World Academy of Science, Engineering and Technology
International Journal of Electrical and Computer Engineering
Vol:16, No:02, 2022

On the Use of Machine Learning for Tamper Detection

Authors : Basel Halak, Christian Hall, Syed Abdul Father, Nelson Chow Wai Kit, Ruwaydah Widaad Raymode

Abstract : The attack surface on computing devices is becoming very sophisticated, driven by the sheer increase of interconnected devices, reaching 50B in 2025, which makes it easier for adversaries to have direct access and perform well-known physical attacks. The impact of increased security vulnerability of electronic systems is exacerbated for devices that are part of the critical infrastructure or those used in military applications, where the likelihood of being targeted is very high. This continuously evolving landscape of security threats calls for a new generation of defense methods that are equally effective and adaptive. This paper proposes an intelligent defense mechanism to protect from physical tampering, it consists of a tamper detection system enhanced with machine learning capabilities, which allows it to recognize normal operating conditions, classify known physical attacks and identify new types of malicious behaviors. A prototype of the proposed system has been implemented, and its functionality has been successfully verified for two types of normal operating conditions and further four forms of physical attacks. In addition, a systematic threat modeling analysis and security validation was carried out, which indicated the proposed solution provides better protection against including information leakage, loss of data, and disruption of operation.

Keywords : anti-tamper, hardware, machine learning, physical security, embedded devices, ioT
Conference Title : ICHSTCD 2022 : International Conference on Hardware Security and Trusted Circuit Design
Conference Location : Dubai, United Arab Emirates
Conference Dates : February 15-16, 2022

Open Science Index, Electrical and Computer Engineering Vol:16, No:02, 2022 publications.waset.org/abstracts/143935/pdf