M-Sec Cookbook – a practical guide for IoT developers

M-Sec released a Cookbook that acts as a practical guide for IoT developers, to help them develop reliable and secure applications for the smart city context

In modern smart city applications, there is an emerging need of end-to-end security since many data sources may contain sensitive information that raises issue on privacy and data protection. The security and privacy issues should be addressed in all layers to ensure “end-to-end security and privacy”. For instance, many smart city applications are utilizing data streams such as images from cameras or mobile applications, and these streams should be protected from attackers in all layers by, for example, hijack protection mechanism in the sensors’ devices, secure IoT gateway connecting the devices and cloud, data encryption and access control in the cloud, and secure applications utilizing the data stream.

It is in this context that the M-Sec solution is being developed, with the main goal of developing a technology capable of ensuring safety and privacy of the data exchanged in highly connected smart cities, through the development of several protection layers: at the device level and applications used, during the exchange of information that is held between the several devices and applications, in storing that information in the Cloud, and at the development and creation of other smart devices and applications, that follow the same data safety and privacy criteria.

M-Sec’s Cookbook – a practical guide for IoT developers

The main focus of M-Sec’s Cookbook is to introduce the M-Sec IoT security framework that has been developed by the European and Japanese consortium researchers for the past two years. Therefore, it presents techniques, methods, and design and operating principles of the M-Sec solution that those researchers believe will help other IoT developers to minimize the risk of suffering critical vulnerabilities in a wide range of IoT devices. In other words, the M-Sec Cookbook is a practical guide for all IoT developers to develop reliable and secure applications for the smart city context.

This document complements and leverages another report already released by M-Sec – its White Paper.

While the White Paper introduces the overall M-Sec architecture and shows how it can be a viable solution for overcoming the main IoT security issues faced nowadays, the Cookbook provides an introduction to the M-Sec components from five different aspects – IoT security, cloud and data level security, P2P level security and blockchain, application-level security, and overall end-to-end security – with their definition and ulterior implementation, thus serving as a practical guide for any IoT developer who wishes to implement the M-Sec solution in order to address the security concerns and risks identified in the M-Sec White Paper.

Want to know more about how to implement the M-Sec solution?

Download the Cookbook

Get involved!

Visit www.msecproject.eu • Join our community on Twitter & LinkedIn • Send us a message to hello@msecproject.eu • Check out our Resources and News sections

The M-Sec project is jointly funded by the European Union’s Horizon 2020 research and innovation programme (contract No 814917) and by the Commissioned Research of National Institute of Information and Communications Technology (NICT), JAPAN (contract No 19501).