World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:04, 2022

Two-Level Graph Causality to Detect and Predict Random Cyber-Attacks

Authors : Van Trieu, Shouhuai Xu, Yusheng Feng

Abstract : Tracking attack trajectories can be difficult, with limited information about the nature of the attack. Even more difficult as attack information is collected by Intrusion Detection Systems (IDSs) due to the current IDSs having some limitations in identifying malicious and anomalous traffic. Moreover, IDSs only point out the suspicious events but do not show how the events relate to each other or which event possibly cause the other event to happen. Because of this, it is important to investigate new methods capable of performing the tracking of attack trajectories task quickly with less attack information and dependency on IDSs, in order to prioritize actions during incident responses. This paper proposes a two-level graph causality framework for tracking attack trajectories in internet networks by leveraging observable malicious behaviors to detect what is the most probable attack events that can cause another event to occur in the system. Technically, given the time series of malicious events, the framework extracts events with useful features, such as attack time and port number, to apply to the conditional independent tests to detect the relationship between attack events. Using the academic datasets collected by IDSs, experimental results show that the framework can quickly detect the causal pairs that offer meaningful insights into the nature of the internet network, given only reasonable restrictions on network size and structure. Without the framework's guidance, these insights would not be able to discover by the existing tools, such as IDSs. It would cost expert human analysts a significant time if possible. The computational results from the proposed two-level graph network model reveal the obvious pattern and trends. In fact, more than 85% of causal pairs have the average time difference between the causal and effect events in both computed and observed data within 5 minutes. This result can be used as a preventive measure against future attacks. Although the forecast may be short, from 0.24 seconds to 5 minutes, it is long enough to be used to design a prevention protocol to block those attacks.

Keywords : causality, multilevel graph, cyber-attacks, prediction
Conference Title : ICCSS 2022 : International Conference on Cyber Security Strategies
Conference Location : Boston, United States
Conference Dates : April 21-22, 2022