Michał Alicki
Wydział Fizyki Uniwersytetu Warszawskiego

Zagrożenia prywatności

Dla przeciętnej osoby rozwój technologii kojarzy się głównie z podwyższeniem komfortu życia. Jednakże wszelkie usługi, tak jak para spodni, by były wygodne, muszą być dopasowane do użytkownika. Wiąże się to z ciągłym przesyłaniem danych, a ostatnio częściej nawet z ich gromadzeniem przez różne instytucje. Przy tak dużej wymianie informacji istotną kwestią staje się prywatność. Nowe metody analizy danych i coraz szybsze komputery pozwalają łamać hasła i algorytmy szyfrowania dotychczas uważane za całkowicie bezpieczne. Miniaturyzacja pozwala na coraz mniejsze urządzenia pozwalające na odbiór dźwięku i obrazu, zaś nośniki danych również ulegają zmniejszeniu. Ilość wszelakich urządzeń, które mogą posłużyć do ograniczenia prywatności wciąż rośnie. Czy zatem czeka nas totalna inwigilacja?

Duża ilość przechowywanych i wymienianych danych w postaci elektronicznej spowodowała rozwój technologii kryptograficznych. Pozwala to szyfrować dane w sposób wystarczający na potrzeby przeciętnego człowieka, tak by obca osoba nie miała łatwego do nich dostępu. Spowodowało to swoisty rozwój technik łamania zabezpieczeń. Tym samym coraz więcej metod kryptograficznych odchodzi do lamusa, lecz na ich miejsce pojawiają się nowe – sprawniejsze. Problem pojawia się niestety tutaj nie w kwestii rozwoju technologii, lecz jej szybkości docierania do przeciętnego odbiorcy i zdolności przystosowania się do niej człowieka. Przykładem może być szyfrowanie sieci bezprzewodowych poprzez algorytm WEP, czy przeglądarka internetowa IE 6 – te dwa swoiste produktu są wciąż obecne na rynku, mimo że ich bezpieczeństwo zostało wielokrotnie zakwestionowane. Jako że rośnie ilość technologii i zostają one coraz szybciej łamane, wręcz pewnym jest, iż coraz częściej brak informacji w społeczeństwie o najnowszych trendach będzie główną przyczyną zagrożenia prywatności.

Jednakże to nie wszystko. W przyszłości niewątpliwie pojawią się komputery kwantowe, czy maszyny innego typu o znaczącej mocy obliczeniowej. Spowoduje to, iż wszystkie metody zabezpieczeń oparte na pojedynczym haśle przestaną być barierą, gdyż takowe będzie można złamać poprzez atak typu Brutal Force. Tym samym należy się zastanowić nad nowymi technologiami zapewniającymi prywatność i zabezpieczającymi poufne dane. Prawdopodobnie spowoduje to rozpowszechnienie się certyfikatów czy haseł jednorazowych, jednakże te drugie musiałyby zostać wysyłane do użytkownika przy każdym wpisaniu niewłaściwego, co oznacza najprawdopodobniej przeciążenie serwerów, a tym samym efekt ataku DDOS. Problem pozostaje więc bardzo trudny do rozwiązania. Ulgę może przynieść technologia kryptografii kwantowej, lecz obecnie nie jest niepozbawiona wad. Tym samym jakże istotny staje się jej rozwój.

Nowoczesne technologie to nie tylko coraz większa moc obliczeniowa i fizyka kwantowa. Miniaturyzacja urządzeń pozwoliła już dziś uzyskać nośniki niemalże niewidoczne ludzkim wzrokiem a zarazem łatwe do odczytania nawet z dystansu. Nic więc dziwnego, że coraz częściej pojawiają się propozycje zastosowania nowoczesnej technologii do znakowania ludzi. Argumentami są niewątpliwa wygoda posiadania wszystkiego przy sobie i ciężkiego do kradzieży (lecz czy aby na pewno?). Prawo jazdy, karty kredytowe, biblioteczne? Po co to wszystko, jest to

przecież takie łatwe do zgubienia, skoro można mieć to w nadgarstku? A w wersji premium rozszerzonej przecież można dorzucić telefon i pocztę mailową. Wszystko łączy się się w czasie rzeczywistym z siecią serwerów, które to wszystko obsługują poprzez olbrzymią międzynarodową sieć (by nawet w Chinach było wiadomo, że Ty to Ty, a komputer, z którego korzystasz u kumpla Tybetańczyka, zmienił język z rodowitego chińskiego na polski). Dodatkowo geolokalizacja informuje znajomych, czy jesteśmy w domu, a może przy okazji dostajemy mailowo filmiki z globalnego systemu monitoringu obywateli, który identyfikuje naszą obecność poprzez chip, byśmy mogli powspominać wakacje nie musząc uprzednio samodzielnie robić zdjęć. Prawda, że cudowna wizja? Wszystko w zasięgu ręki, dosłownie, bo jedynie przyłożyć nadgarstek do czytnika, a może nawet nie, wystarczy przejść obok czujnika... no i uprzednio dać się oznaczyć, by można było Ciebie zidentyfikować.. Warto tu się zatrzymać, gdyż idea może piękna, ale praktyka okazuje się zupełnie nieidealistyczna – zresztą podobnie jak z innymi utopijnymi koncepcjami, takimi jak socjalizm. Porównanie dość słuszne, bo i tu pojawiają się problemy w czasie realizacji. Po pierwsze pojawia się pytanie, kto by przetrzymywał dane i skąd pewność, że nie wykorzysta ich do złych celów? Włamanie zaś do takiej bazy byłoby może trudne, ale jak pokazuje doświadczenie wcale nie takie nierealne. Cicha zmiana pewnych wpisów, by wyeliminować przeciwników również. Nie wspominając już o tym, że dane muszą być odpowiednio zaszyfrowane, by nikt nie podłączył się z podróbką i nie odczytał nie swojego pakieciku. A jak już wspomniano wyżej, każdy szyfr jest możliwy do złamania. Czyli pojawia się coraz więcej niekompatybilnych ze sobą urządzeń i pewnego rodzaju błędów w zabezpieczeniach. Nawet jednak jeśli te zagrożenie wyeliminowano by to pytanie czy właśnie stosując takie znaczenie nie sprzedano duszy diabłu, przepraszam, państwu? Bo państwo przecież, nie mając konkurencji, może pozwolić sobie na drobne błędy w zabezpieczeniach... i nagle dowiaduje się ktoś obcy, że spotykasz się z sąsiadką zza rogu. Tego typu oznaczenia stanowią duże zagrożenie prywatności, a tym samym, mimo że mają zapewniać bezpieczeństwo i wygodę, w przyszłości mogą co najwyżej je zlikwidować

Jednakże warto zauważyć, że rozwój technologii nie jest zły. Kluczowym problemem związanym z prywatnością jest błąd ludzki. Często jest to związane za zbyt wolną reakcją na niekorzystne zmiany większości społeczeństwa. Czasem też dobre zareklamowanie towaru zagrażającego prywatności, albo pewien rodzaj terroryzmu informacyjnego, czyli po prostu dezinformacji. Przykłady tego drugiego można mnożyć. Jednym z nich była próba zakazania prawnie w Polce w 2009 roku sieci VPN Tor ze względu na domniemaną wysoką aktywność pedofilii w tejże. Bezpieczeństwo dzieci rzeczywiście jest bardzo istotną sprawą, jak nie kluczową, lecz przez wiele tygodni media wcale nie zwróciły uwagi na główną rolę tej sieci, to jest zachowywanie anonimowości nawet w miejscach, gdzie istnieje cenzura (warto tutaj zauważyć, iż węzły Tora w Polce są dość istotne ze względu na sąsiedztwo z Białorusią). Jest to w pewien sposób oddziaływanie presji na społeczeństwo. Podobne praktyki stosuje na coraz większą skalę Francja. Były plany zakazania hashowania haseł internetowych, czy instalowania trojanów na fabrycznie kupionym sprzędzie – oficjalnie dla bezpieczeństwa ludności, jednakże w praktyce jest to furtka dla różnego rodzaju hackerów czy crackerów. Co gorsza społeczeństwo często się na to godziło, zaś możliwość tego typu blokad nie jest winą najnowszych technologii, lecz raczej niedoinformowania społeczeństwa. Tym samym nasuwa się jakże kluczowa konkluzja, że wraz ze wprowadzaniem do otwartego rynku nowych technologii, zwłaszcza tych, które w pewnym stopniu zagrażają prywatności, należy

niesamowitą wagę przywiązać do roli informacji w społeczeństwie. I to jej brak, a nie najnowsze osiągnięcia ludzkości, są głównym zagrożeniem prywatności.