ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

Securing Industrial Control Networks with Cyber System Physical Security Method by Using Virtual Honeypots

Divya Ambrita R.L[1], Sujithra Jenifer.M[2], Vinu.J[3]
Department Of Information Technology, Francis Xavier Engineering College, Tirunelveli, India[1]
Department Of Information Technology, Francis Xavier Engineering College, Tirunelveli, India[2]
Assistant Professor, Department Of Information Technology, Francis Xavier Engineering College, Tirunelveli, India[3]

Abstract— This paper presents a design and implementation for self-configuring honeypots that passively examine control system network traffic and actively adapt to the observed environment. In contrast to prior work in the field, six tools were analyzed for suitability of network entity information gathering. Ettercap, an established network security tool not commonly used in this capacity, outperformed the other tools and was chosen for implementation. Utilizing Ettercap XML output, a novel four-step algorithm was developed for autonomous creation and update of a Honeyd configuration. This algorithm was tested on an existing small campus grid and sensor network by execution of a collaborative usage scenario. Automatically created virtual hosts were deployed in concert with an anomaly behavior (AB) system in an attack scenario. Virtual hosts were automatically configured with unique emulated network stack behaviors for 92% of the targeted devices in the AB system alerted on 100% of the monitored emulated devices.

Index Terms—Industrial control, intrusion detection, network security, self configuring honey pots ,deceptive systems

All Rights Reserved © 2015 IJARTET