Security design and assessment of IoT products

Name Cheng Jiang

Abstract text

Internet of Things (IoT) connects traditionally isolated physical objects together to form a harmonized system. It has the potential to revolutionize our daily life and become a fundamental part of it. But are we ready for such a revolution? When we enjoy all the convenience brought by the IoT, do we sometimes wonder the potential risks for our safety and security? For example, if I can unlock my house door through a mobile-phone application, can someone else unlock my door as well? If a pace maker can be remotely controlled by a heart doctor, can malicious attackers obtain such control?

With the IoT technology becoming increasingly powerful, security is becoming one of the main concerns. In a complex system consisting of both hardware and software, such as an IoT product, overall security is determined by the weakest part. On the other hand, ensuring security to every consisting component in a system is expensive and inefficient. Therefore, it is crucial for the IoT industry to set up security assurance processes to build secure products and to agree on methodologies to assess their security strengths without compromising cost and performance.

In many other industries, e.g. Smart Cards used in the financial industry, a well-defined methodology for achieving security assurance has been established and applied. This proposal is intended to introduce the essence of the method in the context of IoT.
The process of producing and gaining security assurance starts at the very beginning of a product lifecycle and not an afterthought. A product should have a well-defined security requirement specification since inception. Then, a security architecture can be planned and more detailed functions can be specified and designed. At last, the achieved security needs to be proven and demonstrated by structured and effective validation testing. Within each production step, security weaknesses should be identified and eliminated by vulnerability assessments, before the product is deployed. All the steps together with a well-controlled lifecycle process ensure delivery of trustworthy products to the market.