How to implement security by design for IoT

ENISA, the European Union Agency for Cybersecurity releases ‘Good Practices for Security of IoT’, a significant report to promote security by design for IoT.

Published on November 19, 2019



Tagged with

* [cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=cybersecurity)
* [Internet of things](https://www.enisa.europa.eu/search?Subject%3Alist=Internet%20of%20things)

**The Rise of IoT and potential attacks**

The number of Internet of Things (IoT) devices is rising constantly with an expected 25 billion IoT devices to be in use by 2021 according to a Gartner study. Notorious examples of IoT attacks such as Stuxnet and Mirai have led to growing concerns about the security measures of IoT devices. IoT is going to have an impact on every aspect of our lives and we need to be prepared**.**For many years, ENISA has been working together with the wider community to promote security by design in the IoT ecosystem.

**Security by Design, fundamental to IoT Security**

The establishment of secure development guidelines is a fundamental building block for IoT security. The '[Good Practices for Security of IoT report](https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1)' has a particular focus on software development guidelines, a key aspect for achieving security by design. The study elaborates and delves into this notion by giving specifics on how to securely collect requirements, design, develop, maintain, and even dispose of IoT systems and services.

In the context of IoT, a rapidly emerging set of technologies that needs to be holistically secured, such work aims to set the reference point for the development of secure by design solutions.

The main contributions of the study include:

* Analysis of security concerns in all phases of IoT SDLC and key points to consider.
* Detailed asset and threat taxonomies concerning the IoT secure SDLC.
* Concrete and actionable good practices to enhance the cybersecurity of the IoT SDLC.
* Mapping of ENISA good practices to related existing standards, guidelines and schemes.

**Cybersecurity throughout the software development lifecycle**

To utilise secure Software Development Life Cycle (SDLC) principles is an effective and proactive means to avoid vulnerabilities in IoT and thus contribute in developing software applications and services in a secure manner.

ENISA’s Executive Director, Juhan Lepassaar, stated:

“*Taking a step back and looking into the entire lifecycle of IoT products and services, ENISA with the input of IoT experts created security guidelines for the whole lifespan: from requirements and design, to development and maintenance, as well as disposal. The motivation is clear: security is not only about the end product, but also about the processes to be followed to develop the product.”*

**Target Audience**

This ENISA study outlines good practices for IoT security with a particular focus on securing the SDLC of IoT systems. This entails defining security measures that apply to the entire IoT ecosystem (devices, communications/networks, cloud, etc.) in order to bolster the security of the development process, resulting in devices that are fundamentally more secure.

The study is complementary to the previous ENISA work on Baseline IoT Security Recommendations and aims to provide guidelines on how to secure the entire lifecycle of IoT.

Given the diverse phases that SDLC entails and the complexity of the IoT ecosystem, the target audience of this study comprises the following profiles:

* IoT software developers
* IoT platform, Software Development Kit (SDK) and Application Programming Interface (API) developers and consumers
* IoT integrators