World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:17, No:07, 2023

An Immune-Inspired Web Defense Architecture

Authors : Islam Khalil, Amr El-Kadi

Abstract : With the increased use of web technologies, microservices, and Application Programming Interface (API) for integration between systems, and with the development of containerization of services on the operating system level as a method of isolating system execution and for easing the deployment and scaling of systems, there is a growing need as well as opportunities for providing platforms that improve the security of such services. In our work, we propose an architecture for a containerization platform that utilizes various concepts derived from the human immune system. The goal of the proposed containerization platform is to introduce the concept of slowing down or throttling suspected malicious digital pathogens (intrusions) to reduce their damage footprint while providing more opportunities for forensic inspection of suspected pathogens in addition to the ability to snapshot, rollback, and recover from possible damage. The proposed platform also leverages existing intrusion detection algorithms by integrating and orchestrating their cooperative operation for more effective intrusion detection. We show how this model reduces the damage footprint of intrusions and gives a greater time window for forensic investigation. Moreover, during our experiments, our proposed platform was able to uncover unintentional system design flaws that resulted in internal DDoS-like attacks by submodules of the system itself rather than external intrusions.

Keywords : containers, human immunity, intrusion detection, security, web services
Conference Title : ICCS 2023 : International Conference on Cyber Security
Conference Location : Zurich, Switzerland
Conference Dates : July 24-25, 2023