Contribution ID: **619** Type: **Paper**

Effective Fuzz Testing for Programmable Logic Controllers Vulnerability Research to Ensure Nuclear Safety

Critical infrastructure, such as nuclear power plants, widely uses various Operational Technology (OT) solutions, such as Industrial Control Systems (ICS). OT networks used to be logically and physically isolated from other business functions, but nowadays it is not always true. Along with the digitalization of such systems, they got interconnected and internetworked. Thus new cybersecurity threats were introduced.
In the case of critical infrastructure, even the smallest disruption can cause undesirable, hazardous outcome. An action, as simple as changing a value of a single variable (e.g. temperature sensors readings) can result in serious damage to the pump control or whole cooling system. The key components of such OT networks are programmable logic controllers (PLCs), which process information about the physical process in order to manipulate it. PLCs are an inseparable part of 80% of ICS designs, thus their robustness has a direct, incontestable impact on the safety of the whole control systems. Some of the publicly reported incidents involving PLCs are: Stuxnet worm attack on Iranian nuclear facilities (2010) that reprogrammed PLCs to operate incorrectly resulting in failure of many centrifuges and an incident in Browns Ferry nuclear plant in Alabama, where a faulty PLC overloaded the network with excessive traffic. Therefore PLCs have been chosen as an object for our studies.
One of the methods commonly used in the security industry to look for vulnerabilities is fuzz testing. It is considered to be one of the most popular vulnerability discovery techniques. It owes its popularity to relatively high accuracy, good scalability as well as easiness of implementation of the method. The fuzzing technique is based on creating a purposely malformed input, delivering it to the target software and checking for failures. It can be applied to communication protocol testing at various stack levels The rationale behind using this method is the belief that it offers unmatched ability to quickly test a wide range of cases.
There is a need to refine fuzz testing methodology for the purpose of security testing of PLCs used in nuclear industry. Therefore this paper aims to answer the following research question: To what extend fuzz testing can be used to find zero-day vulnerabilities in programmable logic controllers commonly used in nuclear industry?
In order to answer the posed research question, specialized laboratory, consisting of several PLCs and a fuzzing tool, was created. Additionally, an existing fuzzing methodologies were reviewed and improved for the purpose of PLC testing. Especially, taking into regards its limitations in terms of data access. Using the built testbed and methodologies, two different models of Siemens PLC were examined regarding robustness of different network protocols implementations. During conducted research several vulnerabilities were found, including a zero day vulnerability in Siemens S7-1500 PLC.
This paper presents requirements for fuzzing laboratory, fuzzing methodology focused on PLCs, and analysis of the found vulnerabilities. This research has been carried out in Nuclear Centre for Nuclear Research (Poland) as a part of IAEA Coordinated Research Project (CRP) J02008 in incident response in nuclear facilities.

Gender

State

Poland

Authors: SUCHORAB, Jakub (National Centre for Nuclear Research); Ms WALKIEWICZ, Joanna (National Centre for Nuclear Research); Ms STASZKIEWICZ, Kinga (National Centre for Nuclear Research); Mr DUDEK, Marcin (National Centre for Nuclear Research)

Co-author: Dr GAJEWSKI, Jacek (National Centre for Nuclear Research)

Presenters: SUCHORAB, Jakub (National Centre for Nuclear Research); Ms STASZKIEWICZ, Kinga (National Centre for Nuclear Research)

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