Forest for the trees: an IoT security standards gap analysis

Published on January 17, 2019



© Copyright: Shutterstock

Tagged with

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

An ENISA analysis, which maps the existing standards against requirements on security and privacy in the area of the Internet of Things (IoT) yields that there is no significant standards gap - every requirement can be met by an existing standard. While standards exist for many different elements of making a device or service secure, when referring to IoT, one refers to an ecosystem of not only devices and services. Moreover, the context of use of IoT, its high scalability and other features further call for flexible approaches. The gap in IoT device standards for security is that the standards are not treated holistically. Therefore, it is possible to introduce to the market a device that can authenticate its user, can encrypt and decrypt data transmitted and received, can deliver or verify the proof of integrity, but which will still is and remains unsecure.  
  
The study pinpoints potential areas of improvement and additional efforts in securing the IoT area. Special attention has been paid to the EU needs related to the European cybersecurity certification framework. In the very case of security, a large number of processes as well as technical standards have to be in place, to ensure that any device placed on the market is assuredly secure. As the standards alone are essential, but not sufficient to ensure open access to markets, the study also proposes an approach towards certification, assurance and validation schemes to identify what is sufficient.   
  
This study concludes that in general there is an identifiable gap in process, by which a vendor can assert that their IoT product or service is secure. There is no significant gap, however, in standards to introduce secure IoT devices to the market.   
  
The process recommended in this report is intended in part to engender a change in attitude towards device security, by making secure IoT the only form of IoT that reaches the market; also, to give confidence to the market through a mix of certification, assurance testing and validation, as well as market surveillance.