SAMOTESTUJĄCA SIĘ MASZYNA DO SZYFROWANIA

Jak zapewnić cyberbezpieczeństwo obywatelom i firmom? To wyzwanie, z którym mierzą się dziś zarówno organizacje rządowe, jak i prywatni przedsiębiorcy. Jednym z ważniejszych aspektów tego problemu jest niemożność zaufania dostawcom urządzeń używanych do szyfrowania. Zdarza się, że maszyny te zawierają w sobie tzw. konie trojańskie. Nad rozwiązaniem tego ambarasu pracuje dr inż. Marcin Pawłowski z Zakładu Optyki i Informacji Kwantowej Wydziału Matematyki, Fizyki i Informatyki Uniwersytetu Gdańskiego w ramach grantu uzyskanego w programie FIRST TEAM 1/2016 realizowanym przez Fundację na rzecz Nauki Polskiej ze środków Programu Operacyjnego Inteligentny Rozwój.

Skąd wynika problem ograniczonego zaufania do dostępnych obecnie na rynku maszyn do szyfrowania? „Stąd, że wystarczy zmiana domieszek półprzewodników w kilku tranzystorach mikroprocesora takiej maszyny, żeby osoba, która tej zmiany dokonała, była w stanie zdekodować każdą wiadomość zaszyfrowaną przy jej użyciu. Taka modyfikacja dokonana na etapie produkcji jest praktycznie niemożliwa do wykrycia, a jest to tylko jedna z wielu znanych metod wprowadzania koni trojańskich do urządzeń szyfrujących. Rozwiązaniem może być pełna kontrola nad procesem produkcji sprzętu do szyfrowania – od fazy projektowej aż po wykonanie każdej części każdego podzespołu. Ale pozwolić sobie na taką kontrolę mogą jedynie wielkie agencje rządowe, dla przedsiębiorstw jest to praktycznie niewykonalne” – wyjaśnia dr Marcin Pawłowski.

Możliwe jest jednak, przy wykorzystaniu mechaniki kwantowej, zbudowanie urządzenia, które podczas pracy, bezustannie, samo się testuje. Jeśli takie urządzenie chciałoby zaszyfrować dane w nie dość bezpieczny sposób i przejść swój własny test, musiałoby złamać prawa rządzące mechaniką kwantową. Ciągle przeprowadzane badanie sprawności nie tylko uniemożliwia umieszczenie koni trojańskich, ale także natychmiast wykrywa każdą usterkę, która powstaje podczas pracy maszyny. A zatem samotestujące urządzenia są, z definicji, niezawodne. Celem projektu dr. inż. Marcina Pawłowskiego jest zbudowanie prototypów takich urządzeń.

„W założeniu prototypy przez nas zaprojektowane mają być na tyle proste i tanie, aby ich zakup i obsługa były w zakresie możliwości małych i średnich przedsiębiorstw. Zapewni im to poziom bezpieczeństwa danych porównywalny z takim, który obecnie dostępny jest wyłącznie dla agencji wywiadowczych. Szeroki dostęp do tanich i niezawodnych systemów kryptograficznych może znacznie zmniejszyć cyberprzestępczość i wspomóc gospodarkę na światową skalę” – podsumowuje dr Pawłowski.

Dr inż. Marcin Pawłowski studiował ekonomię i zarządzanie oraz fizykę techniczną na Politechnice Gdańskiej, a następnie doktoryzował się z informatyki kwantowej na Uniwersytecie Gdańskim. Dzięki stypendium brytyjskiego *Engineering and Physical Sciences Research Council (*EPSRC) odbył kilkuletni staż naukowy w Bristolu. Po powrocie do Polski, założył grupę badawczą na Uniwersytecie Gdańskim.

Fundusze Europejskie Inteligentny Rozwój
FNP Fundacja na rzecz Nauki Polskiej
Unia Europejska Europejski Fundusz Rozwoju Regionalnego