Capitol Graduate Research Summit

Intrusion Detection for 3D-Printers: An Electrical Power Analysis Approach

Michael Rott and Sergio Salinas Monroy

Department of Electrical Engineering and Computer Science, Wichita State University

Manufacturing is one of the largest economic development drivers in the state of Kansas, accounting for more than $25 billion of annual economic output. In recent years, Kansas manufacturers have adopted Industry 4.0 technologies to improve their efficiency and productivity. Unfortunately, by making machine data available over computer networks, these technologies increase the risk of cyberattacks that inject defects into the manufactured objects, and thus can result in financial losses, loss of reputation, and, in safety critical applications such as aerospace, injury and loss of human lives. In this work, we focus on cyberattacks against additive manufacturing, also called 3D-printing. We propose a novel intrusion detection approach that can detect defect injection attacks and it is based on analyzing the 3D-printer's power consumption. Existing intrusion detection techniques are designed for IT systems and ignore attacks that compromise the electronic and physical components of 3D-printers. In contrast, our approach uses the 3D-printers' power consumption to detect malicious intruders that inject defects into the produced object. To analyze the 3D-printer's power consumption, we use a deep learning approach called a multi-layer neural network (NN). The main idea of the NN is to analyze previous power consumption measurements to predict future measurements. If the observed measurement differs from the predicted by more than a specified threshold, then it is likely that an intruder is maliciously manipulating the 3D-printer. Our results show that we can classify 3D prints as benign or malicious with an accuracy of 91.25%, allowing accurate detection of several tested defects.