Application of the OWASP SAMM maturity model to improve IoT security

Pieter Meulenhoff / Eurofins Cyber Security / p.meulenhoff@eurofins-cybersecurity.com

The Software Assurance Maturity Model (SAMM) developed by the OWASP community aims to provide an effective and measurable way for all types of organisations to analyse and improve their software security posture[i]. The model covers the entire development cycle and is technology and process agnostic. The model is organised in five distinct business functions: Governance, Design, Implementation, Verification and Operations that each define practices and activities. The execution of an assessment with the model can be executed with relative ease through a combination of interviews and verification of documentation. An assessment also results in guidance to improve the software development process, which make it, in combination with the required effort to execute an assessment interesting for software developers to adopt and grow into a more secure development process.

In this presentation, we present our results in application of this model to improve IoT security, specifically consumer devices. This with the goal to verify whether the OWASP SAMM model is helpful in providing guidance and useful requirements that help to improve the software development process behind consumer IoT products.

The approach that we used is to assess the requirements in the OWASP SAMM model and their impact on resolving the most significant security problems in IoT devices. This list originates from an extensive (58 sources) literature search[ii] for security problems IoT devices that was performed for the Dutch Telecommunication Authority (Agentschap Telecom). We also make use of the results of a hands-on security assessment of a wide range consumer IoT devices, which was conducted in cooperation with the Dutch Consumer Association (De Consumentenbond). The list of most significant IoT security problems is: *Incorrect Access Control, Overly large attack surface, Outdated software, Lack of encryption, Application vulnerabilities, Lack of trusted execution environment, Vendor security posture, Insufficient privacy protection, Intrusion ignorance, Insufficient physical security, Incorrect user interaction*.

A direct assessment of the impact of the OWASP SAMM model on resolving these security problems is difficult. This is primarily caused by the fact that the OWASP SAMM model is intended to be general applicable and technology agnostic. Nevertheless, we see that all business functions and underlying practices have a positive impact on prevention and improving security. From that perspective, we conclude that the OWASP SAMM model does completely cover our list of security problems and could serve use in software developed for IoT devices.

The *Operations* business function with practices such as incident management and operational management, define activities that have a direct impact on *Intrusion ignorance* and *Vendor security posture*.

Other business functions in the OWASP SAMM model lack a direct relation but have an impact on several security problems. The business functions *Design*, *Implementation* and *Verification* each define activities that have a positive impact on the majority of security problems.

Based on our assessment, we can conclude that the OWASP SAMM model appears to be useful for improving the security of software in consumer electronics devices. The model also includes levels, which make tiered approach possible. A tiered approach could also be achieved by initially focusing on more practical business functions, and adopting the general business functions (such as Governance) at a higher level.

[i] OWASP SAMM website https://owaspsamm.org

[ii] https://www.agentschaptelecom.nl/documenten/rapporten/2020/08/26/onderzoeksrapport-essential-requirements-for-securing-iot-consumer-devices