Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience

Wyniki w skrócie

Nowe narzędzia do zabezpieczania urządzeń wbudowanych

Zwykły układ scalony można zhakować, więc producenci starają się opracowywać różnego rodzaju środki zabezpieczające. Jednak uczciwa ocena takich zabezpieczeń jest procesem złożonym.

GOSPODARKA CYFROWA

BEZPIECZEŃSTWO

© Hamik, Shutterstock

Tak zwane urządzenia wbudowane to proste układy scalone zaprojektowane z myślą o wykonywaniu jednego zadania i umieszczane w przedmiotach codziennego użytku. Znajdziemy je na przykład w kartach kredytowych czy kluczykach samochodowych, dzięki którym można zdalnie otworzyć określony pojazd.

Mimo że urządzenia te stosują szyfrowanie, nadal są podatne na złamanie ich zabezpieczeń. Zwykła deszyfracja (na przykład zaszyfrowanych wiadomości e-mail) wykorzystuje mechanizm analizowania wiadomości wysłanej i otrzymanej, co sprawia, że bezpośrednie uzyskanie klucza szyfrowania jest trudne. Ale w przypadku wbudowanego układu scalonego haker ma fizyczny dostęp do urządzenia. Przy zastosowaniu odpowiednich sygnałów wejściowych i odbiorze sygnałów wyjściowych sam pomiar mocy pobieranej podczas ich przetwarzania może ostatecznie ujawnić klucz kryptograficzny.

To tak zwane ataki side channel. Producenci inteligentnych kart płatniczych podjęli pierwsze prace nad zabezpieczeniem kluczy kryptograficznych przed ujawnieniem już w latach 90. XX wieku.

Problem polega na tym, że trudno ocenić ich skuteczność. W branży do tej pory nie osiągnięto zgody co do wyboru najlepszych metod i jak dotąd nie istniała metoda pozwalająca porównywać różne rodzaje mechanizmów oceny. Oceny te są zazwyczaj złożone (ponieważ natura ataków ulega ciągłej komplikacji) i wymagają znacznej ilości obliczeń, co oczywiście sprawia, że są drogie.

Lepsze zabezpieczenia

W ramach finansowanego ze środków UE projektu REASSURE opracowano usprawnione metody oceny środków chroniących przez złamaniem zabezpieczeń urządzeń wbudowanych. Pierwszymi celami ataków są teraz urządzenia mające połączenie z Internetem rzeczy (IoT), jednakże ich producentom brak doświadczenia i sprzętu niezbędnych do oceny jakości wprowadzonych zabezpieczeń. Aby pomóc producentom, naukowcy pracujący nad projektem REASSURE opracowali zautomatyzowane narzędzia sprawdzające kod, przeznaczone dla programistów IoT. Badacze dostarczyli także pełen zestaw dodatkowych narzędzi programowych i przygotowali program szkolenia.

Opracowane przez inżynierów narzędzia powstały specjalnie z myślą o firmach tworzących urządzenia wbudowane i tworzących ich zabezpieczenia. Firma musi najpierw przeprowadzić wewnętrzną ocenę skuteczności wprowadzonych zabezpieczeń. Następnie zgłasza się do laboratorium potwierdzającego, które prowadzi niezależne badania nad odpornością urządzenia na ataki typu „side channel”. Dr Francois Koeune, koordynator projektu, wyjaśnia: „Ponieważ ocena zewnętrzna jest drogim przedsięwzięciem, w interesie obu stron leży jak największe usprawnienie tego procesu”.

Nowe narzędzia dają większą pewność niż stosowane dotychczas metody oceny i z większym prawdopodobieństwem pozwolą wskazać słabe punkty zabezpieczeń. Dzięki tym narzędziom niezależne laboratorium będzie mogło utrzymać certyfikację w zakresie prowadzenia tego typu ocen.

Większa wydajność

W czasie realizacji projektu partnerzy przemysłowi wdrażali proponowane rozwiązania narzędziowe, niejednokrotnie przyczyniając się do znaczących postępów w pracach. W najlepszych przypadkach narzędzia pozwoliło zredukować liczbę śladów niezbędnych do przeprowadzenia analizy do 10- i 16-krotnie

zmniejszyć zużycie mocy podczas obliczeń. Nowe narzędzia są także pomocne podczas ponownej oceny produktu po wykryciu luki w zabezpieczeniach. Dzięki nim jeden z partnerów zdołał pominąć połowę podejmowanych zwykle podczas testów działań bez utraty jakości zabezpieczeń. Narzędzia okazały się być też bardziej wszechstronne i w 10 % ocen wewnętrznych pozwoliły wykryć luki w zabezpieczeniach, jakich wcześniej nigdy nie wykrywano na tym etapie.

Koeune dodaje: „W tej dziedzinie istnieje też norma ISO, która w czasie trwania naszego projektu weszła w fazę poprawek. „Dostarczyliśmy dokumentację wskazującą na to, co naszym zdaniem jest istotną słabością obowiązującej normy". The Międzynarodowa Organizacja Standaryzacyjna uznała nasze uwagi i udostępni normę do poprawy. Narzędzia REASSURE oraz szkolenie w zakresie korzystania z nich wprowadzą znaczący postęp w zakresie zabezpieczania tych obecnych powszechnie w naszych życiach urządzeń".

Słowa kluczowe

REASSURE | narzędzia | zabezpieczenia | urządzenia wbudowane | bezpieczeństwo | ocena | hakowanie | atak typu „side channel"

Znajdź inne artykuły w tej samej dziedzinie zastosowania

Nowa architektura zwiększa wydajność energetyczną i wydajność pasma na potrzeby bezprzewodowej komunikacji w ramach Internetu rzeczy

29 Sierpnia 2018

Kompleksowe podejście do kwestii cyberbezpieczeństwa

22 Października 2021

Współpraca firm zajmujących się technologią blockchain

14 Października 2022

Ochrona prywatności i bezpieczeństwa online

12 Lutego 2021

Informacje na temat projektu

REASSURE

Identyfikator umowy o grant: 731591

Strona internetowa projektu

DOI
10.3030/731591

Projekt został zamknięty

Finansowanie w ramach
INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

Koszt całkowity
€ 3 528 635,00

Wkład UE
€ 3 478 747,50

Koordynowany przez

Data podpisania przez KE
27 Listopada 2016

UNIVERSITE CATHOLIQUE DE LOUVAIN
Belgium

Data rozpoczęcia
1 Stycznia 2017

Data zakończenia
31 Marca 2020

Ostatnia aktualizacja: 7 Września 2020

Permalink: https://cordis.europa.eu/article/id/422031-new-tools-help-secure-embedded-devices/pl