

Nadchodząca wojna z komputerami ogólnego przeznaczenia

19 stycznia 2012

Komputery ogólnego przeznaczenia są niesamowite. Są tak niesamowite, że nasze społeczeństwo nadal nie jest w stanie w pełni pojąć do czego służą, jak je wykorzystać i jak się do nich przystosować. Dlatego też poruszę temat, o którym być może nie macie już ochoty czytać: prawa autorskie.

Postarajcie się mnie jednak wysłuchać, bo napiszę o czymś dużo ważniejszym. Kształt wojen copyrightowych pokazuje bowiem, jak będzie wyglądała walka o przeznaczenie samej idei komputerów ogólnego przeznaczenia.

Na początku mieliśmy sneakernet. Mieliśmy dyskietki przenoszone w sportowych torbach, tekturowych pudłach, wywieszone w sklepach i sprzedawane jak batoniki. Były podatne na kopiowanie, kopiowano jest szybko i rozpowszechniano powszechnie, ku wielkiemu smutkowi tych, którzy produkowali i sprzedawali oprogramowanie.

Wtedy na scenę wkroczyły systemy DRM, elektroniczne zarządzanie prawami autorskimi, w swojej najprymitywniejszej formie, nazwijmy ją DRM 0.96. Wprowadziły fizyczne znaczniki, których poszukiwało oprogramowanie – celowe uszkodzenia, klucze sprzętowe, ukryte sektory – oraz protokoły, które wymagały znajomości trudnych do skopiowanie manuali pełnych potencjalnych haseł.

Metody te zawiodły z dwóch przyczyn. Po pierwsze, były niepopularne w świecie komercyjnym, ponieważ ograniczały użyteczność oprogramowania dla posiadaczy oprogramowania, którzy nabyli je zgodnie z prawem. Uczciwi nabywcy narzekali na utrudnione robienie kopii zapasowych, nienawidzili marnować

portów w celu wykorzystania kluczy sprzętowych, irytowali się koniecznością taszczenia ze sobą wielkich manuali tam, gdzie chcieli uruchomić swoje programy. Po drugie, nie powstrzymały one piratów, którzy odkryli banalne metody modyfikowania programów i omijania weryfikacji oryginalności. Ludzie, którzy korzystali z oprogramowania bez płacenia za nie, nie zauważyli specjalnej różnicy.

Zazwyczaj wyglądało to tak, że programista będący w posiadaniu technologii i wiedzy porównywalnej z tą, którą posiadał twórca oprogramowania, korzystał z reverse engineering, inżynierii odwrotnej, która pozwalała mu zmodyfikować program i rozpowszechnić scrackowaną wersję. Brzmi to bardzo specjalistycznie, ale w rzeczywistości takie nie było. Odkrywanie, jak funkcjonują odporne programy i obchodzenie błędów i uszkodzeń stanowiły podstawowe umiejętności dla programistów czasów ułomnych dyskietek i początków ery programowania. Strategie przeciwników kopiowania musiały stać się bardziej skuteczne dopiero wtedy, gdy rozpowszechniło się wykorzystanie sieci. Kiedy mieliśmy fora, serwisy internetowe, grupy dyskusyjne i mailingowe, wiedza ludzi, którzy odkryli jak obchodzić systemy zabezpieczeń mogła zostać zapakowana i rozpowszechniona pod postacią niewielkich plików – cracków. Kiedy wzrosła przepustowość internetu, mogły być rozpowszechniane całe scrackowane programy.

Tak narodził się DRM 1.0. W okolicach 1996 roku stało się jasne dla wszystkich ośrodków władzy, że nadchodzi coś ważnego. Staliśmy u progu gospodarki informacyjnej, cokolwiek u diabła miałoby to znaczyć. Założono więc, że oznacza to gospodarkę, w której handluje się informacjami. Technologie informacyjne zwiększały wydajność, więc wyobraźcie sobie, jak mogłyby wyglądać rynki gospodarki informacyjnej! Mógłbyś kupić książkę na jeden dzień, sprzedać prawo do obejrzenia filmu za jedno euro, a następnie wypożyczać przycisk pauzy są centa za sekundę. Mógłbyś sprzedawać filmy w jednej cenie w jednym kraju, a w innej w drugim, i tak dalej. Fantazje tamtych

czasów wyglądały jak nudna, utrzymana w konwencji science fiction adaptacja starotestamentowej Księgi Liczb, stanowiły nieciekawą listę wszystkich permutacji rzeczy, które można zrobić z informacjami – i jaką cenę można nałożyć na każdą z nich.

Niestety dla nich, nic z tego nie było możliwe, dopóki nie udałoby się przejąć kontroli nad tym, w jaki sposób ludzie korzystają ze swoich komputerów i plików, które na nie wgrywają. Wszak łatwo było mówić o sprzedawaniu komuś piosenki do ściągnięcia na odtwarzacz MP3, jednak trudniej o prawa do przekopiowanie tej piosenki z urządzenia na urządzenie. Jak u licha można byłoby powstrzymać kopiowanie, skoro już raz przesłało się dany plik? Aby to zrobić, trzeba wymyślić jak powstrzymać komputery przed uruchamianiem pewnych programów i analizowaniem pewnych plików i procesów. Możesz na przykład zaszyfrować niektóre pliki, a następnie wymagać, aby użytkownik korzystał z programu, który je odszyfruje tylko w określonych okolicznościach.

Ale, jak mawiają w Internecie, teraz masz dwa problemy. Musisz bowiem powstrzymać użytkownika przed zapisaniem pliku po odszyfrowaniu – co przecież w końcu się wydarzy – i musisz powstrzymać go od odkrycia, gdzie program trzyma klucze odszyfrowujące, co umożliwiłoby odszyfrowanie plików na zawsze i całkowite porzucenie durnego programu do ich odtwarzania.

Teraz masz trzy problemy: musisz powstrzymać użytkowników, którzy odszyfrowali pliki przed dzieleniem się nimi z innymi użytkownikami. Teraz masz cztery problemy, bo musisz powstrzymać użytkowników, którzy odkryli metodę odszyfrowania pliki przed dzieleniem się tą wiedzą z innymi użytkownikami. Teraz masz 5 problemów, bo musisz powstrzymać użytkowników, którzy odkryli, jak odkryć metodę odszyfrowania plików, przed dzieleniem się sposobem ich odkrywania z innymi użytkownikami!

To całkiem sporo problemów. Jednak w 1996 roku wymyślono rozwiązanie. Organizacja Narodów Zjednoczonych stworzyła

Traktat Światowej Organizacji Własności Intelektualnej o Prawie Autorskim. Na podstawie traktatu stworzono prawa, które delegalizowały odkrywanie tajemnic programów deszyfrujących i delegalizowały pozyskiwanie utworów (takich jak piosenki czy filmy) z programów deszyfrujących, kiedy te były uruchomione w celu odtwarzania utworu. Stworzono prawa, które delegalizowały dzielenie się wiedzą na temat odkrywania tajemnic programów deszyfrujących i zamieszczanie tych tajemnic – a także chronionych prawem plików – na serwerach. Utworzono też procedury, które umożliwiały łatwe usuwanie treści z Internetu bez zabawy z prawnikami, sędziami i innymi bzdurami.

I tak nielegalne kopiowanie skończyło się na zawsze, gospodarka informacyjna rozkwitła pięknymi kwiatami, które przyniosły dobrobyt dla całego świata; jak piszą na burtach lotniskowców: „Misja wykonana”.

Oczywiście nic takiego się nie wydarzyło, bo każdy, kto rozumiał komputery i sieci, wiedział, że prawa te spowodują więcej problemów, niż mogą rozwiązać. Wszak prawa te zabraniały zaglądać do wnętrza komputera, kiedy ten uruchamiał pewne programy. Delegalizowały mówienie ludziom co widziałeś, kiedy zaglądałeś, oraz czyniły prostym cenzurowanie treści w Internecie bez konieczności udowodnienia, że stało się cokolwiek niewłaściwego.

W skrócie, prawa te stawiały rzeczywistości nierzeczywiste wymagania i liczyły na to, że prawa rzeczywistości nie dotyczą praw własności intelektualnej. Kopiowanie stało się dużo łatwiejsze po ustanowieniu tych praw – kopiowanie już zawsze będzie stawało się łatwiejsze. Dzisiejsze kopiowanie to najtrudniejsze kopiowanie, jakie poznamy. Wasze wnuki będą się do was zwracać, mówiąc „Powiedz mi jeszcze raz, Dziadku, o tym jak trudno było kopiować w 2012, kiedy nie mogłeś kupić dysku wielkości paznokcia, który mógłby pomieścić wszystkie nagrane piosenki, wszystkie nakręcone filmy, wszystkie wypowiedziane słowa, wszystkie wykonane zdjęcia, wszystko, i przekopiować to w tak krótkiej chwili, że nie zauważa się kiedy”.

Rzeczywistość jest nieubłagana. Niczym kobieta z dziecięcej rymowanki, która połknęła pajaka, by złapał muchę, i musi teraz połknąć ptaka, by złapać pajaka, i kota, by złapał ptaka, tak samo muszą postępować regulacje, które, choć przemawiają do pewnych sentymentów, są katastrofalne w implementacji. Każda kolejna regulacja rodzi kolejną, która będzie miała naprawiać niedoskonałości tej pierwszej.

Kusi mnie, by zakończyć tę historię w tym miejscu wnioskiem, że problemem są twórcy prawa, którzy są głupi lub źli, lub być może jednocześnie jedno i drugie. Nie jest to zbyt satysfakcjonująca pointa, bo prowadzi nas jedynie do konkluzji, że problem ten jest nie do rozwiązania dopóty, dopóki głupota i zło będą obecne na salonach władzy – czyli że nigdy nie będzie możliwy do rozwiązania. Mam jednak alternatywną hipotezę tłumaczącą, co się wydarzyło.

Nie powinno być konkluzją, że regulatorzy nie rozumieją technologii informacyjnych, bo powinno być możliwe nie być ekspertem i tworzyć dobre prawo. Parlamentarzyści i kongresmeni są wybierani, by reprezentować regiony i ludzi, nie dyscypliny wiedzy i konkretne problemy. Nie mamy parlamentarzysty wybranego przez biochemię, ani senatora ze wspaniałego stanu planowania przestrzennego. Jednak ludziom tym, którzy specjalizują się w politykach i polityce, nie poszczególnych dyscyplinach technicznych, udaje się czasem tworzyć dobre prawo, które zdaje egzamin. Dzieje się tak dlatego, że rządzenie opiera się na heurystyce: przybliżeniach, pozwalających bilansować wiedzę ekspercką wielu stron.

Niestety technologie informacyjne mylą te przybliżenia – dają im wręcz solidny wycisk – w jeden, istotny sposób.

Głównymi testami na to, czy regulacja jest słuszna, jest po pierwsze to, czy zadziała, i po drugie to, czy w efekcie swojego działania nie wpłynie na wszystko pozostałe. Jeżeli chciałbym, aby kongres, parlament czy Unia Europejska

regulowała koło, trudno byłoby oczekiwać, żeby mi to się udało. Jeśli wskazałbym na fakt, że rabusie uciekają z miejsca napadu na bank w pojazdach korzystających z kół, i zapytałbym „Nie możemy czegoś z tym zrobić?”, odpowiedź brzmiałaby „Nie”. Wynika to z tego, że nie potrafimy wykonać koła zdatnego do swoich ogólnych zastosowań, ale bezużytecznego dla rabusiów. Widzimy, że korzyści korzystania z koła są tak istotne, że byłoby głupotą ryzykować ich utratę w szalonej próbie powstrzymania napadów na banki. Nawet gdyby wystąpiła epidemia napadów, nawet gdyby całe społeczeństwo stało na krawędzi przepaści, nikt nie pomyślałby, że należy zacząć rozwiązywać ten problem poprzez regulowanie koła.

Jednak jeżeli przedstawiłbym w tych samych okolicznościach bezsprzeczne dowody, że telefony z zestawem słuchawkowym sprawiają, że samochody stają się niebezpieczne, i zaproponowałbym prawo zabraniające korzystania z takich telefonów w samochodach, regulator mógłby powiedzieć, „Tak, widzimy twoje argumenty, to możemy zrobić”.

Możemy nie zgadzać się czy to dobry pomysł, albo czy moje dowody były wiarygodne, ale bardzo niewielu skłaniałoby się ku tezie, że bez telefonów samochody przestają być samochodami.

Rozumiemy bowiem, że samochody nadal są samochodami, jeśli usunie się z nich pewne dodatki. Samochody mają dość specyficzne przeznaczenie, przynajmniej jeśli porównać je do kół, i dodanie do nich telefonu oznacza tylko pewien niewielki dodatek do pewnej technologii specyficznego przeznaczenia. Prosty test działa tak: technologie specyficznego przeznaczenia są złożone, ale można z nich usunąć pewne dodatki bez fundamentalnego obniżenia ich podstawowej użyteczności.

Test ten służy dobrze regulatorom, ale nie jest bardzo użyteczny w przypadku komputerów ogólnego przeznaczenia i sieci ogólnego przeznaczenia – czyli w przypadku komputerów PC i Internetu. Jeśli pomyślisz o oprogramowaniu jako o dodatku,

komputer pozwalający pracować na arkuszach kalkulacyjnych ma dodatek arkuszowy, a komputer pozwalający grać w World of Warcraft ma dodatek MMORPG. Test powiedziałby ci, że komputer, który nie uruchamia arkuszy kalkulacyjnych albo gier, to nie większy atak na istotę komputera, niż zakaz korzystania z telefonów na istotę samochodu.

A jeśli myślisz o protokołach i stronach internetowych jako o dodatkach do sieci, to powiedzenie „naprawmy Internet tak, by nie dało się korzystać z BitTorrenta”, albo „naprawmy Internet tak, by nie dało się wejść na thepiratebay.org”, brzmi trochę jak „zmieńmy dźwięk sygnału zajętej linii telefonicznej”, albo „odłączmy tę pizzerię od sieci telefonicznej”, a nie jak atak na elementarne zasady funkcjonowania sieci.

Nasz test działa dla samochodów, domów i większości znaczących obszarów regulacji technologicznych. Brak zrozumienia, że nie działa dla Internetu nie sprawia, że jest zły ani głupi. Oznacza tylko, że należysz do olbrzymiej większości świata, dla której pojęcia takie jak „Kompletność Turinga” czy „sieć typu end-to-end” nic nie znaczą.

Więc nasi regulatorzy beztrąsko przegłosowują te prawa, a one stają się częścią naszego technologicznego świata. Nagle pojawiają się liczby, których nie wolno nam podać w Internecie, programy, których nie wolno nam zamieszczać. Aby z Internetu zniknęły jakieś treści, wystarczy samo oskarżenie naruszenia praw autorskich. Regulatorom nie udaje się osiągnąć swoich celów, bo nie powstrzymują oni ludzi od łamania praw autorskich, ale ich działania przynajmniej powierzchownie przypominają ich egzekwowanie. Spełniony zostaje sylogizm bezpieczeństwa: „coś musi być zrobione, ja robię coś, coś zostało zrobione”. Jako rezultat, wszelkie zawodności, które się pojawiają, mogą być wyjaśnione przez pomysł, że regulacja nie poszła dostatecznie daleko, zamiast zasugerować, że pomysł był wadliwy od początku.

Tego typu powierzchowne skojarzenie z rozwiązaniem problemu i

następujący w jego wyniku rozdzźwięk między intencjami, a rzeczywistością, pojawia się często w innych okolicznościach technicznych. Mam znajomego, który był wyższego szczebla menadżerem w dużej firmie produkującej dobra szybko zbywalne, który opowiedział mi taką historię. Dział marketingu przekazał inżynierom świetny pomysł na proszek do prania: od teraz będą produkować proszki, które po każdym praniu sprawiają, że ubrania stają się nowsze! Inżynierowie próbowali wytłumaczyć marketingowi ideę entropii, jednak ponieważ nie odnieśli skutku, wymyślili inne rozwiązanie: stworzyli proszek, który zawierał enzymy atakujące luźne końcówki włókien w ubraniach, te, które sprawiają, że ubrania wyglądają na stare. Po każdym wypraniu, ubrania wyglądały na nowsze. Niestety powodował też niszczenie materiału. Korzystanie z proszku powodowało rozpuszczanie się ubrania w pralce.

Jak widać, jest to przeciwieństwo sprawiania, by ubrania stawały się nowsze. Zamiast tego sztucznie je postarzamy z każdym praniem, a im częściej użytkownik próbuje wykorzystać zaproponowane przez inżynierów rozwiązanie, tym drastyczniejsze kroki musi podejmować, by ubrania wyglądały przyzwoicie. „Odmładzanie” ubrań kończy się, gdy rozpadną się całkowicie i trzeba będzie kupić nowe.

Dziś działy marketingu mówią „nie potrzebujemy komputerów, potrzebujemy sprzętów. Stwórz mi komputer, który nie uruchamia wszystkich programów, tylko program, który wykonuje konkretne zadanie, jak przesyłanie dźwięku, trasowanie pakietów, uruchamianie gier na Xboxa i upewnij się, że nie będzie uruchamiał programów, których nie autoryzowałem, bo mogę obniżyć nasze zyski”.

Z początku wydaje się to dosyć rozsądne: program, który spełnia jedną, wyspecjalizowaną funkcję. Możemy w końcu wsadzić silnik elektryczny do robota kuchennego, a możemy go wsadzić do zmywarki do naczyń nie martwiąc się czy da się uruchomić funkcje zmywarki w robocie kuchennym. Ale to nie to samo, co zamiana komputera w konkretny sprzęt. Nie budujemy

komputera, który potrafi uruchomić tylko jedną aplikację. Budujemy komputer, który może uruchomić każdy program, i ograniczamy go przy użyciu rootkitów, programów szpiegujących i zabezpieczamy go przed modyfikacją tak, aby użytkownik nie wiedział jakie procesy są uruchomione, aby nie mógł nic zainstalować, ani dezaktywować procesów, których nie chce. Innymi słowy, nasz sprzęt nie zawiera uproszczonego komputera – on zawiera w pełni funkcjonalny komputer, który zawiera złośliwe oprogramowanie w momencie otrzymania go od producenta.

Nie potrafimy stworzyć komputera ogólnego przeznaczenia, który będzie umiał uruchomić każdy program poza tymi, których nie lubimy, które są zakazane przez prawo, albo które zmniejszają nasze zyski. Najbliższym przybliżeniem, jakie jesteśmy w stanie osiągnąć, to komputer ze złośliwym oprogramowaniem: komputer, którego zasady funkcjonowania ustalone zostają przez nieobecną przy użytkowaniu stronę trzecią bez wiedzy użytkownika, lub pomimo sprzeciwu tegoż. DRM zawsze ewoluuje w stronę złośliwego oprogramowania.

W jednym głośnym przypadku – który stanowi prezent dla wszystkich, którzy skłaniają się ku tej hipotezie – Sony wgrało pliki instalacyjne rootkitów na 6 milionów płyt CD z muzyką, które po kryjomu uruchamiały programy monitorujące próby bezpośredniego odczytu plików z płyt i przerywały je. Utrzymywały obecność rootkita w sekrecie, poprzez spowodowanie, że jądro systemu operacyjnego kłamało na temat listy uruchomionych procesów i listy obecnych na dysku plików. Ale to nie jedyny przykład. Konsole Nintendo 3DS robią „aktualizacje” oprogramowania, których celem jest przeprowadzenie testu na modyfikację oprogramowania. W razie wykrycia prób modyfikacji, konsola dezaktywuje się i zamienia w bezwartościową cegłę.

Aktywiści praw człowieka wznosili alarm w kwestii U-EFI, nowego programu rozruchowego, który ograniczał możliwość uruchomienia systemu operacyjnego tylko do systemów

„certyfikowanych”, zwracając uwagę na fakt, że rządy opresyjnych reżimów będą prawdopodobnie przyznawały certyfikaty tylko tym systemom, które będą pozwalały na ukrywanie inwigilacji. Z perspektywy sieciowej, próby stworzenia sieci, która nie może być użyta do naruszenia praw autorskich, zawsze będą zmierzać ku tym samym rozwiązaniom, które są stosowane przez opresyjny reżym do inwigilacji swoich obywateli. Spójrzcie na projekt ustawy SOPA. To amerykańska ustawa przeciwko sieciowemu piractwu (ang. Stop Online Piracy Act), która delegalizuje niewinne narzędzia w rodzaju DNSSec – rozszerzenie systemu DNS weryfikujące informacje o nazwach domen – bo mogą być one wykorzystane w celu obchodzenia blokad nakładanych na poszczególne domeny. Ustawa blokuje też Tora – narzędzie pozwalające zachować anonimowość w sieci sponsorowane przez laboratoria amerykańskiej Marynarki Wojennej, które wykorzystywane jest przez dysydentów opresyjnych reżimów. Tor pada ofiarą ustawy, bo może być wykorzystywany do obchodzenia blokad IP.

W rzeczy samej, Motion Picture Association of America, zwolennik rozwiązań zaprojektowanych w ramach SOPA, rozpowszechniał memorandum, w którym przytaczał analizy stwierdzające, że SOPA może działać właśnie dlatego, że korzysta z tych samych metod, co Syria, Chiny czy Uzbekistan. Argumentują w nim, że skoro rozwiązania działają w tych krajach, to zadziałają też w USA!

Wygląda na to, że SOPA to ostatni etap w długiej wojnie o prawa autorskie i Internet. Może się też wydawać, że jeśli zwyciężymy, będziemy mieć prostą drogą ku zabezpieczeniu wolności komputerów PC i sieci. Ale jak wspominałem na początku, sednem nie są tu prawa autorskie.

Wojna o prawa autorskie to tylko wprawka przed nadchodzącą wojną z możliwościami komputerów. Branża rozrywkowa to tylko pierwsza, która chwyciła za broń, i przywykliśmy do myślenia o ich relatywnym sukcesie na tym polu. W końcu przed nami stoi SOPA, na skraju przegłosowania, grożąc zniszczenie Internetu

na elementarnym poziomie – wszystkie w imię zachowania list przebojów, reality shows i filmów z Ashtonem Kutcherem.

Rzeczywistość jest niestety taka, że ustawy o prawach autorskich osiąają tak wiele właśnie dlatego, że politycy nie traktują ich poważnie. Dlatego z jednej strona kanadyjski parlament proponował jedną fatalną ustawę o prawach autorskich za drugą tylko po to, by żadnej ostatecznie nie przegłosować. To właśnie dlatego czytanie SOPY, ustawy stworzonej z czystej głupoty o stężeniu wysokooktanowego idiotyzmu porównywalnym jedynie do wnętrza nowo narodzonej gwiazdy, zostało odroczone w trakcie przerwy świątecznej – żeby legislatorzy mogli wdać się w zacieklą debatę nad jakimś ważnym problemem, jak ubezpieczenie dla bezrobotnych.

To dlatego Światowa Organizacja Własności Intelektualnej jest co i rusz wrabiana we wprowadzanie szalonych, do bólu ignoranckich propozycji reformy praw autorskich: bo kiedy kraje świata wysyłają swoich ekspertów do Genewy, są to eksperci od dostępu do wody, nie od praw autorskich. Wysyłają ekspertów od zdrowia, nie od praw autorskich. Wysyłają ludzi specjalizujących się w rolnictwie, nie w prawach autorskich, bo prawa autorskie nie są takie istotne.

Kanadyjski Parlament nie przegłosował swoich propozycji reform praw autorskich, bo, z wszystkich rzeczy, które trzeba zrobić w Kanadzie, prawa autorskie znajdują się na liście poniżej zdrowotnych rezerwatów Indian, wykorzystywaniu złóż naftowych w Albercie, interwencji pomiędzy spierającymi się francuskojęzycznymi i anglojęzycznymi Kanadyjczykami, rozwiązania problemów z zasobami ryb i tysiącem innych spraw. Trywialność praw autorskich oznacza, że kiedy nadejdzie czas, gdy inne sektory gospodarki zajmą się swoimi problemami z Internetem i komputerami PC, spory o prawa autorskie okażą się ledwie potyczkami w świetle nadchodzącej wojny.

Dlaczego inne branże miałyby mieć podobne problemy z komputerami, jakie ma branża rozrywkowa? Świat, w którym

żyjemy, jest zrobiony z komputerów. Nie mamy już samochodów – mamy komputery, w których jeździmy. Nie mamy już samolotów – mamy latające komputery chodzące pod Solarisem, podpięte do wielkiego, zautomatyzowanego układu nośnego. Drukarki przestrzenne to tylko peryferia, które nie działają odłączone od komputera. Radio to już nie kryształ: to komputer ogólnego zastosowania uruchamiający specyficzne programy. Żale, które budzą nieautoryzowane kopie Snooki's Confessions of a Guidette są niczym, jeśli porównać je do wezwań do działania, które pobudzi nasza przesycona Internetem rzeczywistość.

Pomyślmy o radiu. Regulacje radiowe oparte są na przesłance, że właściwości radia są ustalone w momencie jego produkcji. Nie możesz po prostu nacisnąć przycisku, który zamieni nadajnik używany do pilnowania dziecka w drugim pokoju, w nadajnik zakłócający inne sygnały. Ale wszechstronne radia programowalne (software-defined radios – SDR), mogą zmienić się ze sprzętu do nadzoru dzieci w sprzęt do nadawania sygnału ratunkowych, albo używany do kontroli lotów, tylko poprzez załadowanie i uruchomienie innego programu. To dlatego Federalna Komisja ds. Komunikacji (Federal Communications Commision – FCC) rozważała, co stanie się, gdy SDRy staną się powszechne i prosiła o opinie na temat tego, czy powinna zadekretować, że wszystkie SDRy będą umieszczone w „zaufanym sprzęcie komputerowym”. Ostatecznie, pytanie sprowadza się do tego, czy wszystkie komputery powinny być zablokowane tak, by programy możliwe do uruchomienia były ściśle regulowane przez organy centralne.

Nawet to stanowi jedynie zapowiedź tego, co może nadejść. Żyjemy w końcu w czasach, w których ukazały się opensourcowe pliki opisujące sposób zamiany strzelb AR-15 w strzelby w pełni automatyczne. W czasach, w których zbudowano pierwszy opensourceowy, sfinansowany poprzez finansowanie społecznościowe sprzęt do sekwencjonowania genetycznego. I podczas gdy drukarki przestrzenne będą źródłem mnóstwa trywialnych zarzutów, znajdą się sędziowie na południu Ameryki

i mułłowie w Iranie, którzy będą wychodzić z siebie na myśl o ludziach pod ich jurysdykcją drukujących zabawki erotyczne. Rozwój druku przestrzennego stanie się źródłem wielu żali, których powodem będzie produkcja laboratoriów metamfetaminy i ceramicznych noży.

Nie trzeba być pisarzem science fiction, żeby zrozumieć dlaczego regulatorzy mogą okazywać nerwowość w kwestii modyfikowalnego przez użytkownika oprogramowania samochodów, które będą prowadzić się same, albo w kwestii ograniczenia zdolności do współpracy pomiędzy systemami kontroli lotów, albo w kwestii rzeczy, które można będzie wykonywać w ramach prostej inżynierii genetycznej. Wyobraźcie sobie dzień, kiedy Monsanto uzna, że sprawą wysokiej wagi jest zapewnienie, by komputery nie były w stanie uruchamiać pewnych funkcji programów kierujących sprzętem produkującym organizmy, które dosłownie zjadają ich lunch.

Nie jest w tej chwili ważne, czy uważacie, że to realne problemy, czy historyczne obawy – tak czy inaczej kwestie te stanowić będą o kierunku działań lobbystów i grup interesu dużo potężniejszych niż Hollywood czy wielkie wytwórnie muzyczne i wydawcy. Wszyscy dojdą do tego samego żądania: „Czy nie możecie dać nam po prostu komputera ogólnego przeznaczenia, który będzie uruchamiał wszystkie programy, poza tymi, których się boimy, albo które nas denerwują? Nie możecie stworzyć Internetu, który przekazuje każdą treść dowolnym protokołem, poza tymi sytuacjami, które nam przeszkadzają?”.

Pojawią się programy uruchamiane na komputerach ogólnego przeznaczenia i sprzęt peryferyjny do nich, którego istnienie będzie niekomfortowe nawet dla mnie. Dlatego domyślam się, że ludzie promujący ograniczenie komputerów ogólnego przeznaczenia trafiają ze swoimi argumentami na podatny grunt. Ale jak widzieliśmy w czasie wojen o prawa autorskie, zakazywanie poszczególnych instrukcji, protokołów czy wiadomości będzie dramatycznie nieskuteczne jako narzędzie

zapobiegania i lek na potencjalne bolączki. Wojna o prawa autorskie pokazała nam, że wszystkie próby kontrolowania komputera PC sprowadzą się do instalowania rootkitów, a próby kontrolowania Internetu doprowadzą do inwigilacji i cenzury. Te rzeczy mają znaczenie, bo przez ostatnią dekadę wydawało nam się, że wysyłamy naszych najlepszych graczy przeciwko ostatecznemu bossowi, podczas gdy prawda jest taka, że jesteśmy dopiero na końcu jednego poziomu, a przeciwników będzie jeszcze wielu. Znacznie urosną też stawki.

Jako członek pokolenie walcmena, pogodziłem się z myślą, że będę potrzebował aparatu słuchowego na długo przed śmiercią. Jednak tak na prawdę, to nie będzie aparat słuchowy; to będzie komputer. Więc kiedy wsiądę do samochodu – komputera otaczającego moje ciało – a w uchu będę miał aparat słuchowy – komputer wewnątrz mojego ciała – chcę mieć pewność, że te technologie nie są projektowane z myślą o ukrywaniu przede mną niektórych rzeczy, albo w celu ograniczenia mojej władzy nad wyłączeniem procesów, które uważam za niezgodne z moimi interesami. W zeszłym roku w Lower Merion, na zamożnych przedmieściach Filadelfii, pewna szkoła dla dzieciaków z klasy średniej wpadła w nie lada tarapaty. Została przyłapana na rozdawaniu uczniom laptopów z oprogramowaniem, które pozwalało na zdalną inwigilację poprzez kamerę i połączenie internetowe. Uczniów fotografowano tysiące razy, w domu i szkole, we śnie i na jawie, ubranych i nagich. W tym samym czasie powstała technologia legalnej inwigilacji, która pozwala potajemnie korzystać z twojej kamery, mikrofonu, nadajnika GPS, tabletu czy sprzętu mobilnego.

Jeszcze nie przegraliśmy, ale musimy wygrać wojnę o prawa autorskie, jeśli chcemy aby Internet i komputer PC pozostał wolny i otwarty. Dla zachowania wolności w przyszłości, konieczna będzie możliwość monitorowania naszych urządzeń i zlecania im tego, czego od nich oczekujemy; zdolności przeanalizowania i zakończenia procesów na nich uruchomionych; zdolności korzystania z nich jako z uczciwych usług naszej

woli, nie jako zdrajców i szpiegów pracujących dla przestępców, bandytów i obsesjonatów kontrolowania wszystkiego.

Autor: Cory Doctorow

Tłumaczenie: Stanisław Kwiatkowski

Źródło oryginalne: BoingBoing.net

Źródło polskie: [Instytut Misesa](http://InstytutMisesa)