World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:5, 2014

Intrusion Detection in SCADA Systems

Authors : Leandros A. Maglaras, Jianmin Jiang

Abstract : The protection of the national infrastructures from cyberattacks is one of the main issues for national and international security. The funded European Framework-7 (FP7) research project CockpitCI introduces intelligent intrusion detection, analysis and protection techniques for Critical Infrastructures (CI). The paradox is that CIs massively rely on the newest interconnected and vulnerable Information and Communication Technology (ICT), whilst the control equipment, legacy software/hardware, is typically old. Such a combination of factors may lead to very dangerous situations, exposing systems to a wide variety of attacks. To overcome such threats, the CockpitCI project combines machine learning techniques with ICT technologies to produce advanced intrusion detection, analysis and reaction tools to provide intelligence to field equipment. This will allow the field equipment to perform local decisions in order to self-identify and self-react to abnormal situations introduced by cyberattacks. In this paper, an intrusion detection module capable of detecting malicious network traffic in a Supervisory Control and Data Acquisition (SCADA) system is presented. Malicious data in a SCADA system disrupt its correct functioning and tamper with its normal operation. OCSVM is an intrusion detection mechanism that does not need any labeled data for training or any information about the kind of anomaly is expecting for the detection process. This feature makes it ideal for processing SCADA environment data and automates SCADA performance monitoring. The OCSVM module developed is trained by network traces off line and detects anomalies in the system real time. The module is part of an IDS (intrusion detection system) developed under CockpitCI project and communicates with the other parts of the system by the exchange of IDMEF messages that carry information about the source of the incident, the time and a classification of the alarm.

Keywords : cyber-security, SCADA systems, OCSVM, intrusion detection
Conference Title : ICAIDM 2014 : International Conference on Artificial Intelligence and Data Mining
Conference Location : London, United Kingdom
Conference Dates : May 26-27, 2014