World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:09, 2015

Requirement Engineering for Intrusion Detection Systems in Wireless Sensor Networks

Authors : Afnan Al-Romi, Iman Al-Momani

Abstract : The urge of applying the Software Engineering (SE) processes is both of vital importance and a key feature in critical, complex large-scale systems, for example, safety systems, security service systems, and network systems. Inevitably, associated with this are risks, such as system vulnerabilities and security threats. The probability of those risks increases in unsecured environments, such as wireless networks in general and in Wireless Sensor Networks (WSNs) in particular. WSN is a self-organizing network of sensor nodes connected by wireless links. WSNs consist of hundreds to thousands of low-power, low-cost, multi-function sensor nodes that are small in size and communicate over short-ranges. The distribution of sensor nodes in an open environment that could be unattended in addition to the resource constraints in terms of processing, storage and power, make such networks in stringent limitations such as lifetime (i.e. period of operation) and security. The importance of WSN applications that could be found in many militaries and civilian aspects has drawn the attention of many researchers to consider its security. To address this important issue and overcome one of the main challenges of WSNs, security solution systems have been developed by researchers. Those solutions are software-based network Intrusion Detection Systems (IDSs). However, it has been witnessed, that those developed IDSs are neither secure enough nor accurate to detect all malicious behaviours of attacks. Thus, the problem is the lack of coverage of all malicious behaviours in proposed IDSs, leading to unpleasant results, such as delays in the detection process, low detection accuracy, or even worse, leading to detection failure, as illustrated in the previous studies. Also, another problem is energy consumption in WSNs caused by IDS. So, in other words, not all requirements are implemented then traced. Moreover, neither all requirements are identified nor satisfied, as for some requirements have been compromised. The drawbacks in the current IDS are due to not following structured software development processes by researches and developers when developing IDS. Consequently, they resulted in inadequate requirement management, process, validation, and verification of requirements quality. Unfortunately, WSN and SE research communities have been mostly impermeable to each other. Integrating SE and WSNs is a real subject that will be expanded as technology evolves and spreads in industrial applications. Therefore, this paper will study the importance of Requirement Engineering when developing IDSs. Also, it will study a set of existed IDSs and illustrate the absence of Requirement Engineering and its effect. Then conclusions are drawn in regard of applying requirement engineering to systems to deliver the required functionalities, with respect to operational constraints, within an acceptable level of performance, accuracy and reliability.

Keywords : software engineering, requirement engineering, Intrusion Detection System, IDS, Wireless Sensor Networks, WSN
Conference Title : ICRE 2015 : International Conference on Requirements Engineering
Conference Location : London, United Kingdom
Conference Dates : September 25-26, 2015