IoT SPAT—Security and Privacy Analysis Toolbox for IoT Applications

D. Vizár, A. Olteanu, C. Kassapoglou Faist

Many IoT applications are comprised of low-end interconnected sensors/actuators, accessed remotely through a cloud. This creates a serious problem in terms of security and privacy, with billions of devices being simultaneously highly exposed to attacks, often inadequately secured, with sensitive user data and even personal safety at stake. A key step towards the development of an IoT application with reliable, cost-effective security is a thorough risk analysis. To this end, we design the IoT SPAT, a layman-friendly toolbox for security and privacy analysis of IoT applications.

While enabling new business models and generating value, the typical IoT application paradigm (massive numbers of inexpensive connected Things) also opens a huge opportunity for computer crime with dire consequences (vulnerable self-driving cars, connected toys prone to eavesdropping, health information leakage, traffic light sabotage etc.). At the same time, the applications that apply this IoT paradigm are very diverse in terms of security and privacy requirements, sensitivity of personal information and the quality of the hardware platforms used. Moreover, many IoT products are cost-sensitive, leaving little-to-no margin for security features. While standards, frameworks and recommendations exist concerning how to secure an IoT application (mostly ISO 27k and NIST CSF), applying them is not easy, especially for non-experts; the main obstacles being a high-entry bar in terms of security/privacy expertise, non-specificity to IoT, and/or the amount of effort required. Some frameworks dedicated to IoT applications exist, notably the IoT Security Foundation's (IoT SF) Compliance Framework, which deals with the heterogeneity of security objectives in the IoT through the concept of security classes. While very useful, this framework does not provide any concrete recommendations on how to select the appropriate security class, thus falling short of overcoming all the challenges.

IoT SPAT. CSEM has developed the *IoT SPAT,* a toolbox for security and privacy analysis dedicated to the IoT, intended to guide even non-expert analysts through the *complete* process of (1) assessing the risks related to the cyber-security threats to an IoT application and (2) using the results to make an informed selection about the required security and privacy controls for the application. The toolbox consists of (1) a security and privacy analysis method, (2) tools that automatize the most labor-intensive parts of the analysis, (3) a default template with useful assessment data easily adaptable to a variety of IoT applications.

The method (see Figure 1) couples a risk assessment following NIST SP 800 30 [1], together with the IoT SF Compliance Framework [2], for selection of security and privacy controls. NIST SP 800 30 constitutes a formal backbone of the assessment, providing a well-defined system for risk quantification. For resource effectiveness and layman-friendliness, its use is kept minimalistic with very high-level threat events (such as "damage due to attack on the Thing"). The methodology of "attack trees" is then used to refine the analysis of each threat event, enhancing the resolution and extending the coverage of various attack vectors in an agile, user-friendly way. An attack tree models a high-level threat event as the root of a directed oriented graph, where nodes describe vulnerabilities, attacker actions and other events, such that all nodes on a path from a leaf to the root constitute an attack, and must be executed/materialize in that order for the attack to succeed. The results of the risk assessment are finally translated into an input to the IoT SF compliance checklist, which generates a list of security and privacy requirements to be implemented.

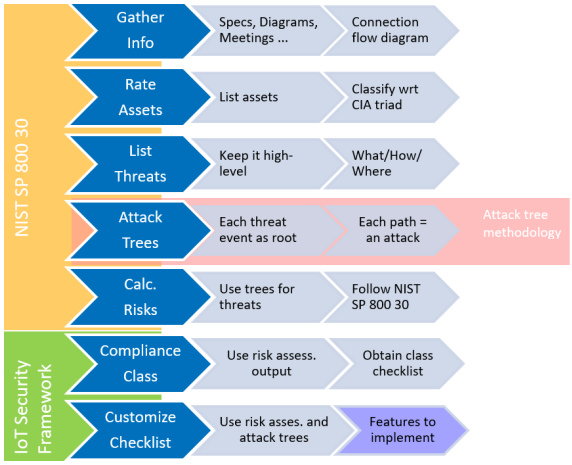

Figure 1: Iot SPAT security and privacy analysis method.

The tools accompanying the method are (1) an MS Visio stencil for efficient and visual system modelling, (2) a Python/Graphviz-based tool for creating attack trees, (3) an MS Word template for risk assessment report with embedded instructions, step-by-step and (4) an MS Excel template for risk quantification tables with macros automating most of the work. The attack tree tool turns an attack tree source file into a visual representation of the tree, using a custom syntax, which allows the likelihood of each node to be estimated individually. When the representation is compiled, the tool automatically evaluates the overall success likelihood of the top-level threat event using the individual likelihoods.

The templates. To maximize usability by the intended, broad audience, a set of default templates is provided to speed up the analysis process, as well as, to assist potential non-expert users in obtaining meaningful results. The following templates are provided: (1) a sample list of threat sources (aka attackers), (2) a sample list of high-level threat events per (generic) IoT system component, (3) an attack tree per default threat event.

Conclusion. The assessment method has been successfully applied to a personal fitness application modelled after Riva Digital, and the in the EU project OffshoreMuster. The experience gained from these two use cases shows that the analysis process with the IoT SPAT is indeed efficient, generates meaningful results and helps gain insight on the overall threat landscape, as well as the weak points, of a given application. The next steps identified are enhancing the template with more real-world data, and integrating the tools under a single UI (e.g. web based).

[1] G. Stoneburner, A. Y. Goguen, A. Feringa, "Sp 800-30. risk management guide for information technology systems" (2002).

[2] A. Abhay Soorya, "IoT Security Compliance Framework" (2019).