Contribution ID: **454** Type: **Paper**

Virtualization-assisted testing of network security systems for NPPs

Monday 10 February 2020 12:15 (15 minutes)

Nuclear power plants are complex systems with critical controls and measures implemented by computers and dedicated programmable logic controllers. These end devices are grouped into different security levels and zones and are connected by computer networks forming a complex trust relationship between the entities. The boundaries of the zones are separated by specialized security systems, e.g. gateways, firewalls, network diodes and other security devices. The thorough testing of these security devices before deployment is a crucial task of the IT staff. In this paper we propose a virtualization-based testing solution, where the stability, security and reliability of the tested devices can be measured in realistic scenarios.

In the first part of the paper we briefly introduce the different kinds of virtualization techniques. Virtualization is a technique which enables the operation of several virtual computers (called virtual machines) running on one or on a limited number of physical hosts. After that we present the concept of Infrastructure as Code (IaC). This concept allows us to store and deploy the configuration of any computer or network of computers as code. Using the two techniques together is an efficient way to deploy large scale computer networks on demand. We demonstrate the capabilities of the technique by designing and deploying a simplified version of a nuclear power plant's security level 4 and 5 systems.

In the second part of the paper, we briefly introduce the concept of defense in depth for the design of the network, in which the systems are separated by distributing them in different layers from lower to higher security requirements and in sub zones, in which diverse controls must be applied to ensure communication and access between systems and at the same time collect the necessary information to detect intrusions. With this information we can take another important step in the direction of defense in depth, which is the early detection of incidents and consequently early response to them, thus protecting the zones and layers of our system.

By applying a list of pre-selected controls from IEC 63096 (Nuclear power plants - Instrumentation and control-systems - Security controls) we evaluate different security solutions with open source software such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), proxies and security incident and event monitoring systems (SIEM). In order to determine the ideal set of solutions to be used on an end device or network infrastructure equipment, we use the realistic network deployed by the technique discussed in the first part of this paper. The work described in this paper is supported by the International Atomic Energy Agency (IAEA) under the collaborative research project CRP-J02008.

Gender

State

Hungary

Authors: Dr HOLCZER, Tamás (BME CrySyS); Mr BERMAN, Gustavo (CNEA); Mr DARRICADES, Sebastian Martin (CNEA); Mr GYORGY, Peter (BME CrySyS); Mr LADI, Gergo (BME CrySyS)

Presenter: Dr HOLCZER, Tamás (BME CrySyS)

Session Classification: IAEA Coordinated Research Programmes for Information and Computer Security

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