szeroki jest zakres działania tego systemu? Jeżeli jego oddziaływanie rozciąga się na konkretne zadanie (lub nawet na konkretny proces), to każdy mechanizm działający między sesjami lub procesami (jak na przykład “wstrzyknięcie” procesu do innego wątku) będzie w stanie obejść zabezpieczenie. Z drugiej strony, jeżeli Microsoft hołduje zasadzie “wszystkie twoje dane należą do

nas”, to jeżeli zadziała system ochrony treści, jednocześnie pogorszeniu ulegną wszystkie dane HD, nawet te przygotowywane przez użytkownika.

Pytanie 3.

Daj palec, wezmą całą rękę. Jeżeli mechanizmy DRM okażą się skuteczne, nie ma powodu dla których nie można by ich było użyć do ochrony każdego rodzaju treści. Bo niby dlaczego nie? Narzędzia są dostępne, czemu z nich nie korzystać? Znamy już tzw. “Enterprise DRM” (E-DRM), który ma za zadanie kontrolować dostęp do dokumentów Worda, PDF-ów czy plików systemów (jakieś dwadzieścia lat temu, gdy sukcesy święciła [Pomarańczowa Księga](#), podobna technologia nazywała się ORCON). Jeżeli DRM zostanie zintegrowany z Vistą na tak niskim poziomie nie wiadomo, jak rozwój tej technologii potoczy się w przyszłości. Bill Rosenblatt wydawca pisma “[DRM Watch](#)” przewiduje, że [obszarem największego wzrostu zapotrzebowania na Microsoftowy DRM będzie sektor korporacyjny](#). Jak w związku z tym będzie wyglądało korzystanie z komputera za kilka lat?

Pytanie 4.

Niejednokrotnie czytałem na sieci narzekania ludzi, którzy nie są w stanie odtworzyć płyt HD-DVD ani Blu-Ray ani na Viście, ani na XP (dostawałem też maile podobnej treści). Czy komuś to się udało? Czy ktoś potrafi odtworzyć na Windows materiał, który Vista uważa za chroniony? Jeżeli tak, to jakiego napędu używacie, jakim programem odtwarzacie te nagrania, jaką macie kartę graficzną i monitor?

(Dostałem wreszcie raport od osoby, której udało się odtworzyć krążek HD-DVD. Powiodło się to na konsoli Xbox360, karcie nVidia 8800GTX z HDCP (sprzęt z najwyższej półki sprzedawany w tej chwili za jakieś 600 dolarów) i wyświetlaczu Westinghouse 37w3 wyposażonym w HDCP na wejściu DVI (37-calowe LCD kosztujące obecnie jakieś 1200 dolarów)

## Odpowiedź Microsoftu

W połowie stycznia 2007 roku, [Microsoft odpowiedział na niektóre ze stawianych przeze mnie zarzutów](#). Część informacji była rzeczywiście nowa i interesująca (jak na przykład wyjaśnienie, jakie są skutki wycofania sterownika urządzenia), inne z kolei robią wrażenie przygotowanych przez [Waggener Edstrom](#) (firma zajmująca się Microsoftu) niż przez menedżera projektu, Dave’a Marsha ([The Inquirer również nie był pod wrażeniem](#)). Będę sukcesywnie wzbogacał główny tekst opracowania o informacje wynikające z tej wypowiedzi Microsoftu, ale na kwestie, które nie dotyczą bezpośrednio meritum sporu odpowiem w tym rozdziale. Ważnymi technicznymi uściśleniami były (1) określenie co faktycznie dzieje się w efekcie unieważnienia sterownika, (2) jak działają “bity spustowe” oraz (3) które fragmenty przekazu ulegają pogorszeniu w skutek zadziałania systemu ochrony treści. Specyfikacja była dość niejasna w tym względzie, więc dobrze, że w końcu udało się uściślić pewne dane.

## Czy takie techniki jak HFS będą miały wpływ na powstawanie sterowników o otwartych źródłach?

Nie. HFS używa innych charakterystyk poszczególnych układów, niż te, które są wykorzystywane przy pisaniu sterowników. Wymagania stawiane przez HFS nie powinny utrudnić dostępu do informacji, które są niezbędne do tworzenia takiego oprogramowania.

To twierdzenie stoi w sprzeczności z fragmentem [dokumentu tego samego autora](#), w którym czytamy:

Testy te mogłyby polegać na ładowaniu tekstury, poddawaniu jej przekształceniom przez układ graficzny i porównaniu wyników pikseli.

i następnie:

Szczegóły działania procesora graficznego muszą być utrzymywane w tajemnicy, tak aby osoba próbująca stworzyć emulator nie mogła uzyskać potrzebnych jej informacji.

Tak więc z dokumentu tego (będącego podstawowym źródłem informacji na temat systemu ochrony treści) wynika coś zupełnie przeciwnego, niż twierdzi teraz Microsoft. Po pierwsze HFS wykorzystuje podstawowe funkcje układu graficznego (renderowanie grafiki), po drugie szczegóły budowy sprzętu mają być ukryte, by uniemożliwić emulację programową.

### **Czy “zasady jakości” określone przez projektantów systemu wpłyną na zwiększenie kosztów kart graficznych i zredukują liczbę ich wariantów?**

Obecny trend i tak jest taki, że wszystkie funkcje są integrowane w jednym układzie, więc rekomendacje nie mają na ten proces żadnego wpływu. Jako że koszt (koszt układów w szczególności) jest determinowany przede wszystkim przez skalę produkcji, to właściwie lepiej jest unikać oferowania dodatkowych rozwiązań poprzez stosowanie zewnętrznych chipów.

Szczerze mówiąc trudno mi w takich momentach powstrzymać się od zacytowania pytania, które padło w komentarzu z serwisu Slashdot: [Z czyjego tyłka wyciągnięto takie założenie?](#) Wyżej zacytowany tekst, z którego wynika że efektem wprowadzenia systemu ochrony treści w Viście będzie spadek cen sprzętu, pochodzi od menedżera projektu odpowiedzialnego za ten system. Menedżer z firmy ATI, który nadzoruje produkcję sprzętu twierdzi coś zupełnie innego:

“Koszty te przenoszone są na konsumenta”

“Koszty przenoszone są na wszystkich konsumentów”

“Koszt ten przerzucany jest na nabywców multimedialnych pecetów”

“Koszty ponoszą konsumenci”

“Koszty ponoszą konsumenci, w szczególności nabywcy sprzętu nowej generacji”

Sami zdecydujcie któremu z nich wierzyć.

### **Czy działanie systemu ochrony treści odbija się niekorzystnie na zwiększonym zapotrzebowaniu na moc procesora?**

Tak. Jednakże zużycie tych dodatkowych cykli jest nieuniknione, jako że nowy system operacyjny dostarcza dodatkowych funkcji.

Proszę zwrócić uwagę na dobór słów: “dodatkowych funkcji”, nie zaś na przykład “ulepszonych rozwiązań”. System ochrony treści tak naprawdę ogranicza możliwości stojące przed użytkownikiem. [Użytkownicy Visty już teraz zwracają uwagę na obciążenie procesora](#) przez proces “Media Foundation Protected Pipeline” (oto [odpowiedni zrzut ekranu](#)) i narzekają, że początkowe zużycie procesora sięga 100%, aby potem utrzymywać się na poziomie 10-20% podczas odtwarzania. Jeden z użytkowników pisze, że proces ten zabiera [50% mocy Pentium 4 taktowanego zegarem 3 GHz](#), podczas gdy podobnych problemów nie ma w XP. Inny z kolei donosi, że “Media Foundation Protected Pipeline” pojawia się na liście procesów również podczas [odtwarzania nagrań w formacie DivX i XviD](#), co sugeruje że nie jest on aktywny tylko owóczas, gdy ma do czynienia z materiałem HD.

(Czy ktoś jeszcze może to potwierdzić? Nie używam Visty, ale jeżeli te doniesienia się potwierdzą, to twierdzenia Microsoftu, że system ochrony treści nie interesuje się nagraniami innymi niż HD staną się mało wiarygodne).

W podobnym stylu można odpowiedzieć na pytanie “Czy wirusy zwiększają zapotrzebowanie na moc procesora?” - “Tak. Jednakże zużycie tych dodatkowych cykli jest nieuniknione, jako że PC dostarcza dodatkowych funkcji” (w rodzaju spammingu, phishingu itp.)

### **Co ze złączami S/PDIF? [...] Czy system ochrony treści będzie wyłączał złącza komponent (YPbPr)?**

Podobnie jak w przypadku złącza S/PDIF, Windows Vista nie wymaga by złącza komponentowe musiały być wyłączone - realizuje raczej zasady określone przez wydawców/nadawców, włączając w to ograniczenia portów wyjściowych i pogorszenie jakości obrazu.

Czyli “tak, będzie wyłączał”. To kolejny z fragmentów pochodzących z Waggener Edstrom.

### **Czy redukcja echa będzie działała gorzej w przypadku “treści kwalifikowanych”?**

Jesteśmy przekonani, że Vista zapewnia aplikacjom wystarczającą ilość informacji niezbędnych do ich poprawnego działania. Redukcja echa będzie działać w pełni sprawnie.

Powodem, dla którego zwracam Waszą uwagę na kwestię redukcji echa jest [dokument, którego autorem jest Dave Marsh](#) - czyli osoba podpisana pod odpowiedzią Microsoftu - a który stwierdza wprost, że system ochrony treści i system redukcji echa wzajemnie się zakłócają. Cytat powyżej twierdzi coś zupełnie przeciwnego. Któryś musi mijać się z prawdą.

### **Czy ochrona treści audio oznacza, że wyjścia HDMI nie będą pokazywane jako S/PDIF?**

Lepiej jest, jeżeli będą rozróżniane, bo to pozwala na rozróżnienie ich w interfejsie użytkownika, co z kolei ułatwia ich rozpoznanie przez użytkownika i usprawnia konfigurację. Użytkownik chce widzieć różnicę między HDMI i S/PDIF, jako że fizycznie są to dwa różne złącza.

Przeglądając komentarze zamieszczone w serwisie Slashdot, miło jest przekonać się, że po przeczytaniu tego fragmentu [nie tylko mnie od razu przed oczami staje powieść Orwella](#):

Wojna	to	pokój!
Niewolnictwo	jest	wolnością!
Zawsze walczyliśmy z konsumentami i piratami!		

To kolejne z marketingowych stwierdzeń, które wciąż pojawiają się, gdy mowa o najnowszym dziecku Microsoftu. Projektanci złącz HDMI w pełni świadomie uczynili to złącze kompatybilnym (jeżeli chodzi o sygnał audio) ze złączem S/PDIF. Udowadnianie, że tworzenie sztucznych różnic pomiędzy oboma typami połączeń pozwala uprościć życie użytkownikowi jest jak twierdzenie, że ręczna skrzynia biegów jest lepsza, bo umożliwia precyzyjniejszą kontrolę nad zachowaniem pojazdu - z technicznego punktu widzenia to może być prawda, ale jeśli nie jest się kierowcą Formuły 1, to raczej na niewiele się zdaje. Mniej oznacza więcej. Wojna to pokój.

### **Czy system ochrony treści spowoduje, że układy graficzne będą musiały wspierać sprzętowe dekodowanie video?**

Nie. System ochrony treści Windows Vista przez lata nie będzie wymagał, by układy zawierały wsparcie dla dekodowania wideo, ale takie wsparcie na pewno poprawi odtwarzanie materiału HD.

Tak jak w przypadku redukcji echa, moim źródłem był [dokument Dave’a Marsha](#). Oto cytat:

PVP-UAB wymaga, bo układy graficzne wspomagały co najmniej przekształcenia iDCT oraz Motion Comp dla formatu MPEG2 oraz Windows Media® wersja 9/VC-1.

Tak jak w przypadku echa, oba te stwierdzenia wzajemnie się wykluczają.

## O autorze

Jestem naukowcem pracującym na [Wydziale Informatyki Uniwersytetu w Auckland](#) w Nowej Zelandii, zajmuję się tworzeniem i analizą rozwiązań kryptograficznych. W przeszłości byłem jednym z współtwórców programu PGP, napisałem wiele [artykułów oraz dokumentów RFC dotyczących bezpieczeństwa i kryptografii](#), między innymi “X.509 Style Guide” oraz [“Cryptographic Security Architecture: Design and Verification”](#) (wydany przez Springer-Verlag). Większość czasu zajmuje mi rozwijanie programów z zestawu [cryptlib](#), co pozwala mi być na bieżąco z najnowszymi osiągnięciami w tej dziedzinie.

W wolnym czasie oddaje się swojej pasji fotograficznej a gdybym tylko miał tego czasu nieco więcej, to poprzedni odnośnik zaprowadziłby was zapewne do porządnej galerii w serwisie Flickr a nie do [skromnej strony WWW](#). Ostatnio dostałem również drugi pełny etat jako rzecznik od spraw systemu ochrony treści Visty :) )

## Cytaty

Kilka zabawnych cytatów, zamieszczam je dla zwiększenia rozrywkowego waloru tego tekstu.

Proponuję żeby kopie systemu dostarczać wraz z kompletem skoczka spadochronowego: pomarańczowym kostiumem i okularami. Skoro Vista uważa mnie za wroga, niech przynajmniej wyglądam jak trzeba - Daniel Nevin

Windows Vista (ang. widok, perspektywa, horyzont - przyp. tłumacza)? Cóż za perspektywa! Gdy rozglądasz się wokół, widzisz tylko wysoki na kilkanaście metrów mur - Crosbie Fitch

Witamy w nowym świecie DRM, gdzie zazdrośni właściciele praw autorskich mogą zdalnie doprowadzić urządzenia elektroniczne do stanu bezużyteczności. Tak trzymać, Hollywood! - Chip Mulligan

Mogę tylko powiedzieć, że pomysł “bitów spustowych” jest szalony. Mogę też sobie wyobrazić producentów sprzętu, którzy go nie implementują, albo raczej udają tylko, że go implementują - Dave Walker

Kupiłem odtwarzacz DVD/SACD (z wyjściem HDMI), wzmacniacz surround (bez HDMI, nie stać mnie jeszcze na taki sprzęt) oraz telewizor LCD z wejściem HDMI. Odtwarzacz połączyłem ze wzmacniaczem za pomocą kabla optycznego, wzmacniacz z telewizorem łączył kabel HDMI. Wydawało mi się, że to wystarczy. Błąd! Działało pięknie, dopóki nie próbowałem odtworzyć mojej jedynej płyty SACD. Zapadła cisza! O co chodzi? Przejrzałem podręcznik obsługi odtwarzacza, gdzie znalazłem niewielką uwagę, wydrukowaną jeszcze mniejszą czcionką: “Podczas odtwarzania płyt SACD dźwięk wyprowadzany jest tylko na analogowe złącza 5.1 RCA” - Anthony May

Nie mogę odtwarzać materiału HD, bo musiałbym wymienić swój zestaw dwóch kart nVidia Quadro 4500 (wart około 2000 dolarów) na kosztującą 200 dolarów kartę FX7600GT, która obsługuje HDCP. Nie mogę się doczekać aż ktoś w końcu złamie ten syf nazywany DRM/HDCP/AACS - “Sy”

Dzięki wielkie, Muslix64 [autor narzędzia łamiącego zabezpieczenia płyt HD-DVD],

widać nie tylko ty masz monitor czy kartę graficzną, która nie obsługuje HDCP. Doceniam Twoje wysiłki - "yodoso"

Najśmieszniejsze jest to, że nie bardzo wiem w jaki sposób HDCP mogłoby powstrzymać piractwo. W rzeczywistości takie urządzenia tylko zachęcają piratów, bo każdy kto w ostatnich latach kupił komputer/monitor/telewizor HDTV, który nie posiada HDCP powinien jeszcze raz pójść do sklepu. Zamiast więc przeznaczyć te pieniądze na oryginalne płyty, będą woleli je wydać na pirackie krążki Blue-ray/HD-DVD, którym HDCP do szczęścia nie jest potrzebne - "Gizza"

Władcy HDCP zbliżają się. Twierdzą, że nie możesz obejrzeć filmu jeżeli nie masz właściwej karty graficznej i cyfrowego monitora. Wszystko po to, żebyś ty, użytkownik-któremu-nie-można-ufać-a-który-kupił-ich-raczej-drogi-sprzęt, nie mógł zrobić kopii zapasowej swojej płyty HD-DVD czy Blu-ray - "verifex"

Technologia ochrony cyfrowych mediów nigdy nie zapobiegnie łamaniu prawa autorskiego, tak jak świnie nigdy nie nauczą się latać. Stwierdzam to rok w rok i za każdym razem mam rację - Ed Felten

Microsoft nie zasypia gruszek w papierze. Trzy dni po udostępnieniu cracka, wypuścił patch łatający dziurę. Wielkie koncerty medialne nie muszą czekać miesiąc na łatkę. To dobitnie uświadamia nam, że ekonomia jest zdecydowanie lepszym motorem postępu niż chęć zapewnienia bezpieczeństwa swoim użytkownikom - Bruce Schneier na temat wydania łatki zapobiegającej działaniu narzędzia FairUse4WM

Nie tak dawno jeszcze pracowałem jako projektant układów elektronicznych, więc łatwo mi sobie wyobrazić uczucia, jakie targają innymi inżynierami i ich pracodawcami [...] To kompletne szaleństwo dla każdego z wyjątkiem dostawców treści, ale oni się tym nie przejmują, bo kto inny przecież ponosi koszty! - Anthony May

Jedynym osiągnięciem HDCP będzie zainteresowanie klientów nielegalnymi produktami, które będą przecież najmniej restrykcyjne. Wystarczy skojarzyć koszty, jakie trzeba będzie ponieść by skompletować sprzęt, na którym będzie można coś legalnego obejrzeć (pomimo że sprzęt który już teraz posiadają klienci w zupełności wystarczy) ze spadkiem wydajności spowodowanym szyfrowaniem/odszyfrowywaniem danych i tak oto otrzymujemy wspaniały przepis na nakłanianie do piractwa - "Greg"

Dobra robota! Spędzić tyle czasu nad rozwijaniem formatu video następnej generacji tylko po to, żeby w imię zabezpieczeń przed kopiowaniem wypracować dwa formaty, które i tak zaraz zostaną złamane przez 14-letnich hackerów i dostępne za darmo w sieci BitTorrent - "SweetMercury"

Sony, MS, studia filmowe... układ jest taki. Spieprzyliście to tak koncertowo, że nie zamierzam kupować napędu HD dopóki nie dadzą mi takiego z nowym komputerem tylko dlatego, że CD i DVD nie będą już dostępne - "zweben"

Microsoft powinien powołać do życia nowy dział. 'Dział przepraszenia klienta', czy jak to sobie tam nazwą. Od rana do wieczora będą wypowiadać kwestie w rodzaju "Ojej, naprawdę nam przykro że nie może pan odtworzyć muzyki kupionej przed epoką PlaysForSure. Proszę nie brać tej nazwy dosłownie" oraz "Tak, wiem że powinien pan być w stanie odtworzyć ten film HD w wysokiej rozdzielczości, ale wygląda na to, że pański kabel miał defekt, który zmienił charakterystykę sygnału, więc, cóż, przykro mi z powodu kabla" - Blake Ramsdell

twoje śmierdzące wypociny są teraz w każdym serwisie w internecie, prawda?  
pokazywali cię już na cnn? czy panienki rzucają w ciebie majtkami? - przyjaciel  
(zastrzegł anonimowość)