Kiedy możemy czuć się bezpieczni?

Zawodowo zajmuję się kryptologią, czyli dziedziną nauki badającą różne aspekty bezpieczeństwa cyfrowego świata. Jest to nauka ścisła, czyli taka, w której królują stricte matematyczne rozumowania. Solą matematyki są, oczywiście, dowody. Również główne wyniki kryptologiczne to właśnie twierdzenia i ich dowody. A twierdzenie to para: założenie i teza. W kryptologii teza zwykle jest podobna: proponowany system jest bezpieczny. Ciekawym i ważnym pytaniem jest jednak wątpliwość: ale przy jakich założeniach?!

I tutaj staramy się być tak paranoiczni, jak to tylko możliwe.

Pierwszą regułą, którą wyznaje środowisko kryptologiczne, jest tak zwana zasada Kerckhoffsa (z roku 1883), czyli zasada, że *wróg zna system*. To założenie mówi, że system powinien być bezpieczny, nawet jeśli nasz przeciwnik (cracker, podsłuchiwacz) zna cały protokół, a jedyne, co pozostaje dla niego tajemnicą, to *klucz kryptograficzny*. Motywacja dla takiego założenia jest dość jasna. Komunikujemy się zwykle nie raz, a wielokrotnie. Nie sposób w praktyce wymyślać i używać nowego protokołu do każdego pojedynczego aktu komunikacji. W związku z tym używa się za każdym razem tego samego systemu, ALE ten system nie jest jednoznaczny, tylko zależy od jakiegoś ciągu bitów, zwanego kluczem. Ponieważ system używany jest wielokrotnie i przez wielu użytkowników, to powinniśmy się liczyć z tym, że – prędzej czy później – zostanie przechwycony i stanie się znany przeciwnikowi. Użytkownicy systemu nie powinni się jednak tej sytuacji obawiać, powinni tylko pilnować swoich kluczy. Więcej, owe klucze można starać się często zmieniać, co jeszcze dodatkowo podnosi bezpieczeństwo (oczywiście, w klasycznych szyfrach pojawia się wtedy problem bezpiecznego ustalenia wspólnego klucza).

Dokładnie w ten sposób działa np. nowoczesne szyfrowanie AES (*Advanced Encryption Standard*) czy inne popularne szyfry symetryczne. Środowisko kryptologów bynajmniej nie próbuje utrzymać w tajemnicy sposobu działania AES-a. Wręcz odwrotnie – system powstał w wyniku jawnego konkursu (w roku 1997), w którym każdy mógł zgłosić (publicznie!) swojego kandydata na szyfr, a ostatecznego wyboru dokonał amerykański instytut NIST. Wygrała propozycja Vincenta Rijmena i Joana Daemena, której szczegóły można znaleźć chociażby w Wikipedii.

Można by sobie, oczywiście, zadać na boku pytanie, czy – tak *na wszelki wypadek* – nie opłacałoby się utajnić również sam system. Powszechnie uważa się, że jest to jednak zły pomysł! Dlaczego? Wierzy się, że system, który ma luki, a jest upubliczniony przed wprowadzeniem do użycia, zostanie skutecznie *zaatakowany* przez społeczność kryptologiczną, zanim jego używanie mogłoby narazić kogoś na straty. Utajnienie systemu pozbawia nas szansy na taką darmową, *środowiskową* weryfikację.

Ale wróćmy do dyskusji na temat założeń. Na razie przyjrzeliśmy się założeniu, że wszystkie szczegóły działania systemu (poza kluczami) są znane przeciwnikowi. Dodatkowo, kryptolodzy powszechnie zakładają również, że cała komunikacja między stronami protokołu może zostać podsłuchana.

Od razu uspokójmy Czytelnika – pomimo że te założenia wydają się bardzo silne, to istnieje wiele protokołów (nie tylko szyfrowanie, ale i podpis cyfrowy, i wiele innych), które są bezpieczne przy założeniu o przeciwniku dokładnie takim jak wyżej (i przy kilku dość wiarygodnych założeniach z dziedziny algorytmiki). Spójrzmy jednak na problem z drugiej, paranoicznej strony i zadajmy sobie pytanie: czy powyższy zestaw założeń (przypomnijmy: wróg zna system i może podsłuchiwać całą komunikację) nie jest, być może, i tak za słaby? To znaczy, czy powyższy *model* dobrze opisuje realia świata i uwzględnia wszystkie sytuacje, w których chcemy się cyfrowo komunikować?

W tym miejscu przebijmy balon suspensu i napiszmy wprost: czasem nawet i ten model jest za słaby! Wszystkiemu *winna* jest ludzka głowa, która nie potrafi ani zapamiętać kilkusetcyfrowych kluczy, ani wykonywać szybko obliczeń na liczbach tego rozmiaru, czego wymaga większość protokołów. Wyręczamy się urządzeniami (smartfonami, kartami płatniczymi, komputerami osobistymi), a te podatne są na ataki nieobjęte w wyżej opisanym modelu! (Nie są przecież zespawaną ołowianą skrzynką, do której tylko wchodzą i wychodzą pakiety komunikacji.)

Może się przecież zdarzyć, że nasz komputer został zainfekowany wirusem, który przejmie kontrolę nad naszym sprzętem i wykradnie nasz klucz trzymany w pamięci komputera. W takiej sytuacji (pełna kontrola przeciwnika nad sprzętem) raczej trudno o nadzieję na bezpieczeństwo. Ale w praktyce często przeciwnik *czegoś* się dowie o naszym urządzeniu, ale nie wszystkiego. Na przykład jest w stanie wykraść tylko jakąś część pamięci komputera. Albo jest w stanie mierzyć pobór mocy karty płatniczej podczas interakcji z bankomatem. Albo może nagrać dźwięk (sic!), który wydaje procesor podczas procesu szyfrowania danych. Dla każdego z powyższych przypadków istnieją protokoły kryptologiczne bezpieczne w standardowym sensie, ale złamane przy obecności opisanej dodatkowej wiedzy przeciwnika (tzw. wycieku). Stanowi to, oczywiście, bezsporną motywację do dyskusji na temat założeń odnośnie przeciwnika w twierdzeniach postulujących bezpieczeństwo różnych rozwiązań.

Kryptolog zawsze powinien oddychać możliwie rozrzedzonym powietrzem. Próbujemy definiować przeciwnika możliwie najsilniejszym, nawet jeśli wydaje się to skrajnie przesadzone (np. zakładamy, że przeciwnik może poznać wartość **dowolnie wybranej przez siebie** funkcji stanu pamięci urządzenia, o ile tylko wartość tej funkcji nie zdradzi więcej niż 90% całości). Sloganowo można by to uzasadnić, pisząc, że przecież czego przestępca nie umiał wczoraj, zrobi jutro. I wcale to nie jest pretensjonalne hasełko. Naprawdę ciężko było kiedyś nawet przypuścić, że dźwięk wydawany przez urządzenie szyfrujące może być jakoś zależny od klucza w nim zapisanego!

Lubię myśleć, że kryptolodzy po prostu sprzedają *pakiety ubezpieczeniowe*. Oczywiście, nigdy żaden nie zabezpieczy nas od wszystkiego, ale stale staramy się poszerzać ich zakres. Z drugiej strony – przeciwnicy też mają coraz potężniejsze narzędzia do ataku... Skojarzenie z kotkiem i myszką narzuca się niemal ostentacyjnie.

Tomasz KAZANA