ATLAS MIST

Methodology for IoT Security Assessment

861/5000

The number of devices connected to the Internet is constantly growing, and it is estimated that by 2025 they will exceed 20 billion. The diversity, as well as the fields of use of these devices, have already exceeded the limits of dedicated industrial applications and thus allowed the connection to the Internet of many personal, public services, governmental and business activities.

In addition to the many benefits, the use and integration of IoT devices leads to increased cyber security risks for various areas of activity that did not have this perspective in mind. The interconnection of devices with different Internet services to process the collected data, leads to the exposure of these devices and implicitly of the collected data or of the services that they control.

MIST

MIST is a methodology used to assess the security of the IoT environment. MIST proposes an analysis and classification of risks and threats, their effects, and how they can be assessed. The methodology proposes a complete analysis of the IoT domain from several points of view: the end users, the channel used for communication, the collected data and of the services available the Cloud.

Characteristics of ATLAS MIST

Security risks

Classifications

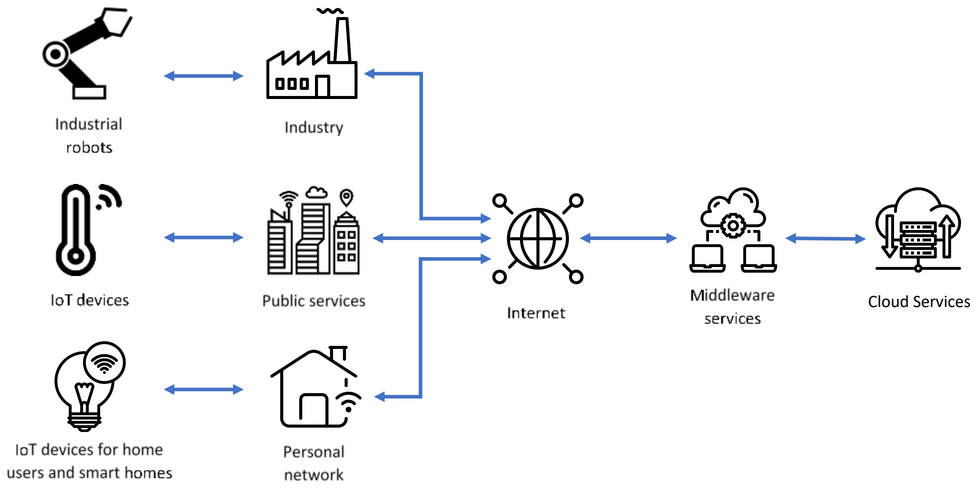
Assessment

Evaluation strategies

User categories

https://mist.ase.ro

ATLAS MIST



MIST Characteristics

The methodology for evaluating IoT security (MIST - **M**ethodology for **I**oT **S**ecuri**T**y) performs a complete analysis of the domain by defining:

- IoT device categories and classification criteria
- The communication channels used and their security
- Generic service-based architecture in which IoT devices are integrated
- Taxonomy of security risks and vulnerabilities
- Taxonomy of security features
- Classification of the consequences generated by the lack of security
- Metrics used to measure the security level of different features

The methodology is used to measure the security of IoT devices used in different scenarios and to provide comparable results that can be used by developers to improve these levels.

To provide a complete 360-degree perspective, are taken into the analysis complete end-to-end streams that connect IoT devices to software services provided in the Cloud. Thus, the security elements related to securing access to these services are also analyzed. To demonstrate how the proposed methodology is used, a proof of concept architecture has been implemented to measure the level of pollution through IoT sensors placed in various locations.

The methodology proposes a procedure for assessing the security of IoT devices used by home users. The procedure takes into account the particularities of personal IoT devices, or used in the context of a smart home, and provides users with easy-to-interpret results that can be used to compare devices according to the offered level of security.

Despre ATLAS

The ATLAS project ("Hub inovativ pentru tehnologii avansate de securitate cibernetică") plans on improving research and collaboration performances in the cyber-security domain, by addressing themes of high interest: security of applications, operating systems, IoT and cloud. The ATLAS project is financed through a research grant from the Romanian Ministry of Research and Innovation, CCCDI - UEFISCDI, project no. PN-III-P1-1.2-PCCDI-2017-0272, in the PNCDI III program.