K.P.
22.06.13

Adam Cebula „Wielki brat”

Adam Cebula

Collage: Krzysztof Pacyński

W prasie mamy kolejną burzę z powodu tym razem polskiej ustawy zezwalającej tak zwanym służbom na inwigilację obywatela praktycznie bez powodu. Awantura buzuje wokół inwigilacji w internecie. Dziwnym trochę przypadkiem, nie bulwersują inne formy, jak podsłuchy telefonów, podsłuchy w pomieszczeniach i tak dalej.

Sprawa bywa tłumaczona - zwłaszcza przez tych co chcą podsłuchiwać - tak, że przecież my jesteśmy ci dobrzy. Jak ktoś nic nie ma na sumieniu, nie ma się czego obawiać, przecież to oczywiste. Można powiedzieć, że poniekąd i racja. Policja w krajach Europy z grubsza nie czepia się osób niewinnych. Zupełnie niewinnych i z grubsza.

Wszelako, jako osoba, która ma za sobą obowiązkowy, może nawet i nieukończony, i bardziej podstawowy, ale jednak kurs konspiry, a przynajmniej elementarne doświadczenia, mam w temacie swoje własne zdanie, które niekoniecznie pokrywa się z tym, co mówią owi dobrzy, ale nie jest również zbieżne ze stanowiskiem protestujących. Jak mi się zdaje, a na uzasadnienie swojego stanowiska posiadam argumenty, jest w wielu sprawach inaczej, niz prezentuja to strony sporu.

Powiedzmy, że zagrożenie terrorystyczne wzrasta. Owszem, jest realny, niewydumany powód, by tak myśleć. To zarówno aktywność tak zwanego Państwa Islamskiego, jak i (w przypadku Polski, o czym mówi się znacznie rzadziej, a moim zdaniem jest to także bardzo ważne), nazwijmy rzecz dyplomatycznie, pewne wypadki w sąsiadującym państwie oraz postawa innego państwa. Mniejsza o to, czy to my sobie nagrabiliśmy, ja bym nie lekceważył sąsiada, który ma w temacie rycia i wywoływania rewolucji znaczne doświadczenia.

Zagrożenia są i nie ma co chować w piasek głowy. Lecz nie wiem, nie za bardzo rozumiem, jak się one mają do inwigilacji wszystkiego, wszystkich i na dodatek na zapas.

Problem jest dużo szerszy niż nasze krajowe poletko: na całym świecie rzesze policjantów chcą większych uprawnień i mniejszej kontroli tego, co robią. Jak się okazało po wycieku danych wywiezionych przez Snowdena, podsłuchiwanie wszystkiego i wszystkich weszło w krew rządom na całym świecie. Także rząd USA, który zdaje się być strażnikiem światowego porządku, podsłuchiwał w najlepsze, nie zawracając sobie głowy żadnymi regułami prawa.

Słusznie? To dyskusja dla filozofów. Lepiej zadać inne pytanie: czy faktycznie jest to skuteczna metoda na wykrycie naprawdę groźnych spiskowców?

Być może praktyka pokazuje coś takiego, że na przykład islamiści „umawiają się" na forach internetowych, że używają do tego niewyszukanych, powszechnie dostępnych narzędzi, wręcz zakładają profile na Facebooku. Że kontaktują się za pomocą zwykłych e-maili, w bardziej wyszukanych formach za pomocą serwerów jakichś gier internetowych. Być może.

Przeczytałem kiedyś prostą odpowiedź człowieka zajmującego się bezpieczeństwem internetowym, co zrobiłby on do skomunikowania się w niecnych celach. Umieściłby na jakimś masowo odwiedzanym portalu zdjęcie, film, nagranie dźwiękowe i w nim - za pomocą steganografii - wiadomość. Oczywiście, sposób nie jest idealny. Można sobie wyobrazić, że od dostawcy Internetu ktoś wydobędzie informację, że z tego IP kontaktowano się z portalem, może nawet podejrzeć transmisję. Informacji już nie podejrzy.

Steganografia działa tak, że dopóki nie odszyfrowaliśmy informacji, dopóty nie mamy sposobu, by odróżnić ją od szumu. W filmie, dźwięku ostatnie, najmniej znaczące bity zapisu szumią. To właściwie jest kres możliwości podsłuchu: można stwierdzić, że ktoś informację wysłał, przy pewnej dozie szczęścia można stwierdzić, że ktoś odebrał. Owszem, jeśli mamy logi, gdzie zapisano wszystkie wejścia do sieci, można by skorelować dane, że x wysyłał, a y odbierał, wchodził na stronę... Że coś jest na rzeczy. Można to stwierdzić, jeśli mamy owe logi zarchiwizowane. Jakkolwiek naprawdę dowiemy się tylko tego, że x np wysłał zdjęcie, a y je pobrał, wczytując stronę internetową.

Otóż, drobna modyfikacja. Jak już wiele razy pisałem, kolega admin wylał na mnie kubeł zimnej wody, gdy miałem pomysł, by namierzyć gościa, który dokonał włamu na mój komputer. Okazało się, że owszem - być może da się stwierdzić, która mniej więcej grupa studentów jest podejrzana. Mniej więcej. Można bowiem doprowadzić do tego, że elektroniczne ślady zaprowadzą tropiciela donikąd.

To było jeszcze przed epoką radiowych routerów. Cóż współcześnie da się uzyskać, śledząc trasę pakietów w sieci? Prawdopodobnie zakończymy na numerze sprzętowym karty sieciowej urządzenia, które zalogowało się w jakimś punkcie dostępowym. Numerze, który został wygenerowany i jest psu na budę.

Z punktami dostępu do internetu jest tak, że owszem, bywa, że ktoś nie zabezpieczy swej sieci. Może się zdarzyć, że ktoś pobierze trojana, który udostępni nam jego hasło i login do jakiejś sieci. Ale najczęściej i najzwyczajniej w wielu miejscach - takich jak restauracje, kluby, hotele - zalogujemy się albo bez podawania swoich danych, albo znajdziemy routery w ogóle nie chronione.

Warto sobie uświadomić, że bez wielkiego sprytu da się zorganizować wszystko tak, że nie zostanie najmniejszy ślad po delikwencie, który z sieci korzystał. Nie zarejestruje go żadna kamera, nigdzie nie zostawi swoich - nawet zmyślonych - danych. Nie zwróci niczyjej uwagi, jeśli wejdzie na popularny serwis, taki jak YouTube, poprzeglądać filmy czy zdjęcia, albo je tam dodać. Korespondencja będzie się odbywać poza jakąkolwiek kontrolą.

Bardzo chętnie się pisze przy okazji tematu inwigilacji w sieci o sieciach Tor, o serwerach proxy, bramkach internetowych i tak dalej. Nie wiem, z czego korzystają na przykład ludzie budujący bootnety, jak działają serwisy, na których handluje się skradzionymi numerami pin kart płatniczych. Nie muszę wiedzieć. Każdy może sprawdzić, że na jego konta pocztowe spływa rzeka spamu. Oceniam, że u mnie stosunek wiadomości do reklam jest znacznie wyższy niż 1 do 1000. Wniosek jest taki, że nielegalna działalność w sieci jest prowadzona na wielką skalę i jest mało niebezpieczna.

Już banalne korzystanie z proxy w warunkach ustawy o inwigilacji może się okazać bardzo mocną

zaporą przeciw służbom. Proxy - w uproszczeniu - to komputer, z którym się łączymy, najczęściej protokołem z szyfrowaniem danych. Pełni on rolę pośrednika w połączeniu z jakimś docelowym serwisem. Część z nich gubi (wymazuje) całkowicie z pakietów dane o komputerze, który chce się połączyć przez pośrednika. Jedyne, co się da stwierdzić, obserwując pakiety na linii łączącej taki serwer z internautą, to, że taka komunikacja występuje. Za serwerem, obserwując wychodzące z niego pakiety, nie będziemy mogli zapewne nawet próbować skorelować na podstawie czasu wysyłki pakietów, gdzie one są kierowane. Albowiem ruch na wyjściu jest znaczny. Ale poza tym, jeśli serwer jest gdzieś daleko, to nasza, albo nawet amerykańska służba specjalna zwyczajnie nie ma do niego dostępu.

Jeśli ktoś, rejestrując pakiety u dostawcy Internetu, wyłapie delikwenta łączącego się poprzez proxy, może nabrać podejrzeń. Ale, jeśli okaże się, że choćby dziesięć procent internautów używa proxy, będzie miał zgryz. Owszem, proxy przydaje się do wielu innych rzeczy poza cyberatakami czy wymianą informacji pomiędzy przestępcami. Obserwacja Internetu da nam kilkaset tysięcy potencjalnych podejrzanych, trochę za wiele, by się nimi móc zająć.

Czy służby specjalne mogą odszyfrować dowolną wiadomość, mają dostęp do każdego programu szyfrującego? Owszem, są takie legendy, że w każdym z nich są „tylne drzwi" i na przykład automatycznie wysyła hasło służbom rządowym. Otóż programy te są autonomiczne (mówimy o dobrych, realnie działających), to znaczy - można je uruchamiać np. spod programu pocztowego, ale możemy zaszyfrować wiadomość np., w ogóle nie mając połączenia z siecią. Potem przenieść zakodowany plik na komputer podłączony do sieci i go wysłać.

Wiarygodne programy mają w pełni otwarty kod. Oznacza to, że społeczność informatyczna może prześwietlić je nie tylko pod kątem „back doorów", ale wszelkich możliwych słabości lub błędów. Taki los spotkał program TrueCrypt. W 2014 roku został on porzucony przez twórców na skutek nacisków rządu USA. Twórcy na stronie projektu ostrzegali przed użyciem programu. W roku 2015 przeprowadzono społeczny audyt oprogramowania i stwierdzono brak „tylnych drzwi", całkowitą zgodność wersji skompilowanej z kodem źródłowym. Znaleziono kilka błędów które nie mają zasadniczego wpływu na działanie programu.

Jak widać z wielu przykładów, łatwo zdobyć silne oprogramowanie, którego nie pokona nikt na naszej planecie. Gdyby było inaczej, nie byłoby nacisków na jego twórców, a losy ludzi, którzy się nim posługują, toczyły by się innym torem. Warto tu przypomnieć na przykład Snowdena, który po ujawnieniu tajnych danych rządu USA komunikował się z wieloma dziennikarzami i wielokrotnie ujawniał różne dane, a komunikacji tej nie dawało się odkryć dzięki stosowaniu narzędzi szyfrujących. To po prostu działa.

Przewaga, i to dramatyczna, jest po stronie prowadzącego tajną łączność. Można sam napisać program do szyfrowania. Zwłaszcza w przypadku tak zwanego szyfrowania symetrycznego jest to proste. To zazwyczaj jedno z pierwszych ćwiczeń programistycznych. Jeśli ktoś chce odczytać wiadomość, to wówczas algorytm, jaki zastosowaliśmy, już stanowi element klucza do złamania. Bo przecież trzeba wiedzieć, po pierwsze, że zrobiono coś nietypowego, po drugie - co to było. Pisałem kilka razy, złożenie banalnego kodu Cezara z powszechnie dostępnym programem szyfrującym może okazać się zaporowe dla wszelkich prób dekryptażu. Program, który tego dokonuje, musi w jakiś sposób poznać, ze trafił na właściwą kombinację hasła.

Można założyć, że powszechnie znany, nawet uznawany za bardzo mocny, program został przećwiczony przez kryptologów i może znaleźli jakieś jego słabe strony. Wystarczy jednak przed „mocnym" kodowaniem dokonać na bajtach reprezentujących tekst jakiejś całkiem „durnej" operacji typu właśnie kodowanie Cezara, który spowoduje zamianę bajtów odpowiadających literom, znakom niedrukowalnym (dzwonek, potwierdzenie poprawności, koniec papieru, takie są tam zakodowane

sygnały), a program deszyfrujący nie ma sposobu odkryć, że złamał hasło. Każda kombinacja będzie wyglądała równie kiepsko. Ktoś musi mu dopisać fragment kodu, który będzie sprawdzał, czy wyszło coś sensownego po zastosowaniu dodatkowego łamania kodu. Sęk w tym, że ten dodatkowy moduł musi być kompatybilnym z tym, co zrobił szyfrujący.

W przypadku szyfrowania asymetrycznego złamanie kodu polega na znalezieniu dwóch liczb pierwszych, które tworzą bardzo wielką liczbę, tak zwany klucz publiczny. Klucz publiczny, jak sama nazwa wskazuje, jest często powszechnie znany. Czyli tekst nam nie jest potrzebny. Teoretycznie to ułatwia zadanie, lecz znalezienie owych liczb pierwszych na dzień dzisiejszy uważa się za beznadziejne. Dla kluczy powyżej 1024 bitów szacuje się czas łamania na kilka lat dla klastrów obliczeniowych. Dlatego, o ile istniałyby jakieś metody „na przełaj", to prawdopodobnie z użyciem zakodowanego tekstu. Potrzebne są dodatkowe dane. Czyli analiza przesyłanego tekstu i sprawdzanie na nim zgadniętego hasła. Z tego powodu stosowanie kodowania kaskadowego, nawet z użyciem kodu Cezara, wydaje się bardzo sensowe.

Gdy dziennikarze zajmują się problematyką kryptografii, zazwyczaj - niechcący i bez uświadomienia sobie tego - przyjmują pewne ograniczenia na tworzenie metod szyfrowania, które wynikają w dużej mierze z mocno rozrywkowego podejścia do tematu. Owszem, część z nich może mieć sens praktycznie, lecz, po pierwsze, zmieniają one dość trywialne ostatnimi zadanie w zabawę na miarę zagadek Szeherezady. Jedno z założeń jest takie, ze algorytm szyfrujący jest powszechnie znany, tajne jest jedynie hasło. Owszem, to pozwala opublikować kod programu na licencji OpenSource, lecz powiedzmy sobie szczerze, gdyby algorytm nie był znany, zupełnie nie byłoby zabawy. Dlaczego? Bo w takiej sytuacji nie mamy z definicji żadnych szans odkodowania wiadomości.

Inne założenia są tylko po trosze „praktyczne". Klucze powinny być krótkie, a program szyfrujący musi w możliwie najmniejszym stopniu obciążać komputer. Tak to poniekąd praktyczne, ale głównie uatrakcyjnia intelektualnie zabawę z kryptologią. Rzecz w tym, że w jednostkowej komunikacji i przy dzisiejszym poziomie i przepustowości łączy oraz mocach obliczeniowych, nie musimy sobie tym zawracać głowy. Możemy sobie pozwolić na komplikacje pożerające moc czy szastające ilością danych, które z bardzo kiepskich metod ukrywania wiadomości uczynią w praktyce bardzo trudne do złamania narzędzie. Banalny przykład: można do naszej wiadomości dorzucić powiedzmy bite 1000 stron tekstu. Nawet jeśli nie użyliśmy żadnego kodu, to przechwytujący tajną komunikację musi mieć sposób, jak odcedzić właściwy kawałek z gigantycznego tekstu. A, powiedzmy to od razu, generatory tekstu także są dość prostym ćwiczeniem informatyka. Durnowata metoda, która wydaje się godna pensjonarki, w przypadku, gdy nie wiemy, co wpisać w okienko „znajdź" (zaś adresat zaszyfrowanego komunikatu ma na to sposób), może okazać się wygodnym i niezmiernie skutecznym narzędziem.

Dawno temu już pisałem: istnieje szyfr nie do złamania. To tak zwany szyfr jednorazowy. Jego działanie można wyjaśnić na podstawie tzw. „znaku umówionego". Widzisz na niebie czerwoną rakietę. Możesz jedynie zgadywać, co ona oznacza. Może do ataku, a może sp… , bo nie masz żadnych danych, by cokolwiek wygłówkować. Seria znaków umówionych jest właśnie kodem jednorazowym. Istotą sprawy jest to, że za każdym razem od nowa umawiamy się, co będzie oznaczać owa czerwona rakieta.

Jeśli korespondenci wymienią się kartami pamięci z zapisanym tym samym ciągiem szumu, zgranym np. z odpowiednio spreparowanej diody, to mogą przesłać między sobą ilość informacji odpowiadającą wielkości zbioru zapisanego na karcie. Ile? Powiedzmy - 64 gigabajty.

Analiza słynnych wpadek cyberprzestępców prowadzi do wniosku, że owszem, analiza ruchu, sprawdzenie zawartości dysku komputera, w okolicznościach, gdy delikwent jest już i tak podejrzany, może pomóc organom ścigania. Np. opisywano historię człowieka, który umieścił w sieci listę płac

firmy i pomimo użycia sieci Tor wpadł. Lecz stało się tak, ponieważ był na liście niewielu osób, które mogły dokonać takiego wygłupu, i nie złamano zabezpieczeń sieci Tor, tylko na komputerze zostały (na skutek użycia systemu Windows) ślady manipulacji.

Wyobrażenia na temat możliwości inwigilacji są wyprowadzone z sytuacji, w których podsłuchiwani nie zrobili niczego, by się bronić. Warto przy okazji zauważyć, że o sytuacjach, gdy zrobili cokolwiek i to było skuteczne, prawie nigdy się nie dowiadujemy. Bo o to chodziło, by delikwenta nie znaleźć. W powszechnym obiegu znajduje się wiedza o przypadkach nieudanych. Zapotrzebowanie na sensacyjne informacje plus to nieuchronne filtrowanie stwarza w rezultacie zupełnie nieprawdziwy obraz.

Wygląda na to, że „służby", zwłaszcza w sieci, mogą sobie pohulać, pod warunkiem że strona przeciwna nie czuje się w żaden sposób zagrożona i dosłownie nic nie robi, by się bronić. Jeśli spojrzeć na rozmiary internetowej przestępczości, to wygląda, że podjęcie stosunkowo prostych kroków wytrąca śledzącym wszystkie narzędzia z ręki.

Można podejrzewać, że wprowadzenie powszechnych podsłuchów i monitorowania sieci będzie miało skutki odwrotne do zamierzonych. Jeśli ludzie zaczną masowo używać szyfrowania, serwerów proxy, to w tej masie spokojnie ukryją się użytkownicy coś tam knujący. Współcześnie osobnik szyfrujący dysk wzbudza natychmiast podejrzenie. Wywołajmy modę na stosowanie silnych narzędzi kryptograficznych, a przekonamy się, że one są naprawdę silne. Władze USA biedziły się nad dyskiem z komputera bodaj handlarza narkotyków kilka lat i w końcu musiały ogłosić kapitulację. Jaka to była piękna katastrofa... Owszem, inwigilacja dostarcza jakichś informacji, ale jaki będzie bilans pomysłów podsłuchiwaczy?

Jest tu inna rzecz, dużo bardziej niepokojąca. Do czego powszechna inwigilacja naprawdę dobrze się nadaje? Do zbierania haków. Widać dobrze na przykładzie afer podsłuchowych: jeśli się dobrze im przyjrzymy, to stwierdzimy, że część osób chciała zrobić argument przeciw bardzo nie lubianym przez siebie podsłuchiwanym praktycznie tylko z tego, że dali się podsłuchać.

Jeśli ktoś nazbiera danych, to zawsze da się z tego coś poskładać. Powiedział „nie dam w łapę" słówko „nie" zginie, zagłuszone pozornie przypadkowym stukiem, mamy aferę korupcyjną. Ludzie, którzy mają coś na sumieniu, planują coś niebezpiecznego, bez trudu ukryją swoją elektroniczną aktywność. Taka jest rzeczywistość tej technologii. Ktoś świadomy, że wszystkie jego działania zostawiają mnóstwo śladów na dyskach komputera, uruchomi system operacyjny, który pracuje jedynie w pamięci operacyjnej, i po odłączeniu zasilania znikną wszystkie zapisy. Osoba normalnie pracująca robi na odwrót, archiwizuje dane choćby na wypadek awarii, i przez to tworzy potencjalne pokłady dowodów. Jeśli poszukujemy kogoś, kto robi ciągle szkody, choćby spamuje, to na przykład pozbieranie adresów ludzi, którzy używają serwerów proxy, najpewniej nic nam nie da. Po pierwsze, ten ktoś zapewne nie znajdzie się w spisie, po drugie - utoniemy w masie danych. Do sprawdzenia będzie za wiele osób, za wiele faktów. Odwrotnie, jeśli chcemy skompromitować na przykład jakiegoś konkretnego działacza politycznego, to fura zarejestrowanych zdarzeń, dokumentów, jak możemy się łatwo przekonać, pozwala oczernić nawet Matkę Teresę z Kalkuty. To, że nie złapaliśmy spamera, bardzo łatwo poznać po sypiącym się spamie, zaś udowodnienie, że Matka Teresa czegoś nie zrobiła, jest właściwie niemożliwe.

Inwigilacja jest, odwrotnie niż w powieściach antyutopijnych, świadectwem nie mocy władzy, ale słabości, braku pomysłu na to, jak się bronić. Gdy się wie, kto zagraża, nie śledzi się wszystkich. A jeśli wszyscy są podejrzani, znaczy to, że władza mimo totalnej inwigilacji jest zupełnie zdezorientowana. Najpewniej uderzy nie w tych, co są groźni, tylko w tych, których się boi. Jeśli rządy sięgają po takie środki, to znaczy, że coś się na świecie poważnie sypie.

Największym problemem jest chyba to, że o inwigilacji pisze się, kręci materiały telewizyjne, wedle wzorców wziętych z literatury sensacyjnej. Upatruje się zagrożeń, których nie ma, możliwości, które nie istnieją, skali nie do zrealizowania, czy wreszcie nieprawdopodobnej skuteczności, w oderwaniu od technicznych realiów. W rezultacie dyskutujemy o rzeczach, których nie ma albo są, lecz nie w tym rozmiarze, o zjawiskach, których nie zaobserwujemy. Największy problem owej inwigilacji jest taki, że ona nie zadziała. Owszem, da się tego czy owego wrobić, tamtego oczernić, ale skutki bynajmniej nie będą takie, jak w antyutopiach - w postaci totalnej kontroli społeczeństwa. Wydarzą się rzeczy nie z literatury, ale z realu. Jakiś kolejny Snowden opublikuje tajne dane, lecz o wiele bardziej prawdopodobne jest to, że ktoś je wykradnie i posłuży się nimi przestępczych celów, ktoś inny spreparuje te dane dla wrobienia swojego przeciwnika. Generalnie, to nie zadziała tak, jak sobie założyła mityczna władza. Nie ma powodu, by skutki były inne, niż programu walki z alkoholizmem, analfabetyzmem czy przemocą w rodzinie. Będzie to przedsięwzięcie sto razy droższe niż zakładano, a zamiast rozwiązać problemy, narobi nowych, o wiele większych.

Moim zdaniem to jest największym problemem. Bać się inwigilacji chyba nie ma wielkich powodów, trzeba się martwić.

Adam Cebula