Krzysztof Korolczuk
MIMUW

Zagrożenia prywatności

Na przestrzeni lat prawo do prywatności kształtowało się zależnie od czasów, panującego ustroju, polityki. Jednak jak daleko w przeszłość byśmy się nie oddalili myślą, tak istnieli ludzie, którym odbieranie tego prawa innym przynosiło korzyści. Szpiedzy, donosiciele, czy nawet zwykłe plotkary z rynku podsłuchały niejedno słowo, których nie powinny, przynajmniej z punktu widzenia wypowiadającego.

Dzisiaj w dobie internetu i sieci radiowych oraz konstytucyjnego prawa do prywatności, pojęcie to nabiera nieco innego charakteru. To już nie chowanie się przed podsłuchem i gumowym uchem ale codzienna walka z milionami bitów informacji nad którymi nasza kontrola może być znikoma.

Weźmy dla przykładu tak popularne od jakiegoś czasu sieci wifi. Wydają się być idealnym rozwiązaniem oszczędzającym kładzenie setek metrów kabli. Jednak coś za coś. Przeciętny Kowalski nie zdaje sobie sprawy, iż wszystko, co robi w internecie, może być (często bez żadnego trudu) dzięki temu podejrzane przez osoby trzecie, bez uciekania się do znanych z filmów sensacyjno/szpiegowskich metod. Wystarczy zwykły laptop i odpowiednie oprogramowanie.

Internet w całej swej okazałości jest również pełnym polem dla popisu dla wszelkiej maści podsłuchiwaczy. Jednak można się zastanawiać nad pewnym usprawiedliwieniem. Przeciętny Kowalski korzysta tak naprawdę z technologii o których nie wie praktycznie nic. Protokoły sieciowe i internetowe są jednak w większości otwarte, tzn jest wolny dostęp do opisu ich działania. Spora część z nich z założenia nie miała być odporna na podsłuchiwanie. Prywatność i anonimowość w sieciach komputerowych to (przynajmniej w większości przypadków) bajka, a na pewno coś trudno osiągalnego dla owego ‘chcącego poklikać’ Kowalskiego. Jakkolwiek ta ciut niejasna kwestia niewiedzy użytkowników współczesnych technologii informatycznych by nie była, użytkownicy bardziej ich świadomi stworzyli szereg narzędzi pomocnych w zapewnieniu prywatności. Na szczególną uwagę zasługuje tak niedawno w sumie odkryta kryptografia z kluczem publicznym, która wraz z kryptografią symetryczną otworzyła drogę do bezpiecznych protokołów sieciowych. Programy typu PGP czy programy klienckie protokołu SSH to jedne z wielu przykładów. Tak więc nie taka sieć straszna jeżeli wie się z czego korzystać.

Spoglądając jednak jeszcze raz na historię prywatności i jej zagrożeń nasuwa się pytanie o bardziej ogólną jej naturę i związek z postępem technologicznym. Wydaje się, że wprowadzanie nowych technologii komunikacyjnych stwarza zawsze potencjalne ryzyko wycieku informacji, tym większe im bardziej złożony i nieznany jest mechanizm przesyłu tej informacji. Z drugiej strony komplikacja tego mechanizmu może działać na korzyść prywatności, uniemożliwiając osobom niepowołanym przechwyt komunikacji. Jedno jest pewne. Obecne systemy komunikacji mogą być nieporównywalnie bardziej bezpieczne niż te nawet sprzed 20-30 lat. Doświadczenia z rozwoju internetu nie poszły na marne. Stworzyły zapotrzebowanie na coś, co wydaje się, że daje kryptografia kwantowa. Jej przyszłość wydaje się być świetlana. Jednak jakkolwiek by teoria piękna nie była, póki służy komunikacji między ludźmi, zawsze znajdzie się sposób na jej podsłuchanie. Jeżeli nie sposób czysto techniczny to sposób czysto ludzki...