Od kusz do kryptografii, czyli psucie państwu szyków przy pomocy techniki

8 czerwca 2011

O tej maksymie – przysłowiu – powszechnie przypisywanej Eskimosom zapewne słyszeliśmy wszyscy; lecz o ile prawdopodobnie nie będziemy sprzeczać się z mówiącym to, o tyle możemy odbierać ją jako zwyczajny frazes, który niczego już nas nie nauczy i być może jesteśmy już zmęczeni jej wysłuchiwaniem. Dlatego powtórzę to teraz:

„Jeśli dasz człowiekowi rybę, to nakarmisz go na jeden dzień. Ale jeśli nauczysz człowieka, jak łowić ryby, to nakarmisz go na całe życie".

Prawdopodobnie postrzegałeś ten cytat w kontekście opozycji „workfare" do „welfare"; mianowicie, jeśli chce się naprawdę pomóc komuś w potrzebie, powinno się go nauczyć, jak ma zarabiać na środki swojego utrzymania, a nie, jak po prostu o nie żebrać. I jest to oczywiście prawda, choćby dlatego, że jeśli będzie on głodny następnym razem, to w pobliżu może nie być nikogo, kto chciałby czy nawet mógłby dać mu rybę, podczas gdy dysponując informacją, jak łowić ryby, jest on całkowicie niezależny.

Twierdzę jednak, że wyczerpuje to jedynie pierwszą warstwę zawartości tego cytatu i zmarnowałbym nasz czas cytując go po raz kolejny, jeśli nie było tam nic więcej do zebrania. Zresztą wydaje się on mieć niemal kryptoaltruistyczny wydźwięk, sugerując jak gdyby, że powinniśmy układać nasze sprawy tak, by zwiększać korzyści głodnych żebraków, jakich możemy napotkać.

Ale zauważmy: przypuśćmy, że ten Eskimos nie wie, jak łowić ryby, ale wie, jak polować na morsy. Ty zaś podróżując przez

kraj morsów bywasz często głodny, bo nie masz pojęcia, jak chwytać te przeklęte stworzenia i być może zjadły ci one wiele ryb, które mógłbyś złapać. Przypuśćmy teraz, że decydujecie się wymienić informacjami, wymieniając wiedzę o łowieniu ryb na wiedzę o polowaniu na morsy. Pierwszą rzeczą, jaką obserwujemy jest to, że tego rodzaju transakcja kategorycznie i niedwuznacznie obala marksistowskie założenie, że każdy handel musi mieć „zwycięzcę" i „przegrywającego" – ideę, że jeśli jedna osoba zyskuje, musi to koniecznie zachodzić „kosztem" innej osoby, która traci. Rzecz jasna w tym scenariuszu taki przypadek nie zachodzi. Każda ze stron zyskała coś, czego nie miała przedtem i nie została przy tym w jakikolwiek sposób uszczuplona w swym stanie posiadania. Gdy przychodzi do wymiany informacji (a nie przedmiotów materialnych), życie nie jest już dłużej grą o sumie zerowej. Jest to niezwykle doniosłe. „Prawo malejących zysków", „pierwsze i drugie prawo termodynamiki" – wszystkie te „prawa", które w innych kontekstach ograniczają nasze możliwości – nie krępują nas więcej! Jest to anarchia nowego i podniecającego rodzaju!

Rozważmy inną możliwość: przypuśćmy, że ten głodny Eskimos nigdy nie nauczył się łowić ryb, bo władca jego plemienia uznał łowienie za nielegalne. Mówi on nam, że ponieważ ryba zawiera niebezpieczne małe ości, a czasami szpiczaste kolce, jego władcy zarządzili, że konsumpcja, a nawet posiadanie ryb jest zbyt ryzykowne dla ludzkiego zdrowia, aby było dozwolone – nawet dla dobrze poinformowanych, chętnych dorosłych osób. Być może jest tak dlatego, że ciała obywateli uważane są za własność plemienną i co za tym idzie funkcją władcy jest karanie tych, którzy niewłaściwie troszczą się o ten majątek. Albo może jest tak dlatego, że jego władca wspaniałomyślnie rozszerza na kompetentne dorosłe osoby „korzyści" przewidziane dla dzieci i umysłowo chorych: pełnoczasowy, wszechogarniający nadzór – tak, by nie musieli się oni kłopotać dokonywaniem wyborów zachowań uważanych za fizycznie ryzykowne lub moralnie „nieprzyzwoite". W każdym razie patrzysz zdumiony, gdy twój

eskimoski informator opowiada, że prawo to traktowane jest tak poważnie, iż jego przyjaciel został niedawno uwięziony na wiele lat za zbrodnię „posiadania dziewięciu uncji pstrąga, z zamiarem sprzedaży”.

Możesz teraz dojść do wniosku, że społeczeństwo tak groteskowo opresywne, że narzuca tego rodzaju prawa jest po prostu afrontem dla godności wszystkich ludzkich istot. Możesz pójść dalej i zdecydować się poświęcić część swojego czasu na psucie szyków tyranowi. (Twój motyw może być „altruistyczny”, w rodzaju pragnienia wyzwolenia uciskanych, lub „egoistyczny”, w rodzaju chęci dowiedzenia, że możesz przeciwstawić się uciskającemu, lub – bardzo możliwe – może być on kombinacją tych lub innych powodów).

Ale skoro nie masz ochoty zostać męczennikiem swojej „sprawy”, nie będziesz montował kampanii wojskowej czy nawet próbował przemycić łodzi ryb. Jednak technika – w szczególności technika informacyjna – może zwielokrotnić twoją skuteczność dosłownie sto razy. Mówię „dosłownie”, bo za ułamek wysiłku (i właściwie bez ryzyka) towarzyszącego przemycaniu stu ryb, możesz całkiem łatwo wyprodukować sto kserokopii instrukcji łowienia ryb. Jeśli rząd, jak we współczesnej Ameryce, pozwala przynajmniej otwarcie dyskutować o rzeczach, których robienie jest zabronione, powinno to wystarczyć. Ale jeśli rząd próbuje zlikwidować również przepływ informacji, to będziesz musiał podjąć trochę większy wysiłek i być może napisać swoją instrukcję łowienia ryb w zaszyfrowanej formie na dyskietce lub zagrzebać ją w nie wykonywanej części kodu gry komputerowej. Odbiorca (skoro tylko zna sekret) może łatwo wyciągnąć informację ze swego komputera, ale żaden nieproszony plemienny szpicel nie dowie się niczego.

Technika – w szczególności komputerowa – dostawała często niezasłużone szturchańce od miłośników wolności. Mamy skłonność myśleć o 1984 Orwella czy o Brazil Terry’ego Gilliama, czy o wykrywaczach ciał utrzymujących niewolników-obywateli Berlina Wschodniego po ich stronie granicy, czy o

wyszukanych urządzeniach używanych przez Nixona do szkodzenia ludziom ze swej „listy wrogów”. Albo przyznajemy, że za cenę biletu na Concorde możemy lecieć z dwukrotną prędkością dźwięku, ale tylko wówczas, gdy przejdziemy najpierw przed magnetometrem obsługiwanym przez rządowego policjanta, pozwalając mu nas przeszukać i obmacać nasze bagaże, jeśli urządzenie zapiszczy.

Ale takie nastawienie umysłu jest poważnym błędem! Zanim zaczęto używać elektrycznych pastuchów, rządy torturowały swych więźniów kijami i gumowymi wężami. Zanim do szpiegowania zaczęto używać lasery, rządy używały lornetek i ludzi czytających z ruchu warg. Chociaż rząd w oczywisty sposób używa techniki w celach ucisku, zło tkwi nie w narzędziach, lecz w tych, którzy je dzierżą.

W rzeczywistości technika stanowi jedną z najbardziej obiecujących dróg odebrania naszej wolności tym, którzy ją ukradli. Ze swej natury faworyzuje ona bystrego (który potrafi ją użyć) nad tępym (który nie potrafi). Faworyzuje ona elastycznego (który szybko dojrzy zalety nowego) nad ospałym (który trzyma się wypróbowanych metod). A czy są lepsze słowa do opisania jakiejkolwiek rządowej biurokracji niż „tępa” i „ospała”?

Jednym z najjaskrawszych, klasycznych triumfów techniki nad tyranią był wynalazek „broni osobistej” – przenośnej kuszy. Dysponując nią, niewyćwiczony wieśniak mógł łatwo i śmiertelnie trafić w cel z pięćdziesięciu metrów – nawet jeśli ten cel był konnym, opancerzonym rycerzem. (Inaczej niż długi łuk, który był niewątpliwie potężniejszy i mógł wystrzelić w danym czasie więcej strzał, kusza nie wymagała żadnych specjalnych ćwiczeń. Podczas gdy łuk wymagał dla osiągnięcia jakiegokolwiek stopnia celności opanowania wzrokowej, dotykowej i mięśniowej koordynacji, dzierżyciel kuszy mógł po prostu położyć broń na ramię, nacelować ostrze strzały i mieć uzasadnione podstawy pewności trafienia w cel).

Co więcej, skoro jedynymi konnymi rycerzami odwiedzającymi naszego przeciętnego wieśniaka byli rządowi żołnierze i poborcy podatków, użyteczność tego urządzenia była oczywista. Pospólstwo mogło się z nim bronić nie tylko przed sobą nawzajem, ale i przeciw swoim rządowym panom. Był to średniowieczny odpowiednik pocisku przeciwpancernego i co za tym idzie królowie oraz księża (średniowieczny odpowiednik Biura ds. Alkoholu, Tytoniu i Kusz) grozili za jego bezprawne posiadanie odpowiednio śmiercią i ekskomuniką.

Wracając do teraźniejszości, komputer osobisty (z uruchomionym na nim systemem szyfrującym z kluczem publicznym) przedstawia sobą odpowiednik przeskoku kwantowego – w dziedzinie broni defensywnej. Taka technika może być używana nie tylko do ochrony posiadanych przez kogoś wrażliwych danych, ale też do wymieniania przez dwie obce sobie osoby informacji przez niezabezpieczony kanał komunikacyjny – na przykład podsłuchiwaną linię telefoniczną czy nawet radio – bez jakiegokolwiek wcześniejszego spotkania w celu wymiany kluczy do szyfru.

Dysponując komputerem za pięćset dolarów możesz stworzyć szyfr, którego wart setki milionów dolarów Cray X-MP nie złamie w rok. Za parę lat powinno być ekonomicznie wykonalne szyfrowanie w podobny sposób także komunikatów głosowych; wkrótce potem pełnokolorowych, cyfrowo przetworzonych obrazów video. Technika odeśle podsłuch do lamusa! Ogólniej mówiąc, zniszczy ona całkowicie rządową kontrolę nad przepływem informacji!

Najbardziej obiecującym z tych kryptograficznych schematów wydaje się być algorytm RSA, nazwany tak od Rivesta, Shamira i Adelmana, którzy go wspólnie stworzyli [1]. W formalnym wyprowadzeniu zawiera on trochę umiarkowanie trudnej matematyki (liczby pierwsze, modulo, „małe twierdzenie Fermata”), ale jego istotą jest to, że jeśli dany jest iloczyn dwóch bardzo wielkich liczb pierwszych, otrzymanie ich z jego analizy jest obliczeniowo niewykonalne. „Obliczeniowo

niewykonalne” znaczy, że jeśli każdy czynnik ma około 200 cyfr, to najpotężniejszy istniejący komputer będzie potrzebował ponad wiek na rozłożenie ich 400-cyfrowego iloczynu.

Zamieniając czyjąś wiadomość na „liczbę” (nawet stosując coś tak prostego, jak A=01, B-02, …, Z=26) i wykonując na niej odpowiednie przekształcenie, uzyskuje się nową liczbę, która jest zaszyfrowanym przekazem. Odbiorca wykonuje następnie na tej liczbie podobne przekształcenie w celu odtworzenia pierwotnej wiadomości.

Tym, co czyni to przełomowym odkryciem i ze względu na co nazywa się to szyfrem z kluczem publicznym jest fakt, że mogę jawnie opublikować dwa liczbowe parametry, które pozwolą każdemu wysłać do mnie zaszyfrowaną wiadomość, utrzymując równocześnie w tajemnicy trzeci parametr, tak, że nikt poza mną nie może rozszyfrować takiego przekazu. Wyeliminowany został krok stanowiący uprzednio trudność (wymienianie kluczy szyfrujących z inną osobą). W ten sposób ludzie, dla których fizyczne spotkanie jest niemożliwe, niekorzystne lub niebezpieczne mogą łatwo wymieniać zaszyfrowane wiadomości – każda strona wybiera i rozpowszechnia swoje dwa publiczne parametry, utrzymując równocześnie w tajemnicy trzecie.

Inną korzyścią tego systemu jest pojęcie „podpisu cyfrowego”, umożliwiające identyfikację źródła danego przekazu. Dokonując dodatkowego kroku szyfrującego przy pomocy mojego tajnego parametru i wymagając od odbiorcy dokonania przy rozszyfrowaniu dodatkowego działania przy użyciu moich publicznych parametrów – mogę dowieść, że otrzymany przez niego przekaz nie mógł być wysłany przez nikogo innego prócz mnie! Tak, że nie tylko mamy łatwe zabezpieczenie transmisji przekazu przez anonimowy, niezabezpieczony kanał komunikacyjny, ale również możemy pozytywnie zidentyfikować nadawcę takiej wiadomości!

Oczywiście są to dokładnie te troski, które dziś dręczą w

kwestii komputerów osobistych Związek Radziecki [2]. Z jednej strony przyznają oni, że uczniowie amerykańscy dorastają w tej chwili dysponując komputerami będącymi rzeczą tak pospolitą, jak suwaki logarytmiczne – nawet bardziej, bo komputery mogą robić wiele rzeczy interesujących i instruujących 3-4-latki. I są to ci sami uczniowie, którzy za jedno pokolenie staną naprzeciw swych sowieckich odpowiedników. Trzymanie się z tyłu musi być dla Sowietów tak samobójczym krokiem, jak kontynuowanie nauki szermierki, gdy przeciwnicy produkują karabiny. Z drugiej strony komputer, czymkolwiek jeszcze może być, jest także niezwykle skuteczną maszyną kopiującą – dyskietka za 25 centów zawiera z górą 50000 słów tekstu i może być powielona w parę minut.

Jakby samo to nie byłoby wystarczającym zagrożeniem, komputer tworzący kopie może jeszcze szyfrować dane w sposób, który jest prawie nie do złamania. Pamiętajmy, że w społeczeństwie sowieckim nie są znane publicznie dostępne kserokopiarki (stosunkowo mała liczba istniejących maszyn jest kontrolowana intensywniej niż w USA pistolety maszynowe).

Dzisiejsi polityczni „konserwatyści” twierdzą, że nie powinniśmy sprzedawać Sowietom komputerów osobistych, bo mogą użyć je do celów militarnych. „Liberałowie” utrzymują, że powinniśmy im je sprzedawać w interesie wolnego handlu i współpracy – i jeśli nie będziemy tego robić, to zrobi to jakiś inny kraj.

Jako wolnościowy cyberpunk twierdzę, że powinniśmy dać je Sowietom za darmo i, jeśli będzie to konieczne, zrobić je dla nich – i, jeśli to nie wystarczy, być może powinniśmy załadować je do Blackbirda SR-71 i zrzucić je o północy nad Moskwą. Płacąc oczywiście z prywatnej subskrypcji, nie z przymusowego opodatkowania…

Przyznaję, że nie jest to stanowisko, które uzyskałoby duże poparcie wśród członków konwencjonalnego lewicowo-prawicowego politycznego spektrum, ale mówiąc słowami jednej z postaci

Illuminatusa, jesteśmy politycznymi nieeuklidesowcami: najkrótsza odległość do danego celu nie musi wyglądać jak cos, co większość ludzi uważa za „linię prostą”. Łamanie totalitarnym rządom monopolu na informację jest równoznaczne z łamaniem kręgosłupa ich zdolności uciskania. Komputeryzacja powiększa wolność każdego mężczyzny, kobiety i dziecka na tej planecie – i zrobi to bez jawnego czy ukrytego otwierania ognia!

Przyznajemy, że historię kształtowali ludzie o nazwiskach takich, jak Waszyngton, Lincoln, …, Stalin, Nixon, Marcos, Duvalier, Noriega i tym podobnych. Ale powinniśmy przyznać, że kształtowali ją także ludzie o nazwiskach Edison, Curie, Marconi, DeForest i Wozniak. I to drugie kształtowanie było co najmniej tak samo skuteczne, i nawet w przybliżeniu nie tak krwawe.

W swej książce How I Found Freedom in an Unfree World, Harry Browne czyni znaczące spostrzeżenie, że prawdopodobieństwo sukcesu jakiegokolwiek przedsięwzięcia jest odwrotnie proporcjonalne do liczby ludzi, których trzeba przekonać w celu jego dokonania. Tak, ze o ile przekonanie rządu, by skończył z praktyką cenzury i podsłuchiwania może być niemożliwe, o tyle zatrudnienie techniki szyfrującej do skończenia z tym samemu jest zadaniem trywialnym.

Patrząc dookoła, natychmiast widać nasuwające się dodatkowe zastosowania technarchii do rozwiązywania tego, co inaczej byłoby problemem politycznym: Saudyjczyk pragnący cieszyć się psychoaktywnym narkotykiem alkoholem zrobiłby mądrzej ucząc się chemicznego procesu fermentacji i destylacji, niż zużywając czas na nakłanianie swoich władców do zmiany islamskiego prawa. Niemiec ze Wschodu, który wolałby być Niemcem z Zachodu postąpiłby lepiej studiując aerodynamikę szybowców czy balonów, niż prosząc lub żebrząc o wizę wyjazdową.

Nie bez powodu rewolwer kalibru .45 nazywano na Dzikim

Zachodzie „zrównywaczem”. Stwarzał on najdrobniejszej dziewczynie z rewii możliwość obrony przed najbardziej krzepkim i brutalnym kowbojem. (Niektórzy mówią, że ruch na rzecz „kontroli broni” zrodził się, gdy okazało się, ze pozwala jej to także odeprzeć napaść rządowego szeryfa, ale to już inna historia). Komputer osobisty jest dziś „zrównywaczem” nie w dziedzinie brutalnej siły, ale przetwarzania informacji i idei.

Jak tylko nanotechnologia dostarczy urządzeń peryferyjnych, jakakolwiek rzecz złożona z jakichkolwiek substancji będzie mogła być zbudowana w czyimkolwiek garażu, jak tylko ta rzecz i te substancje zostaną wymodelowane matematycznie. W rezultacie rząd nie będzie mógł dłużej ogłaszać rzeczy i substancji za nielegalne – i będzie musiał znów wejść w jedyną uprawnioną rolę, jaką kiedykolwiek odgrywał: rolę tego, kto chroni obywateli przed innymi, którzy ich atakują. Tygrys zostanie wsadzony do klatki, na dobre i złe!

Co za tym idzie, gdy następnym razem będziesz patrzeć na tych, którzy będą chcieli być twoimi „wodzami” ze zdziwieniem i poczuciem zniewagi, i myśleć: „Dobrze, jeśli 51% tego narodu, 51% tego stanu i 51% tego miasta musi zmądrzeć, zanim będę wolny, to równie dobrze każdy mógłby podciąć mi moje pieprzone gardło i zostawić mnie na pastwę losu!” – uznasz, że sytuacja nie jest całkiem ponura. Technika – w szczególności technika komputerowa – może pomóc ci uczynić się jednostronnie wolnym!

Wchodzimy w ostatnią dekadę tego, co Timothy Leary nazwał Ryczącym Dwudziestym Stuleciem i każdy jej dzień ukazuje nam coraz bardziej oczywistość prawdy zawartej w jego zachęcie: „If you’re wise… digitize”.

Autor: Chuck Hammill
Tłumaczenie: Jacek Sierpiński
Źródło: Libertarianizm

OD TŁUMACZA

Tekst ten różni się częściowo od anglojęzycznej wersji najczęściej spotykanej w Internecie; jest on tłumaczeniem wersji otrzymanej listownie od autora w 1993 r.

PRZYPISY

[1] Już są znane lepsze (przyp. tłum.)

[2] Tekst ten powstał w 1989 r. (przyp. tłum.)