Securing the Internet of Things with a unique microchip fingerprinting technology

Wyniki w skrócie

Innowacyjne metody identyfikacji chronią urządzenia IoT

Urządzenia IoT są tak słabo zabezpieczone, że stanowią zagrożenie dla całego internetu. Na szczęście powstało rozwiązanie, które umożliwia identyfikację i uwierzytelnianie milionów starszych urządzeń.

GOSPODARKA CYFROWA

BEZPIECZEŃSTWO

© Blue Planet Studio, Shutterstock

Internet rzeczy (IoT) to urządzenia sprzętowe połączone ze sobą przez internet. Przykładami są wideodomofony, ubieralne urządzenia do monitorowania stanu zdrowia, przeciwpożarowe systemy alarmowe i miejskie systemy sygnalizacji świetlnej. Według niektórych szacunków na świecie ma działać 50 miliardów takich urządzeń do 2025 roku oraz 1 bilion do 2030 roku.

Mimo zapewniania wygodnego dostępu do usług, urządzenia IoT są bardzo słabo zabezpieczone i można je łatwo zhakować. Zhakowane urządzenia mogą być z kolei wykorzystane do ataków na inne urządzenia, co zagraża reputacji przedsiębiorstw i może być źródłem różnorodnych zagrożeń dla ludzi. Problem wynika ze zbyt małej mocy obliczeniowej i pamięci urządzeń, co nie pozwala na zapewnienie zaawansowanych zabezpieczeń.

Wymiana miliardów starszych urządzeń na nowsze modele nie jest wykonalna. Na szczęście w ramach finansowanego przez UE projektu INSTET opracowano sposób na zabezpieczenie urządzeń IoT, który pozwala obyć się bez konieczności ich wymiany. Projekt udoskonalił technologię identyfikacji urządzeń opracowaną we wcześniejszym studium wykonalności Fazy 1 instrumentu dla MŚP o tej samej nazwie. Nowy projekt umożliwił potwierdzenie potencjału komercyjnego koncepcji.

Identyfikacja wszystkich urządzeń

Innowacyjna metoda najpierw przypisuje każdemu urządzeniu IoT identyfikator w oparciu o jego wyjątkowe cechy fizyczne. Fizyczne identyfikatory są generowane przy pomocy specjalnych algorytmów, które mierzą losowe różnice powstające w procesie produkcji sprzętu, za pomocą opracowanej w ramach projektu funkcji fizycznie nieklonowalnej (ang. „physical unclonable function", PUF). Metoda ta nosi nazwę biometrii krzemowej i polega na oznaczeniu każdego urządzenia IoT w sposób niemożliwy do podrobienia.

Gdy każde urządzenie ma już identyfikator, zanim możliwa będzie bezpieczna wymiana danych, musi on zostać uwierzytelniony, w przeciwnym razie nie można zagwarantować, że urządzenia komunikują się z właściwą stroną. Możliwość weryfikacji tożsamości urządzenia pozwala na zabezpieczenie prostych urządzeń IoT.

Funkcja PUF jest elementem systemu bezpieczeństwa INSTET, która wspiera cały system bezpieczeństwa dzięki silnym i niemożliwym do podrobienia usługom ochrony wysokiej jakości. „Główną zaletą tego rozwiązania", twierdzi koordynator projektu Georgios Selimis, „jest to, że nie trzeba programować klucza głównego z zewnątrz. Klucz zawsze pozostaje po stronie urządzenia, dzięki czemu jest zawsze bezpieczny".

Łatwe uaktualnianie chipów

Dodatkowo, funkcja PUF jest oparta na wszechobecnych układach pamięci statycznej (SRAM). „Dlatego też nasze podejście jest skalowalne i może objąć wszystkie urządzenia IoT", dodaje Selimis, „ponieważ pamięć SRAM jest komponentem występującym we wszystkich mikrokontrolerach, nawet najtańszych spośród nich". Dzięki temu jesteśmy w stanie uaktualnić miliony urządzeń IoT zainstalowanych w terenie bez konieczności przeprojektowywania produktów". Jest to jedyne rozwiązanie na rynku, które zapewnia silne zabezpieczenia sprzętowe, wykorzystując jedynie oprogramowanie, oraz które można łatwo wdrożyć na urządzeniach IoT o ograniczonej mocy obliczeniowej.

System został opracowany z myślą o trzech oddzielnych segmentach IoT. INSTET

Wearables zapewnia kompleksowe zabezpieczenia urządzeń ubieralnych. INSTET Medical umożliwia łączenie oprogramowania z urządzeniami medycznymi. Z kolei INSTET Critical Infrastructures wspiera łączność IoT w chmurze. Naukowcy opracowali różne architektury oprogramowania dla każdego z zastosowań. Zespół stworzył też i uruchomił prototypy dla każdego segmentu rynkowego. Powstały także szczegółowe analizy rynku i plany wykorzystania.

W dalszej kolejności konsorcjum zajmie się opracowaniem standardów i regulacji z myślą o poszczególnych rynkach. Efektem tych prac będzie wyeliminowanie poważnej luki zabezpieczeń w urządzeniach IoT.

Słowa kluczowe

INSTET, IoT, bezpieczeństwo, internet rzeczy, identyfikacja urządzeń, fizyczna funkcja nieklonowalna, biometria krzemowa

Znajdź inne artykuły w tej samej dziedzinie zastosowania

Długotrwała cyfrowa ochrona danych naukowych

Inspirowane naturą urządzenie zmniejsza zużycie energii

Lepsza lokalizacja obiektów w środowiskach przemysłowych dzięki sztucznej inteligencji

Jakość tłumaczeń maszynowych lepsza niż kiedykolwiek wcześniej

Informacje na temat projektu

INSTET

Identyfikator umowy o grant: 811509

Strona internetowa projektu

DOI
10.3030/811509

Projekt został zamknięty

Data podpisania przez KE
30 Maja 2018

Data rozpoczęcia
1 Czerwca 2018

Data zakończenia
31 Maja 2020

Finansowanie w ramach
INDUSTRIAL LEADERSHIP - Innovation In SMEs

Koszt całkowity
€ 2 496 362,50

Wkład UE
€ 1 747 453,75

Koordynowany przez
INTRINSIC ID BV
Netherlands

Ostatnia aktualizacja: 6 Listopada 2020