KRYPTOGRAFIA KONTRA SPRZĘTOWE KONIE TROJAŃSKIE

Dr hab. Stefan Dziembowski, prof. UW z Instytutu Informatyki Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego pracuje nad stworzeniem mechanizmów obrony przed zagrożeniami wynikającymi z outsourcingu produkcji układów scalonych, stosowanych w sprzętach elektronicznych. Ze względu na złożoność tych układów, sprawdzenie czy producent wytworzył je prawidłowo jest bardzo trudne. A nieuczciwy producent może zmienić działanie urządzenia, poprzez wprowadzenie do niego złośliwych modyfikacji, nazywanych sprzętowymi koniami trojańskimi. Celem projektu finansowanego w programie TEAM 1/2016, realizowanym przez Fundację na rzecz Nauki Polskiej w ramach Programu Operacyjnego Inteligentny Rozwój, jest opracowanie technik zapobiegającym tego typu zagrożeniom.

Urządzenie z wprowadzonym przez nieuczciwego producenta koniem trojańskim może spowodować znaczne szkody dla jego użytkowników, np. poprzez kradzież prywatnych danych, czy własności intelektualnej. Biorąc pod uwagę ogromne uzależnienie współczesnego społeczeństwa od urządzeń elektronicznych, problem ten nabiera wielkiej wagi. Metody przeciwdziałania zagrożeniom związanym z outsourcingiem produkcji układów scalonych są od kilku lat intensywnie badane przez naukowców zajmujących się bezpieczeństwem sprzętowym. Dotychczas w pracach tych nie były jednak powszechnie stosowane zaawansowane metody kryptograficzne.

„W naszym projekcie spojrzymy na to zjawisko z punktu widzenia kryptograficznego. W ciągu ostatnich 2-3 dekad stworzonych zostało wiele narzędzi kryptograficznych, które zwiększają bezpieczeństwo obliczeń wykonywanych na urządzeniach, a nie tylko komunikacji między urządzeniami (co było tradycyjnym celem kryptografii). W ramach projektu zajmiemy się dostosowaniem tych metod do przeciwdziałania tego rodzaju atakom sprzętowym” – mówi dr hab. Stefan Dziembowski.

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

Dr hab. Stefan Dziembowski, prof. UW jest informatykiem, specjalizującym się w kryptografii. Studia informatyczne ukończył na Uniwersytecie Warszawskim, stopień doktorski uzyskał na duńskim Uniwersytecie w Aarhus, habilitację otrzymał na Uniwersytecie Warszawskim. Staże podoktorskie odbył na szwajcarskiej Politechnice Federalnej w Zurychu, w CNR w Pizie oraz na Uniwersytecie La Sapienza w Rzymie. Swoje prace publikował na takich konferencjach jak CRYPTO, Eurocrypt, STOC, FOCS, IEEE S&P, czy CCS oraz w czasopismach takich jak m.in. „Journal of Cryptology", „IEEE Transactions on Information Theory", oraz „Communications of the ACM". Laureat stypendium Marie Curie, kierownik grantów finansowanych przez Europejską Radę ds. Badań Naukowych (ERC), Fundację na rzecz Nauki Polskiej oraz Narodowe Centrum Nauki (NCN). Wyróżniony m.in. Nagrodą dla Młodego Naukowca im. Prof. Kazimierza Bartla przyznawaną przez Fundację im. Prof. K. Bartla.

Na zdjęciu: Dr hab. Stefan Dziembowski, fot. Michał Jędrak

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