Piotr Przybyła
Instytut Podstawowych Problemów Techniki PAN

Kryzys kryptograficzny

Kryzys kryptograficzny (nazywany również trzecią bańką internetową, kryzysem jednego dolara lub oszustwem eliptycznym) to jedno z najistotniejszych zjawisk dwudziestego pierwszego wieku, które nie tylko stanowiło wstrząs dla ówczesnej gospodarki światowej, ale także wyznaczyło kierunek rozwoju techniki na następne dziesięciolecia.

Trudno jednoznacznie wskazać przyczyny Kryzysu. Z perspektywy czasu wydaje się, że wielkie znaczenie miała rozpowszechniająca się w latach 2010-2017 tzw. paranoja prywatności. Spowodowana była nie tyle rozwojem cyberprzestępczości, ile raczej postępującym procesem przenoszenia coraz większej części aktywności ludzkiej do sieci. Wzrastała także świadomość użytkowników, pobudzana przez takie urządzenia, jak CopperSniffer, umożliwiające podsłuchiwanie łącz kablowych, do tej pory uważanych za bezpieczne. Panowało powszechne przekonanie, że wszystkie transmisje w Internecie powinny być szyfrowane; nie tylko na poziomie warstwy sieciowej (IPSec, później IPv6) ale także aplikacji (HTTPS, POP3S etc.). Dotychczasowa pewność, że wystarczy chronić transmisje bankowe, ewentualnie przesył haseł, stawała się bardzo niemodna.

W tych okolicznościach następował również szybki rozwój technik kryptograficznych. Dotychczas powszechnie używany algorytm RSA powoli odchodził w niebyt. Ponieważ udało się utrzymać tempo miniaturyzacji jednostek obliczeniowych (tranzystor grafenowy, 2015) długość klucza, uznawana za bezpieczną, stale rosła. Z drugiej strony zdawano sobie sprawę z faktu, że nie stanowi on żadnego zabezpieczenia wobec komputerów kwantowych (algorytm Shora, 1995). Wobec powyższego wdrażano algorytmy oparte na krzywych eliptycznych (np. w IPv6.1 , 2013; IEEE 802.11s , 2014) które pracowały na krótszych kluczach i opierały się atakom.

Z drugiej strony, obawy te zdawały się być trochę na wyrost. Ewolucja komputerów kwantowych przebiegała w iście ślimaczym tempie. Dotychczasowe podejścia do tematu stwarzały ogromne problemy przy próbach zwiększania ich mocy obliczeniowej (ukuto nawet prześmiewcze hasło *one bit every 24 months*). Użycie kryptografii kwantowej do ochrony łącz pozostawało kosztownym luksusem, a nie powszechną techniką. Istniejące łącza, na które mogły sobie pozwolić jedynie duże banki, i tak były zabezpieczane także tradycyjnymi algorytmami „na wszelki wypadek”.

Prawdziwa rewolucja nadeszła w roku 2018 wraz z pracami prof. Rigauta z Uniwersytetu w Grenoble. Zaproponował rozwinięcie techniki przechowywania qubitów w kropkach kwantowych i pokazał, jak można użyć technik ich rozmieszczania w półprzewodniku (tzw. *precise epitaxy*, 2016), by powstała odpowiednia dwuwymiarowa matryca. Przy użyciu precyzyjnie sterowanej fali elektromagnetycznej możliwe stało się kontrolowanie stanu elektronów nawet w układzie zawierającym setki kropek. Najistotniejsze w jego pracach nie były jednak szczegóły techniczne, które później ulegały wielokrotnym zmianom, ale pomysł, by

użyć istniejącej technologii epitaksjalnej. Umożliwiło to dostosowanie linii produkcyjnych wiodących producentów układów (którymi stały się AMD i NVIDIA po wyparciu CPU przez GPGPU nowej generacji) do wytwarzania nowych elementów.

Pierwsze moduły kwantowe (karty QUANTAS 100) trafiły do komputerów konsumentów w styczniu 2019 roku (dla zastosowań rozrywkowych). RSA od dawna stanowił już eksponat muzealny, jednak powszechność dostępu do urządzeń kwantowych spowodowała niechciany przełom. Chińsko-amerykańska grupa naukowców (o nazwiskach nieznanych do dziś) zdołała z ich użyciem złamać powszechnie stosowaną w transmisjach internetowych rodzinę algorytmów EEC (*Enhanced Elliptic Coding*, 2014). Ze względu na wagę odkrycia i dla uniknięcia niepotrzebnej paniki rządy ChRU (Zjednoczone Republiki Chińskie od rewolucji w 2013) i USA zdecydowały wspólnie, że grupa ta nie opublikuje algorytmu, dopóki nie dowiedzie bezsprzecznie jego skuteczności przez deszyfrację i modyfikację transmisji bankowej. Niestety eksperyment się powiódł i 30 kwietnia 2020 roku jeden dolar amerykański zniknął z konta prezydenta ChRU i odnalazł się na koncie organizacji ekologicznej walczącej o reintrodukcję pandy wielkiej (PNPU).

W tej sytuacji chińsko-amerykański komitet sterujący złamał umowę z naukowcami i zabronił im dalszego zajmowania się tematem. Najprawdopodobniej jeden z nich sprzeciwił się i opublikował algorytm w Internecie. Choć mało kto rozumiał opis w zawiłym technicznym chińskim, internauci rozprzestrzenili go po całym globie w ciągu kilku godzin. W odpowiedzi rząd amerykański nakazał IANA (*Internet Assigned Numbers Authority*) odłączenie głównych serwerów DNS, de facto unieruchamiając światowy Internet. Przez 34 godziny świat był pozbawiony osiągnięć globalizacji – nie wydawano żadnych gazet międzynarodowych ani ogólnokrajowych, telewizja satelitarna, telefony komórkowe nie działały (tzw. wielka majówka).

Po ponownym podłączeniu serwerów zapanował nieopisany chaos. Utrzymywanie szyfrowanych transmisji nagle stało się pozbawione sensu. Część dostawców usług internetowych po prostu zawiesiła działalność. Inni zdołali wytłumaczyć użytkownikom, że naprawdę nie potrzebują szyfrowania w portalach społecznościowych czy poczcie internetowej. Głównym motorem kryzysu były jednak instytucje finansowe. Banki zamknęły internetowe systemy transakcyjne i nakazały klientom korzystanie z oddziałów. Wielu z nich nie wiedziało, że takie w ogóle istnieją. W efekcie powstała panika i w samej tylko Unii Europejskiej 56 banków ogłosiło niewypłacalność.

Wszystkie światowe giełdy, oprócz Zurychu (gdzie transmisja z domami maklerskimi była chroniona kryptografią kwantową) ogłosiły „przerwę techniczną” do czasu wdrożenia tymczasowego systemu opartego na szyfrze Vernama, co trwało wiele miesięcy. Szacuje się, że w okresie pierwszych 4 miesięcy około 24% przedsiębiorstw z USA, UE i ChRU ogłosiło upadłość. Jedynie firmy ochroniarskie notowały zyski (ochrona transferu kluczy). Długofalowym efektem Kryzysu stało się znaczne ograniczenie skali konsumpcji w krajach wysoko rozwiniętych – wszystko, co wymagało transmisji danych stało się nagle bardzo kłopotliwe. Przez następne lata nie opracowano algorytmu szyfrowania, który oparłby się atakom. Dopiero w 2026 Arjun Rampal udowodnił, że nie istnieje szyfr asymetryczny, którego nie dałoby się złamać w czasie wielomianowym z użyciem GQC (*Generalized Quantum Computer*).