A Reasoning Method of Cyber-Attack Attribution Based on Threat Intelligence

Authors : Li Qiang, Yang Ze-Ming, Liu Bao-Xu, Jiang Zheng-Wei

Abstract : With the increasing complexity of cyberspace security, the cyber-attack attribution has become an important challenge of the security protection systems. The difficult points of cyber-attack attribution were forced on the problems of huge data handling and key data missing. According to this situation, this paper presented a reasoning method of cyber-attack attribution based on threat intelligence. The method utilizes the intrusion kill chain model and Bayesian network to build attack chain and evidence chain of cyber-attack on threat intelligence platform through data calculation, analysis and reasoning. Then, we used a number of cyber-attack events which we have observed and analyzed to test the reasoning method and demo system, the result of testing indicates that the reasoning method can provide certain help in cyber-attack attribution.

Keywords : reasoning, Bayesian networks, cyber-attack attribution, Kill Chain, threat intelligence
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020

Open Science Index, Mathematical and Computational Sciences Vol:14, No:12, 2020 publications.waset.org/abstracts/50175.pdf