World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:01, 2017

Modeling of Timing in a Cyber Conflict to Inform Critical Infrastructure Defense

Authors : Brian Connett, Bryan O'Halloran

Abstract : Systems assets within critical infrastructures were seemingly safe from the exploitation or attack by nefarious cyberspace actors. Now, critical infrastructure is a target and the resources to exploit the cyber physical systems exist. These resources are characterized in terms of patience, stealth, replication-ability and extraordinary robustness. System owners are obligated to maintain a high level of protection measures. The difficulty lies in knowing when to fortify a critical infrastructure against an impending attack. Models currently exist that demonstrate the value of knowing the attacker's capabilities in the cyber realm and the strength of the target. The shortcomings of these models are that they are not designed to respond to the inherent fast timing of an attack, an impetus that can be derived based on open-source reporting, common knowledge of exploits of and the physical architecture of the infrastructure. A useful model will inform systems owners how to align infrastructure architecture in a manner that is responsive to the capability, willingness and timing of the attacker. This research group has used an existing theoretical model for estimating parameters, and through analysis, to develop a decision tool for would-be target owners. The continuation of the research develops further this model by estimating the variable parameters. Understanding these parameter estimations will uniquely position the decision maker to posture having revealed the vulnerabilities of an attacker's, persistence and stealth. This research explores different approaches to improve on current attacker-defender models that focus on cyber threats. An existing foundational model takes the point of view of an attacker who must decide what cyber resource to use and when to use it to exploit a system vulnerability. It is valuable for estimating parameters for the model, and through analysis, develop a decision tool for would-be target owners.

Keywords : critical infrastructure, cyber physical systems, modeling, exploitation
Conference Title : ICCPS 2017 : International Conference on Cyber-Physical Systems
Conference Location : Zurich, Switzerland
Conference Dates : January 13-14, 2017