Cyber(nie)bezpieczeństwo a kryptografia kwantowa

Deklaratywnie cyberbezpieczeństwo jest jednym z podstawowych celów przy budowaniu systemów teleinformatycznych. Praktycznie dominuje jednak podejście, w którym podstawowym priorytetem jest uruchomienie określonych funkcjonalności i ich płynne działanie, zaś bezpieczeństwo bywa przeszkodą w realizacji tego celu.

Mirosław Kutyłowski

profesor na Wydziale Informatyki i Telekomunikacji Politechniki Wrocławskiej, założyciel Katedry Podstaw Informatyki i badań z zakresu kryptografii na tej uczelni. Przez lata był związany z: Uniwersytetem Wrocławskim (gdzie otrzymał wszystkie stopnie naukowe), Uniwersytetem Technicznym w Darmstadt, Instytutem Heinza Nixdorfa na Uniwersytecie Paderborn. Profesor wizytujący na Uniwersytecie Xidian.

Zajmuje się głównie tematyką wrogiej kryptografii, obroną przed słabymi punktami technologii kryptograficznych oraz rozwiązaniami implementowanymi na elektronicznych dokumentach tożsamości.

Reakcją na zagrożenia czy poważne incydenty bezpieczeństwa jest często nie konkretne działanie, ale poszukiwanie *Wunderwaffe* – cudownych technologii, które mają zniwelować skutki naszych zaniedbań. W sensie praktycznym niewiele zmieniają wymagania typu *privacy-by-design*. Już samo wprowadzenie do regulacji prawnych typu RODO tego typu wymagań jest dowodem, że fundamentalne zasady ochrony danych mogą być ignorowane.

Z drugiej strony finansowanie prac nad technologiami, które mogą doprowadzić do lockdownu systemów teleinformatycznych, jest co najmniej niezrozumiałe. Do technologii tego typu należy z pewnością zaliczyć kryptoanalizę kwantową. Powodzenie prac nad konstrukcją komputera kwantowego realizującego łamanie systemów opartych na RSA i DLP w skali produkcyjnej doprowadziłoby do olbrzymich perturbacji w obrocie gospodarczym, załamania się ochrony wielu systemów i powrotu do papierowych mechanizmów obrotu sprzed kilkudziesięciu lat.

Błędy podstawowe

Obrona przed katastrofalnymi zagrożeniami dla systemów teleinformatycznych to nie tylko budowa rozwiązań typu *post-quantum*. W istocie popełniamy bardzo wiele błędów o charakterze strategicznym, zwiększających o rząd wielkości skalę zagrożeń. Dotyczy to nie tylko kryptoanalizy kwantowej, lecz również bardziej konwencjonalnych ataków. Warto dodać, że niekonwencjonalne metody prowadzenia obliczeń, odmienne od modelu von Neumanna, nie są zarezerwowane dla komputerów kwantowych. Szczególnie groźne mogłoby się okazać metody wtórnie wykorzystujące powszechnie dostępny hardware w niekonwencjonalny sposób. Nie należy wierzyć, że metody takie nie pojawią się nieoczekiwanie, tak samo jak kilkanaście lat temu pojawiły się nieoczekiwanie nowe jakościowo ataki na funkcje hashujące.

Błąd 1: centralizacja. Implementacja systemu informatycznego jest zwykle dużo łatwiejsza, gdy wszystkie komponenty systemu są centralnie i bezpośrednio sterowalne. Dotyczy to wszystkich faz cyklu życiowego – od projektowania, przez realizację i administrację, do rozmontowania systemu. Centralne zarządzanie w znakomity sposób ułatwia szybkie reagowanie na zagrożenia i systematyczne likwidowanie odkrytych podatności.

Ułatwienia stwarzane są niestety również dla atakującego: redukcji ulegają koszty wrogich operacji przy jednoczesnym wzroście efektywności. Nie sposób zapomnieć o asymetrii środków – obrona systemu zwykle bazuje na skromnych środkach finansowych, występują niedobory wykwalifikowanego personelu, często osoby te są przesuwane do zadań o wyższym priorytecie dla decydentów – takich jak wygoda systemu z punktu widzenia klienta. Po stronie atakującego ograniczeniem jest zwykle tylko wielkość potencjalnych profitów wynikających z przeprowadzenia ataku, zaś środki do ataku mogą być alokowane przeciwko dowolnemu systemowi w skali globalnej.

Problemu nie rozwiązuje tworzenie systemów mirrorów. Manipulacje danych dokonane przez atakującego mogą być automatycznie replikowane na systemy zapasowe. Problemu nie rozwiązuje również zabezpieczenie danych wykorzystujące mechanizmy blockchaina jako struktury istniejącej w pojedynczej fizycznej lokalizacji. Taki blockchain w niczym nie utrudnia zniszczenia danych przez atakującego.

Strategią, która niebywale utrudnia zaatakowanie systemu, jest jego rozproszenie i zaimplementowanie mechanizmów samostabilizacji i samonaprawy. Oczywiście, budowa takich systemów jest o rzędy wielkości trudniejsza pod względem koncepcyjnym, jednak w efekcie zainfekowanie nawet sporej frakcji komponentów nie prowadzi do załamania się systemu i utraty wiarygodności dokumentów cyfrowych. Przykładem podejścia tego typu jest koncepcja European Identity Wallet – europejskiej tożsamości cyfrowej. W rozwiązaniu tym odchodzi się od centralistycznych systemów, dostarczających wiarygodnych danych o tożsamości, na rzecz agregacji uwierzytelnionych informacji z różnych źródeł w portfelu użytkownika i pod jego kontrolą.

Błąd 2: brak planu B. Systemy informatyczne zazwyczaj są budowane i testowane pod kątem sytuacji standardowych. W tym zakresie bardzo niebezpieczna jest wiara w siłę rozwiązań kryptograficznych jako nienaruszalnych i niezmiennych w czasie. Perspektywę złamania algorytmów kryptograficznych, na przykład w kontekście metod kryptoanalizy kwantowej, traktuje się jako problem do rozwiązania w przyszłości, w przypadku pojawienia się takiej sytuacji. Niestety, wtedy będzie za późno i trudno będzie opanować powstały chaos.

Obawy należy mieć nie tylko ze względu na rozwój kryptoanalizy, w szczególności kwantowej. Przykładem krytycznego obszaru jest digitalizacja wielu kluczowych rejestrów danych i oparcie ich na standardowych systemach bazodanowych. Systemy takie niekoniecznie biorą pod uwagę niestandardowe zagrożenia, takie jak choćby możliwość fałszowania podpisów cyfrowych/pieczęci elektronicznych uwiarygadniających poszczególne wpisy (o ile w ogóle takie zabezpieczenia się wprowadza). W przypadku systemów takich jak księgi wieczyste, digitalizacja powinna być poprzedzona budową odpowiedniej infrastruktury typu *distributed ledger*, nie tylko uniemożliwiającej modyfikację już wprowadzonych rekordów (modyfikacja tylko w trybie append), lecz także pozwalającej na zrekonstruowanie rejestru z rozproszonych

części przechowywanych przez niezależnych uczestników. Wiarygodna rekonstrukcja powinna być możliwa nawet wtedy, gdy część uczestników jest nieuczciwa i pragnie zrekonstruować dane w nierzetelny sposób na swoją korzyść.

Jedną z zasad, która powinna obowiązywać w przypadku rozwiązań kryptograficznych, jest implementacja systemów automatycznie wykazujących, że system został skutecznie zaatakowany. Przykładem takiego pragmatycznego podejścia jest system podpisów elektronicznych realizowanych przez estońskie dokumenty tożsamości. Po pierwsze – rozproszono generowanie i użycie klucza podpisującego pomiędzy obywatela a serwer (plan B wobec groźby dostarczenia przez producenta kart kryptograficznych z zapadkami z jednej strony, a groźbą nieuczciwego wykorzystania podpisów serwerowych przez podmioty kontrolujące je – z drugiej strony), po drugie – zaimplementowano *nonces* w procesie generowania podpisu w taki sposób, by wykrywać nie tylko nieautoryzowane użycie, lecz także pojawienie się klonów elektronicznego dokumentu tożsamości.

Niewątpliwie hasła eliminacji gotówki z obrotu gospodarczego i oparcia obrotu finansowego na niewielkiej liczbie organizacji obsługujących rynek są krańcowym przykładem działania bez planu B, gdzie pojedyncze zdarzenie technologiczne (na przykład budowa efektywnych narzędzi podrabiania kodów MAC) może doprowadzić do załamania elektronicznej wymiany danych.

Błąd 3: tolerowanie produktów niebezpiecznych. Tak jak wiele innych nowoczesnych technologii, kryptografia, a w tym metody kwantowe, są nie tylko szansą, lecz także zagrożeniem. Kryptografia może chronić użytkownika, ale i w perfidny sposób służyć do atakowania go. Do użytku wszedł termin *malicious cryptography*, oznaczający wykorzystanie zaawansowanych metod nie tylko do zaatakowania, lecz także do skutecznego zamaskowania ataku. Niestety, mamy do czynienia z technikami, które w dowodliwy sposób zapewniają niewykrywalność – przynajmniej na poziomie klasycznej analizy inputu i outputu.

Kryptowaluty pozwalają na wolny obrót bardzo dużymi sumami i częstokroć zapewniają wysoki poziom anonimowości. Bez kryptowalut poziom zagrożenia atakami typu *ransomware* byłby zdecydowanie niższy, ze względu na trudności odebrania okupu w sposób bezpieczny dla przestępcy.

Wiele problemów wiąże się z używaniem narzędzi informatycznych w sposób nieodpowiadający istniejącym ryzykom z jednej strony, a własnościom narzędzi – z drugiej (na przykład smartfonów). W kontekście metod kryptograficznych istnieje tendencja do zastępowania twardej analizy bezpieczeństwa założeniami przyjmowanymi ad hoc. Dobrym przykładem jest sposób interpretacji norm FIPS 140-2 dla modułów kryptograficznych. Zamiast rozumienia ich jako *warunków koniecznych* (implementacja dobrych praktyk), posiadanie certyfikatu FIPS 140-2 bywa interpretowane jako *warunek wystarczający* dla zapewnienia bezpieczeństwa modułu i jego zastosowania.

> *Sztandarowym przykładem niekonsekwencji w działaniu jest z jednej strony zaostrzanie rygorów związanych z praniem brudnych pieniędzy, a z drugiej – tolerowanie rozwoju narzędzi znakomicie wspierających takie działania. Za przykład mogą posłużyć kryptowaluty.*

Catacrypt

Kilka lat temu powstał termin *catacrypt* jako skrót utworzony ze słów *katastrofa* i *kryptografia*. Nie brak opinii, że w istocie niekontrolowany i mało odpowiedzialny sposób budowy systemów informatycznych doprowadził do sytuacji, gdy w wielu obszarach istnieje sytuacja analogiczna do złamania podstawowych założeń kryptograficznych za sprawą powstania komputera kwantowego. Brak wykorzystania istniejących ścieżek ataku na szerszą skalę może być krokiem czysto taktycznym – nie zawsze istniejące możliwości wykorzystuje się natychmiast, ale czeka się na najbardziej odpowiedni moment. Jest to szczególnie ważne w przypadku zastosowań militarnych.

Zasada najsłabszego ogniwa łańcucha

Tak jak w każdej innej dziedzinie, obrona przed cyberatakiem powinna brać pod uwagę najsłabsze punkty systemu, a nie jego najmocniejsze strony. Niestety, w praktyce zbyt często upajamy się zaletami najbardziej dojrzałych komponentów, ignorując czasami fundamentalne słabości i nierozwiązane problemy innych składników tego samego systemu. Epatowanie zaletami najsilniejszych komponentów daje z jednej strony fałszywe poczucie bezpieczeństwa, a z drugiej strony jest cenną wskazówką dla atakującego, które scenariusze ataku są mało obiecujące i które komponenty atakujący powinien po prostu obejść, nie tracąc czasu na ich złamanie.

Dobrym przykładem jest skądinąd genialnie prosty protokół BB84 uzgadniania klucza drogą transmisji kwantowej. Przypomnijmy, że podstawową siłą tego schematu jest możliwość kwantowego przesyłania bitów w taki sposób, że atakujący *man-in-the-middle* przy próbie odczytu zmie-

nia wartość bitu z prawdopodobieństwem 0.25. Wynika to z faktu, że wysyłający i odbiorca, nazwijmy ich tradycyjnie Alicją i Bobem, wybierają przy przesłaniu każdego bitu jedną z dwóch baz do kodowania. Robią to niezależnie, bez jakiegokolwiek uzgadniania w tej fazie protokołu. W końcowej fazie do konstrukcji klucza sesyjnego brane będą tylko te bity, gdzie wybór bazy przez Alicję był taki sam jak wybór Boba. Z kolei, jeśli atakujący, nazwijmy go tradycyjnie Mallet, podsłuchuje komunikację, to aby odczytać wartość przesyłanego bitu, musi zdecydować się na jedną z baz. Jeśli wybierze inną bazę niż Alicja, to poprzez odczyt zmieni wartość przesyłanego bitu z prawdopodobieństwem 0.5. Tu kryje się pułapka na Malleta: w kolejnej fazie protokołu Alicja ujawnia Bobowi (już tradycyjnym kanałem) wybór bazy dla każdego bitu oraz wartości pewnej liczby bitów z losowo wybranych pozycji. Dzięki temu Bob może sprawdzić, czy ktoś po drodze nie zmienił wartości tych ujawnionych bitów poprzez błędny wybór bazy.

> *Tak więc BB84 nie jest w istocie protokołem uniemożliwiającym podsłuchiwanie komunikacji. Jest to protokół, który wykrywa podsłuch w kwantowym kanale komunikacji. Dzięki temu wydaje się, że omijamy wszystkie problemy występujące w klasycznej komunikacji radiowej, gdzie Mallet po prostu włącza odpowiedni odbiornik.*

Jak zwykle, diabeł tkwi w szczegółach i protokół BB84 jako taki nie stanowi wystarczającego zabezpieczenia. Najprostszy atak wiedzie poprzez urządzenie Alicji służące do generowania pomocniczych wartości losowych. Jeśli Mallet jest w stanie przewidzieć te wartości losowe, to cała argumentacja o wykrywaniu aktywności podsłuchującego wali się. Na przykład, gdy Mallet jest w stanie przewidzieć, które pozycje zostaną użyte do wykrycia podsłuchu, może po prostu nie ingerować w transmisję w tych momentach.

Jak widzimy, BB84 w krytyczny sposób zależy od generatora wartości losowych. Ten nie jest już związany w jakikolwiek sposób z mechanizmami kwantowymi i tym samym powracamy do starego problemu bezpieczeństwa klasycznych systemów informatycznych. Warto dodać, że nawet gdy odpowiedni generator jest zaszyty w bezpiecznym urządzeniu uniemożliwiającym infiltrację na drodze technicznej, to atakującym może być producent. Dzięki ujawnianiu dużej liczby wartości losowych w protokole BB84 bardzo łatwo jest zaimplementować podręcznikowy wyciek wewnętrznego stanu generatora metodami kleptograficznymi.

Jak widać, bezpieczeństwo uzgadniania klucza za pomocą protokołu Charlesa Bennetta i Gileada Brassarda wcale nie musi być wyższe niż w przypadku powszechnie stosowanego protokołu Diffie-Hellmana: oba są bezsilne, gdy generator wartości losowych Alicji został skutecznie zaatakowany. Tyle, że wykonanie protokołu Diffie-Hellmana prawie nic nie kosztuje…

Dokąd zmierzamy?

Na pewno konieczna jest koncentracja wysiłku na krytycznych obszarach i najbardziej pragmatycznych rozwiązaniach. Wymaga to, niestety, odważnego przedefiniowania priorytetów. Zarówno środowisko naukowe, przemysłowe, jak i działania podmiotów publicznych muszą przezwyciężyć swe przyzwyczajenia czy też partykularne interesy.

Dla przykładu, w środowisku naukowym badania są rozwijane bardzo często siłą inercji i podstawowym kryterium oceny jest poziom wyników, liczba punktów, cytowań itp., a niekoniecznie ich użyteczność.

Jakkolwiek systemy ewaluacji nauki zdają się zmieniać w dobrym kierunku, wiele jest w tym względzie do poprawy. Podobnie naturalnym procesem w sektorze gospodarczym jest maksymalizacja zysku, a niekiedy nawet dostarczanie produktów, które nie są trwale bezpieczne.