Contribution ID: **26**   Type: **Poster**

CYBER ATTACK SIMULATION SYSTEM FOR BOILING WATER REACTOR CONTROL ROOM

Abstract

In this work, a cyber security simulation testbed for Boiling Water Reactor is proposed. It is built up in the form of Client-Server. The Server being the reactor core and the Client being the control room. The Client performs continuous check on power level values of the reactor and runs machine-learning Intrusion Detection algorithm and. The performance of the proposed algorithm is evaluated on the KDD dataset after performing dimensionality reduction using Recursive Feature Elimination; which identifies the set of the KDD features that mostly affect the detection. The algorithm is compared with others yielding accuracy of 99.41%. The testbed simulates the dynamic behavior of the nuclear reactor by running a set of differential equations on the Server. The Server continuously communicates the reactor parameters to the Client to ascertain that there is no change in parameters due to disruption in communication. If discrepancy in parameters' readings occurs, the reactor issues an alarm and displays the change graphically on screen. This initiates the operation of the machine learning algorithm to determine the type of abnormality; whether system fault or intrusion. The whole simulation is developed using LabView and Python.

State

Egypt

Gender

Female

Primary authors: Prof. KANDIL, Magy (Nuclear and Radiological Regulatory Authority, ENRRA,Cairo, Egypt); Dr SALAMA, may (Faculty of Engineering Banha university); Mr IBRAHIM, Ziad (Faculty Engineering, Banha University Cairo)

Presenter: Prof. KANDIL, Magy (Nuclear and Radiological Regulatory Authority, ENRRA,Cairo, Egypt)

Track Classification: CC: Information and computer security considerations for nuclear security