instituto de telecomunicações

IT-Covilhã

System and Attack Modelling for the Internet of Things

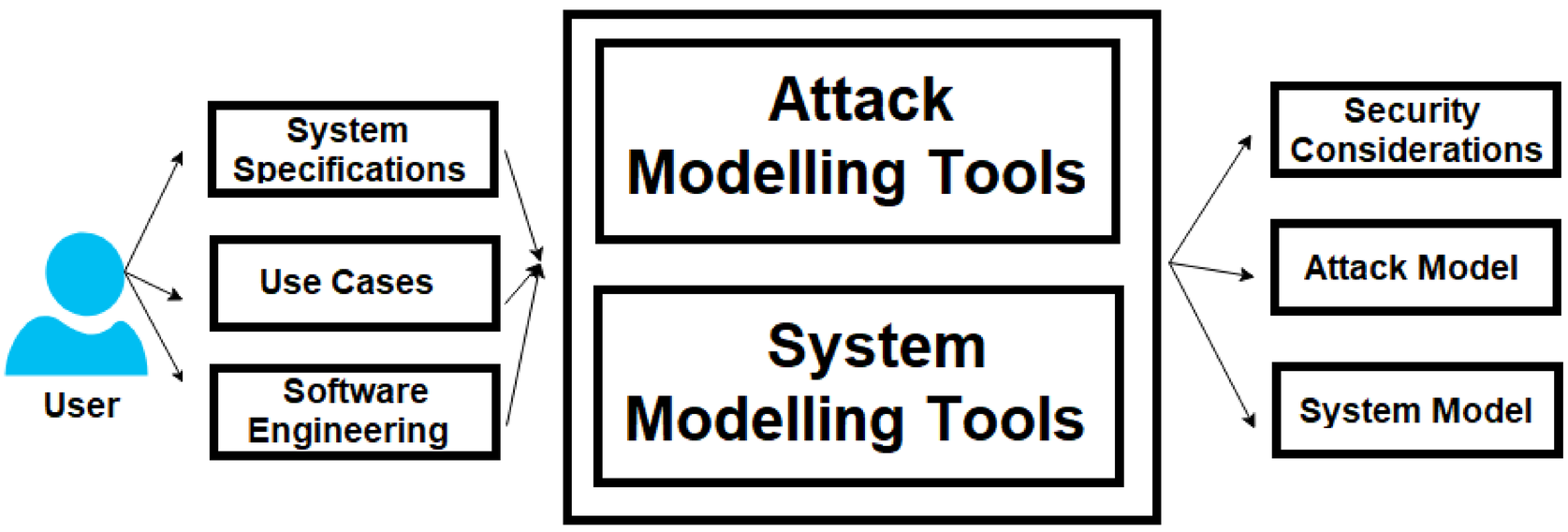
Multimedia Signal Processing

Background and challenges

- The Internet of Things (IoT) has the potential for revolutionizing businesses and industries. Connecting hundreds of thousands of devices, it allows for sensing and control on a scale never possible before. However, and though its growth has been ever increasing, security issues have arisen in a proportional scale. Short time to market and a lack of knowledge in terms of security practices has left devices vulnerable to attack, as they are designed with security as an afterthought.

Description and main innovation

- To better allow the development of IoT systems that are secure by design, we are developing a workflow for the security engineering process, through the definition and implementation of attack and system modelling tools that will allow the identification of key points, through defined use cases, where security analysis, modelling, integration and validation should be considered, and streamlining the main processes for the analysis of security requirements and attack and system modelling. The outputs will later on be used for mapping security requirements and technology.



Functional architectural scheme.

Achievements and next steps

- Currently there is an ongoing study on the state-of-the-art on attack and system modelling for the IoT ongoing.
- Being a work integrated in the project, the main communication and development elements of the project (e.g., web page, social media accounts, Research Gate, repositories) have been created and configured.

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA
SECUR IoT ESIGN
UNIVERSIDADE BEIRA INTERIOR
UID/EEA/50008/2013 and POCI-01-0145-FEDER-030657, SFRH/BD/133838/2017