Academia Tehnică Militară

Abstract

Implicații de securitate în domeniul Internet of Things

Autor: Ing. Bogdan-Cosmin Chifor

Internet of Things (IoT) este un domeniu care cuprinde dispozitive embedded conectate la rețea și folosite în multiple aplicații precum: transporturi, telecomunicații, medicină, domeniul industrial și multe altele. Conceptul IoT a început ca și un subiect abordat de către presa tehnică și de către cercetările academice, însă în ultimii ani a devenit o realitate, acest domeniu fiind susținut atât de către companiile hardware cât și de către cele software. Dispozitivele IoT își au originile în rețelele wireless de senzori (WSN) și extind acest concept prin propunerea unor aplicații în care dispozitivele embedded conectate la Internet ajută în automatizarea sarcinilor utilizatorului. Astfel dispozitivele IoT sunt imaginate în multiple aplicații, de la scenarii casnice (smart home) până la scenarii industriale. Luând în considerare faptul că dispozitivele IoT impactează viața utilizatorului, există o nevoie stringentă de mecanisme de securitate care să vizeze atât securitatea, cât și siguranța.

Securitatea este considerată una dintre cele mai importante verticale IoT, fiind un factor cheie care influențează rata de acceptare și instalarea la scară largă a soluțiilor IoT. Securitatea IoT primește și mai multă atenție datorită contextului actual al securității cibernetice, în care noi vulnerabilități și atacuri apar în mod constant. Dispozitivele IoT sunt o țintă atractivă pentru atacatori, deoarece acestea operează cu date private ale utilizatorilor și pot fi folosite ca și vector de atac (de exemplu pentru atacuri de tip DoS), dacă mai multe dispozitive sunt compromise. Particularitatea contextului IoT este aceea că o breșă de securitate poate să pună în pericol și viețile omenești, pe lângă provocarea pagubelor economice. O altă particularitate a contextului IoT constă în dificultatea de proiectare a soluțiilor de securitate, datorită multiplelor limitări ale dispozitivelor, printre care: limitări computaționale și de consum, lipsa modulelor de intrare-ieșire, scenariile de instalare și multe altele. Având în vedere aceste caracteristici ale dispozitivelor IoT și adăugând multitudinea de platforme software și hardware, împreuna cu lipsa de standardizare, există o nevoie stringentă de noi soluții de securitate. O cerință importantă în studierea soluțiilor de securitate este vizarea noțiunilor de interoperabilitate și modularitate, peisajul IoT fiind unul dinamic care necesită structuri generice.

Această teză explorează mai mulți vectori de securitate IoT precum algoritmi criptografici, securitarea protocoalelor de comunicație, încredere, reputație și confidențialitate, analizând soluțiile existente și propunând noi soluții de securitate. Cercetarea din această teză tratează mai multe studii de caz și analizează aspectele soluțiilor de securitate în scenarii precum *smart home* sau *smart city*. Scopul principal al acestei teze este de a analiza și propune soluții de securitate independente de platforma hardware, soluții care vizează cerințele fiecărui nivel din stiva de aplicații IoT.