ATLAS MIST

Metodologie pentru Evaluarea Securității IoT

Numărul de dispozitive conectate la Internet este într-o continuă creștere, fiind estimat că până în 2025 aceste vor depăși 20 de miliarde. Diversitatea, precum și domeniile de utilizare ale acestor dispozitive, au depășit deja limitele aplicațiilor industriale dedicate și astfel au permis conectarea la Internet a multor activități cu caracter personal sau din zona serviciilor publice, guvernamentale și de afaceri.

Pe lângă numeroasele avantaje, utilizarea și integrarea dispozitivelor IoT conduce la creșterea riscurilor de securitate cibernetică pentru diferite domenii de activitate care nu aveau în vedere această perspectivă. Interconectarea dispozitivelor cu diferite servicii Internet în vederea prelucrării datelor colectate conduce la expunerea acestor dispozitive și implicit a datelor colectate sau a serviciilor pe care acestea le controlează.

MIST

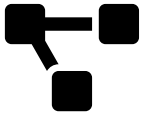
MIST este o metodologie utilizată pentru evaluarea securității mediului IoT. MIST propune o analiză și o clasificare a riscurilor, a efectelor acestora, precum și a modului în care acestea pot fi evaluate. Metodologia propune o analiză completă a domeniului IoT din mai multe puncte de vedere: al utilizatorilor finali, al mediilor folosite pentru comunicație, al datelor colectate și al serviciilor aflate în Cloud.

Caracteristicile ATLAS MIST

Riscuri de securitate

Clasificări

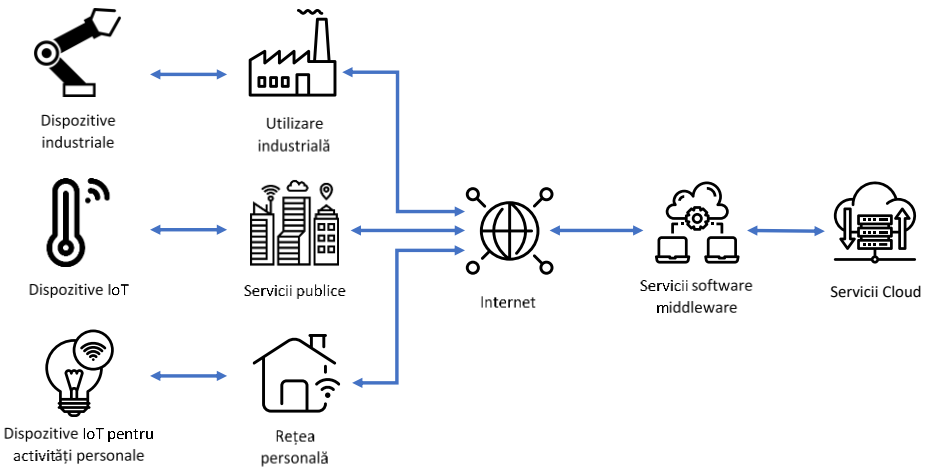
Evaluare



Strategii evaluare

Categorii utilizatori

https://mist.ase.ro



Caracteristici MIST

Metodologia pentru evaluarea securității IoT (MIST - **M**ethodology for **I**oT **S**ecuri**T**y) realizează o analiză completă a domeniului prin definirea:

- Categoriilor de dispozitive IoT și a criteriilor de clasificare
- Canalelor de comunicație utilizate și a securității acestora
- Arhitecturii generice bazate pe servicii în care sunt integrate dispozitivele IoT
- Taxonomiei riscurilor și vulnerabilităților de securitate
- Taxonomiei caracteristicilor de securitate
- Clasificării consecințelor generate de lipsa securității
- Metricilor utilizate pentru a măsura nivelul de securitate al diferitelor caracteristici

Metodologia este utilizată pentru a măsura securitatea dispozitivelor IoT utilizate în diferite scenarii și pentru a oferi rezultate comparabile și care să fie utilizate de dezvoltatori pentru a îmbunătăți aceste niveluri.
Pentru a oferi o perspectivă completă, la 360 de grade, sunt luate în considerare și fluxurile complete *end-to-end* care conectează dispozitivele IoT la serviciile software furnizate în Cloud. Astfel sunt analizate și elementele de securitate ce țin de securizarea accesului la aceste servicii. Pentru a demonstra modul în care este utilizată metodologia propusă a fost implementată o arhitectură ce permite măsurarea nivelului poluării prin intermediul unor senzori IoT amplasați în diverse locații.
Metodologia propune și o procedură de evaluare a securității dispozitivelor IoT destinată utilizatorilor casnici. Procedura ține cont de particularitățile dispozitivelor IoT personale sau utilizate în contextul unei locuințe inteligente și oferă utilizatorilor rezultate ușor de interpretat și ce pot fi utilizate pentru a compara dispozitive în funcție de nivelul de securitate oferit.

Despre ATLAS

Proiectul "Hub inovativ pentru tehnologii avansate de securitate cibernetică (ATLAS)" își propune îmbunătățirea performanțelor de cercetare și de colaborare în domeniul securității cibernetice, adresând teme de mare interes: securitatea aplicațiilor și sistemelor de operare, securitatea IoT și cloud. Proiectul ATLAS este finanțat printr-un grant acordat de Ministerul Cercetării și Inovării din România, CCCDI - UEFISCDI, proiect nr. PN-III-P1-1.2-PCCDI-2017-0272, în cadrul PNCDI III.