World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:16, No:11, 2022

Threat Modeling Methodology for Supporting Industrial Control Systems Device Manufacturers and System Integrators

Authors : Raluca Ana Maria Viziteu, Anna Prudnikova

Abstract : Industrial control systems (ICS) have received much attention in recent years due to the convergence of information technology (IT) and operational technology (OT) that has increased the interdependence of safety and security issues to be considered. These issues require ICS-tailored solutions. That led to the need to creation of a methodology for supporting ICS device manufacturers and system integrators in carrying out threat modeling of embedded ICS devices in a way that guarantees the quality of the identified threats and minimizes subjectivity in the threat identification process. To research, the possibility of creating such a methodology, a set of existing standards, regulations, papers, and publications related to threat modeling in the ICS sector and other sectors was reviewed to identify various existing methodologies and methods used in threat modeling. Furthermore, the most popular ones were tested in an exploratory phase on a specific PLC device. The outcome of this exploratory phase has been used as a basis for defining specific characteristics of ICS embedded devices and their deployment scenarios, identifying the factors that introduce subjectivity in the threat modeling process of such devices, and defining metrics for evaluating the minimum quality requirements of identified threats associated to the deployment of the devices in existing infrastructures. Furthermore, the threat modeling methodology was created based on the previous steps' results. The usability of the methodology was evaluated through a set of standardized threat modeling requirements and a standardized comparison method for threat modeling methodologies. The outcomes of these verification methods confirm that the methodology is effective. The full paper includes the outcome of research on different threat modeling methodologies that can be used in OT, their comparison, and the results of implementing each of them in practice on a PLC device. This research is further used to build a threat modeling methodology tailored to OT environments; a detailed description is included. Moreover, the paper includes results of the evaluation of created methodology based on a set of parameters specifically created to rate threat modeling methodologies.

Keywords : device manufacturers, embedded devices, industrial control systems, threat modeling
Conference Title : ICICSOT 2022 : International Conference on Industrial Control Systems and Operational Technology
Conference Location : Venice, Italy
Conference Dates : November 10-11, 2022