Real-Time Attack Detection in Cyber-Physical Systems

Industrial Control Systems (ICS) are examples of Cyber-Physical Systems (CPS) that have human, cyber, and physical components which interact with each other in subtle ways. Malicious adversaries can attack such systems by compromising the physical components and exploiting the vulnerabilities inherent in the systems and cause grave damage. The complexity of such systems makes attack prevention and detection non-trivial. In this work, we plan to make an attempt to detect events leading to an attack in a timely manner so as to subvert the attack. We begin by representing attacks in the form of a CPS attack graph that captures three types of events, namely, physical events, human-generated events, and cyber-events, and the dependencies of such events leading up to an attack. The various events that occur in the system are captured in various logs and correlated in real-time and checked against the CPS graph to verify whether the events are of interest to the attacks being detected. The events in the CPS attack graph and those collected through logs may be at different levels of abstractions. The major research challenge is how these two classes of events can be correlated in real-time so as to foresee the occurrence of an attack and help thwart it in a timely manner.