Nidhi Chovatiya
10457344
May 3, 2021

Cyber-attack taxonomy for digital environment in nuclear power plants

Review Essay - CS 573 Assignment 2

In this day and age where most of the wars are fought online in the form of cyber attacks and cyber ransoms, it has become even more important for governments, private companies and even everyday users to secure their devices from being caught up in it. Also, cyber security at nuclear power plants (NPPs) has become a hot issue. Ongoing occasions like, the Stuxnet, which obliterated Iran's uranium improvement facility. The cyber-attack cases explored utilizing the proposed cyber-attack scientific categorization can be utilized as information for assessment and approval of network safety conformance for advanced gadgets to be applied, and as powerful avoidance and moderation for cyber-attacks of NPPs. The main point of this paper is to contemplate the high-level examination on the cyber-attack scientific classification of ICS and SCADA frameworks, recommends illustration of the cyberattack scientific classification layout and the attributes of scientific categorization in NPPs. PC and organization assaults are arranged into four stages dependent on the attack class, attack target, weaknesses, and payload. The classes of scientific classification are gathered by specific ideas. By expanding instances of cyber-attack utilizing formats produced using the proposed taxonomy categorization classes, they can be utilized as information for check of the conformance of advanced I&C gadgets to be applied in NPPs. This information additionally can be utilized as proficient countermeasure techniques against cyber-attacks. This paper suggests categories of taxonomy to fulfill these purposes, which are - the attack procedure, attack vector, attack consequence, countermeasure, and vulnerability.

- Attack procedure:

  The attack strategy can be utilized as the measures for simplicity of a methodical digital assault case examination. The attack methodology comprises of four stages: gathering data, securing access right, command and control, and action and exfiltration. Information can be assembled by utilizing hacking strategies, the information or data of items and weaknesses can be spilled to the assailant. Following

stage is gaining access right, which includes getting the authority of the manager from the client by attacking into the framework just as discovering a secret phrase through a cyber-attack. In order and-control stage, orders are executed distantly. The last advance of attack system is activity and exfiltration are eliminating or adjusting the put away log records so the client can't be mindful of the encroachment by cyber-attack.

- Attack vector:

  Attack vectors are classified into physical access and network access. As the name proposes, Physical access alludes to situation where a versatile stockpiling medium, for example, a USB is utilized to move information or to refresh the framework, Importing and introducing gear from production network and the most fragile mark of ICS and SCADA framework is an assault by insider. Another is network access, which implies a method of interfacing through the computerized gear and organization of NPPs. network access can be partitioned into the utilization of an inadequate organization for refreshing and upkeep, distant access, and the utilization of remote communication.

- Attack consequences:

  In this paper author think about the attributes of NPPs and arranging the results of cyberattacks as they influence the Safety, Security and Emergency Preparedness (SSEP) capacities or not the cyber-attacks which influence SSEP works, or functions likewise partitioned into attacks that identify with illicit exchange or harm. This can be utilized as fundamental information for measuring the danger of a cyber-attack.

- Vulnerability:

  As the significance of the word is a weakness, which is in the plan and activity of a framework which can be abused by an attacker, to perform unapproved activities. In this paper, the weakness is characterized as a particular state of the OS, equipment, programming, CPU type, specialized technique, and CVE. Frameworks utilized in NPPs cannot refresh or fix the immunization progressively, in contrast to IT security. Cyber-attacks are misused through the weakness of the objective.

- Countermeasure:

  The countermeasure has been coordinated with CDAs and security control. This strategy empowers vital reactions when nuclear power plants are presented to cyber threats. To show the effectiveness of taxonomy, this paper proposes a countermeasure when a plant checking framework (PMS) is

attacked by ping of death and discloses how to utilize the taxonomy in the conformance test.

This paper recommends how to utilize cyber-attack scientific classification by applying ping of death with the proposed format. The motivation behind the proposed scientific taxonomy is to develop key countermeasures reflecting attack result and attack vectors, and to be utilized for conformance testing. Ping of death is a sort of DOS where an IP bundle bigger than the length indicated in the standard is sent, consequently causing a DOS attack by not taking care of the unusual parcel in the OS accepting this parcel. An archive-based test is a technique for confirming whether the security control introduced in security norms contrast and the security plan prerequisites of the computerized gadgets. Infiltration testing can affirm the security control of the advanced gadgets meet the suggested administrative rules. In any case, there is an issue where cyber-attacks will be utilized to direct penetration testing. This issue can be tackled through the taxonomy introduced in this paper.

As I would like to think, the work done in this paper is exceptional and the correct way to protect frameworks of nuclear power plant. To anticipate the cyber-attacks on NPPs and assess the network safety conformance, there ought to be cyberattack contextual investigations dependent on a cyber-attack scientific classification that mirrors the attributes of NPPs. Nonetheless, there is an absence of examination on the precise cyber-attack taxonomy that mirrors the attributes of NPPs. Thus, this paper proposes a cyber-attack taxonomy that mirrors the qualities of a NPP, like the assault method, assault vector, assault result, weakness, and countermeasures.

In conclusion, this paper has introduced a better than ever cyber-attack taxonomy that mirrors the qualities of NPP, like the attack technique, attack vector, attack consequence, vulnerability, and countermeasures. What is more, a taxonomy layout made out of the proposed taxonomy things is introduced to act as an illustration of cyberattack (ping of death). Additionally, the cyber-attack cases explored utilizing the proposed cyber-attack taxonomy in this paper can be utilized as information for assessment and approval of network protection conformance for computerized gadgets to be applied, and as compelling counteraction and moderation for cyber-attacks of NPPs.

Source:

https://www.sciencedirect.com/science/article/pii/S1738573319305443

Received: 29 June 2019
Received in revised form: 17 September 2019.
Accepted: 1 November 2019
Available online: 4 November 2019