Michał Radwański
Wydział Matematyki, Informatyki i Mechaniki

Poprawka IV, terroryści, i my, zwykli ludzie.

Konstytucję Stanów Zjednoczonych uchwalono w 1787 roku. Szybko się okazało, że ochrona, jakiej udziela obywatelom przed rządem obywatelom nie wystarcza. Wśród Karty Praw, zbioru dziesięciu poprawek utworzonych dwa lata później, widniała m.in. Poprawka IV:
Prawa ludu do nietykalności osobistej, mieszkania, dokumentów i mienia nie wolno naruszać przez nieuzasadnione rewizje i zatrzymanie; nakaz w tym przedmiocie można wystawić tylko wówczas, gdy zachodzi wiarygodna przyczyna potwierdzona przysięgą lub zastępującym ją oświadczeniem. Miejsce podlegające rewizji oraz osoby i rzeczy podlegające zatrzymaniu powinny być w nakazie szczegółowo określone.

Ciężko jest przewidzieć rozwój technologii. Rząd federalny też zapewne się nie spodziewał znaczenia tego aktu prawnego, gdy w 1967, zostało osądzone, że podsłuch budki telefonicznej bez uprzedzenia dzwoniącego jest naruszeniem IV poprawki, bowiem poprawka nie chroni miejsc, a ludzi. Wiele rozpraw sądowych po tym wydarzeniu pomogło wyklarować, jakie zachowania naruszające zdroworozsądkową prywatność są nieprawomocne w Stanach Zjednoczonych. Oczywiście, przy budżecie organizacji rządowych, racjonalnie jest oczekiwać, że nawet gdy dokona się na Tobie bezprawnego przeszukania, masz szansę nigdy się o tym nie dowiedzieć.

Taka sielankowa dla rządów rzeczywistość zapewne by trwała, gdyby nie dostępna dla publiczności wysokiej jakości kryptografia. W roku 1977 powstał algorytm RSA, pierwszy kryptosystem, który umożliwia szyfrowanie innym kluczem niż deszyfrowanie. Po dziś dzień, stosując klasyczne komputery, nie potrafimy skutecznie odszyfrowywać treści, dla których klucza prywatnego nie znamy (chyba że klucz publiczny dobrano niestarannie, ale to już inna kwestia[1]). Rok wcześniej, w 1976, opublikowano algorytm Diffiego-Hellmana, służący do bezpiecznego ustalenia wspólnej sekretnej wartości (nawet w obliczu przechwycenia całej komunikacji między stronami). Późniejsze lata przyniosły duży rozwój wszelkim konstrukcjom kryptograficznym, z czego duża większość była stosowana powszechnie, nawet na urządzeniach przeznaczonych dla zwykłych konsumentów (choć nie bez przeszkód prawnych, wystarczy przyjrzeć się historii szyfru DES[2]). Organizacje rządowe nie omieszkały się upomnieć o swoje odwieczne prawa, w końcu powszechność kryptografi sprawia, że takie przeszukania bez wspomnienia stają się niemożliwe, a szalki wagi balansującej siły obywatela i państwa przechylają się w stronę tego pierwszego. Ale chwila, może jeszcze coś da się zrobić? Może da się w jakiś sposób zabronić kryptografii? Ale trzeba mieć najpierw jakiś powód, bo ten oczywisty, zwyczajnej chęci kontroli obywateli (bo tak jest po prostu łatwiej) nie ma szans na wygraną w sądzie. Różni reprezentanci rządu wielokrotnie się wypowiadali w tej sprawie, twierdząc, że to jest nieakceptowalne, aby dostęp do pewnych danych był dla rządu niemożliwy, nawet jeśli uzyskano odpowiedni nakaz sądowy. W końcu, co zrobić, gdy przechwycimy telefon terrorysty, ale nikt nie potrafi odkodować komunikacji, która była zapisana na urządzeniu? Istnieją więc pomysły, aby stworzyć takie szyfrowanie, które można złamać tylko przy prawomocnym wyroku sądowym, i takie umieszczać w dostępnych urządzeniach. Przykładowo, dostępne drukarki odmówią drukowania treści, które wyglądają na banknoty. Czemu więc miałby być problem ze stworzeniem tak niewyszukanej modyfikacji systemów szyfrujących? Zgodnie ze zbiorową opinią kryptologów, stworzenie takich systemów wystawia wszystkich korzystających na wielkie niebezpieczeństwo, bo matematyka nie rozróżnia między dobrym a złym użyciem, więc ułatwiony dostęp dla jednego rządu ułatwia dostęp nie tylko dla innych rządów (o co i tak by się upomniały), ale także dla organizacji

1 https://www.ams.org/notices/199902/boneh.pdf
2 http://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/des%20history.html

przestępczych, czy choćby tego ciekawskiego dzieciaka sąsiada, który chce poznać zdjęcia, które wysyłasz.

Wciąż nie wiadomo, czy taka walka jest dla rządu przegrana, jest jednak coś co może zmienić przebieg debaty. Pojawienie się komputerów kwantowych sprawi, że niektóre z klasycznie trudnych problemów (takich jak faktoryzacja liczb, wystarczająca do złamania schematu RSA) staną się proste. Nic w tym dziwnego zatem, że trwają wzmożone działania, aby z jednej strony doprowadzić komputery kwantowe do staniu używalności, z drugiej by stworzyć asymetryczną kryptografię odporną na algorytmy kwantowe, z trzeciej aby pomimo ich obecności, legalność swobodnego użytku szyfrowania była kwestionowana. NIST, Narodowy Instytut Standardów i Technologii zorganizował konkurs[3], który doprowadzi do wyłonienia znanych asymetrycznych kryptosystemów, które są odporne na ataki wykonane na komputerach klasycznych i kwantowych. Konkurs wciąż trwa, ale można oczekiwać, że zwycięski system nie będzie wydmuszką – wiodące propozycje były dostarczone przez czołowych badaczy, takich jak Daniela Bernsteina[4], czy Tanję Lange[5]. Inną kwestią jest, czy systemy te znajdą powszechne użycie, nim powstaną odpowiednio potężne komputery kwantowe.

Na przykładzie szyfrowania, jeszcze raz się przekonujemy, że to legislacja musi nadążać za rozwojem technologii, a nie na odwrót. W różnych miejscach na świecie były głosy, że winno być odwrotnie. Niedawno, premier Australii wypowiedział się, iż prawa matematyki są bardzo pociągające, ale jedynym prawem obowiązującym w Australii jest prawo Australii. Głupotę tej wypowiedzi komentowano w mediach, jednakże jest to jasny sygnał dla społeczeństwa, że rozwiązania polityków mogą opierać się wyłącznie na prawnej stronie zagadnienia, a nie technicznej. Przykładowo, można zabronić szyfrowania, ale biorąc pod uwagę fakt, że powszechnie wiadomo, jak sprawnie szyfrować, takie przepisy jedynie powstrzymają ludzi, którzy pragną postępować zgodnie z prawem z obawy przed reperkusjami. Przestępcy zaś, i tak działając poza prawem, nie mają nic do stracenia w użyciu tych dobrodziejstw. Prowadzi to do wniosku, że jedyne co stracimy na takich prawnych zabiegach, to prywatność zwykłych ludzi, i nie jest to coś, na co powinniśmy sobie pozwolić.

Warto pomyśleć też nad możliwym rozwojem sytuacji w Polsce. Niestety, żyjąc w świecie gdzie produkty i usługi są tworzone przez ludzi na całym świecie, możemy oczekiwać, że zmiana prawna w Stanach Zjednoczonych obejmie też polskich użytkowników, którzy codziennie wymieniają się wiadomościami za pomocą amerykańskich komunikatorów. Co gorsza, osłabione szyfrowanie bez żadnej zmiany prawnej, znacznie ułatwi dostęp do naszych danych rządowi Chińskiej Republiki Ludowej, Rosji, Izraelowi, czy innym państwom znanym z braku demokratycznego podejścia. Jest coś jednak, co możemy robić – szerzyć wiedzę wśród ludzi o tym, co jest technicznie możliwe, co nie jest, i co jest odpowiedzialne – i dać znać też o tym politykom, bo w końcu po to właśnie mamy w kraju d e m o k r a c j

3 https://csrc.nist.gov/Projects/post-quantum-cryptography
4 https://cr.yp.to/djb.html
5 https://www.hyperelliptic.org/tanja/