ES-SECS/GEM: An Efficient Security Mechanism for SECS/GEM Communications

ABSTRACT

Industry 4.0, as a driving force, is making massive achievements, notably in the manufacturing sector, where all key components engaged in the production processes are being digitally interconnected. However, when combined with enhanced automation and robotics, machine learning, artificial intelligence, big data, cloud computing, and the Internet of Things (IoT), this open network interconnectivity renders industrial systems more vulnerable to cyberattacks. Cyberattacks may have a variety of different impacts and goals, but they always have negative repercussions for manufacturers. These repercussions include financial losses, disruption of supply chains, loss of reputation and competitiveness, and theft of corporate secrets. Semiconductor Equipment Communication Standard/Generic Equipment Model (SECS/GEM) is a legacy Machine-to-Machine (M2M) communication protocol used profoundly in the semiconductor and other manufacturing industries. SECS/GEM is mainly designed to be utilized in a trusted, controlled, and regulated factory environment separated from external networks. Industry 4.0 has revolutionized the manufacturing industry and has brought SECS/GEM back to the limelight, as SECS/GEM is completely devoid of security features. This research proposes ES-SECS/GEM, an Efficient Security mechanism that provides authentication, integrity, and protection against cyberattacks. The proposed mechanism is compared to other security mechanisms in terms of processing time, control overhead, and resilience against cyberattacks. The ES-SECS/GEM demonstrated promising results, suggesting that it allowed SECS/GEM devices to only connect with authorized industrial equipment, maintained message integrity, discarded forged messages, and prevented cyberattacks on SECS/GEM communications. In terms of processing time and control, ES-SECS/GEM likewise outperformed other mechanisms and incurred the lowest values for these metrics.