World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:06, 2021

Understanding Cyber Kill Chains: Optimal Allocation of Monitoring Resources Using Cooperative Game Theory

Authors : Roy. H. A. Lindelauf

Abstract : Cyberattacks are complex processes consisting of multiple interwoven tasks conducted by a set of agents. Interdictions and defenses against such attacks often rely on cyber kill chain (CKC) models. A CKC is a framework that tries to capture the actions taken by a cyber attacker. There exists a growing body of literature on CKCs. Most of this work either a) describes the CKC with respect to one or more specific cyberattacks or b) discusses the tools and technologies used by the attacker at each stage of the CKC. Defenders, facing scarce resources, have to decide where to allocate their resources given the CKC and partial knowledge on the tools and techniques attackers use. In this presentation CKCs are analyzed through the lens of covert projects, i.e., interrelated tasks that have to be conducted by agents (human and/or computer) with the aim of going undetected. Various aspects of covert project models have been studied abundantly in the operations research and game theory domain, think of resource-limited interdiction actions that maximally delay completion times of a weapons project for instance. This presentation has investigated both cooperative and non-cooperative game theoretic covert project models and elucidated their relation to CKC modelling. To view a CKC as a covert project each step in the CKC is broken down into tasks and there are players of which each one is capable of executing a subset of the tasks. Additionally, task inter-dependencies are represented by a schedule. Using multi-glove cooperative games it is shown how a defender can optimize the allocation of his scarce resources (what, where and how to monitor) against an attacker scheduling a CKC. This study presents and compares several cooperative game theoretic solution concepts as metrics for assigning resources to the monitoring of agents.

Keywords : cyber defense, cyber kill chain, game theory, information warfare techniques
Conference Title : ICCWS 2021 : International Conference on Cyber Warfare and Security
Conference Location : Paris, France
Conference Dates : June 24-25, 2021

Open Science Index, Computer and Information Engineering Vol:15, No:06, 2021 publications.waset.org/abstracts/137878.pdf