Discovering causal relationships between events in device logs

Abstract

Industrial control systems (ICSs) are increasingly the target of multi-phase, sophisticated cyber-attacks called Advanced Persistent Threats (APTs) which act out their behaviour over an extended period. The attack's true purpose is often obfuscated making mounting a defence difficult. The low-level components which make up an ICS are interlinked and analysing the logs of one device may reveal events triggered in another. ICS APT attacks use multiple steps to reach their target devices. Causal analysis of anomalies can help to detect these attacks in early phases before the final stage of the attacks can be executed against ICS endpoints, and it prevents attackers from achieving their final goals. In this paper, we propose using a causal relationship algorithm to detect causality between individual intrinsic mode functions (IMF) within ICS device logs. If the IMF which contains the data of the attack is removed, then the causal response from that attack will also be removed. Developing causal relationship graphs for events prior to, during, and after an attack gives insight into what causal interactions are linked to the attack, and what action the attack is likely to take next. We analyse the effectiveness of the causal algorithm against two datasets which simulate attacks on different ICSs. We test the causal algorithm under different attack types, input parameters and noise level of the device logs. The results show that the causal algorithm can correctly identify the causal relationship of the attack when the data is non-linear and non-stationary. The results also show that the number of false positives is dependent on the threshold value for the causal relationship score. Insight gained by the causal relationship graph is highly dependent on the structure of the data of the ICS device logs. For ICSs which record events as non-linear and non-stationary, the causal algorithm can be used to develop system wide causal relationship diagrams which provide visibility of the network and can be used as a potential assistant in mounting a defence against an APT.

Joshua Hagemann