World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:17, No:12, 2023

Moving Target Defense against Various Attack Models in Time Sensitive Networks

Authors : Johannes Günther

Abstract : Time Sensitive Networking (TSN), standardized in the IEEE 802.1 standard, has been lent increasing attention in the context of mission critical systems. Such mission critical systems, e.g., in the automotive domain, aviation, industrial, and smart factory domain, are responsible for coordinating complex functionalities in real time. In many of these contexts, a reliable data exchange fulfilling hard time constraints and quality of service (QoS) conditions is of critical importance. TSN standards are able to provide guarantees for deterministic communication behaviour, which is in contrast to common best-effort approaches. Therefore, the superior QoS guarantees of TSN may aid in the development of new technologies, which rely on low latencies and specific bandwidth demands being fulfilled. TSN extends existing Ethernet protocols with numerous standards, providing means for synchronization, management, and overall real-time focussed capabilities. These additional QoS guarantees, as well as management mechanisms, lead to an increased attack surface for potential malicious attackers. As TSN guarantees certain deadlines for priority traffic, an attacker may degrade the QoS by delaying a packet beyond its deadline or even execute a denial of service (DoS) attack if the delays lead to packets being dropped. However, thus far, security concerns have not played a major role in the design of such standards. Thus, while TSN does provide valuable additional characteristics to existing common Ethernet protocols, it leads to new attack vectors on networks and allows for a range of potential attacks. One answer to these security risks is to deploy defense mechanisms according to a moving target defense (MTD) strategy. The core idea relies on the reduction of the attackers' knowledge about the network. Typically, mission-critical systems suffer from an asymmetric disadvantage. DoS or QoS-degradation attacks may be preceded by long periods of reconnaissance, during which the attacker may learn about the network topology, its characteristics, traffic patterns, priorities, bandwidth demands, periodic characteristics on links and switches, and so on. Here, we implemented and tested several MTD-like defense strategies against different attacker models of varying capabilities and budgets, as well as collaborative attacks of multiple attackers within a network, all within the context of TSN networks. We modelled the networks and tested our defense strategies on an OMNET++ testbench, with networks of different sizes and topologies, ranging from a couple dozen hosts and switches to significantly larger set-ups.

Keywords : network security, time sensitive networking, moving target defense, cyber security
Conference Title : ICICTI 2023 : International Conference on Industrial Cybersecurity and Threat Intelligence
Conference Location : Tokyo, Japan
Conference Dates : December 04-05, 2023