INL/EXT-17-44207-Revision-0

Nuclear Power Plant Simulation and Cybersecurity

Brandon Rice

January 2018

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-17-44207-Revision-0

Nuclear Power Plant Simulation and Cybersecurity

Brandon Rice

January 2018

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy

Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Nuclear Power Plant Simulation and Cybersecurity

Brandon Rice
Idaho National Laboratory
brandon.rice@inl.gov

Abstract

Critical infrastructure protection is vital to the day-to-day operation of any country, and those systems need to be protected to the fullest extent possible. As with what was seen in Ukraine in late 2016, with the cyber attack on the power grid, these systems are susceptible to attacks that can cause serious damage, both physically and economically. This incident shut down the power grid for 6 hours, with nearly 80,000 people affected.

Cyber security can be referred to as the protection of data and systems in networks, both wired and wireless, from unauthorized access or attack. In nuclear power plants, assessments of cyber security are critical to ensuring the safe and reliable operation of the systems used. According to the Nuclear Regulatory Commission (NRC), the purpose of cyber security assessments is to detect and then eliminate or mitigate vulnerabilities in the digital system that could be exploited either from outside or inside the digital system protected area [1]. These cyber security assessments are essentially intended to reduce cyber security risk. The NRC refers to cyber security risk as the combination of the consequence to the nuclear power plant and the susceptibility of a digital system to internal and external cyber attack [2].

Executive Summary

Nuclear power plants are already ensuring strict standards for their control rooms when it comes to cyber security. These measures usually introduce barriers to the control room that require a vetting process before something or someone is allowed entry. While this practice maintains a decent security posture for the main nuclear power plant (NPP) control room (CR), often the simulator is treated with much less scrutiny.

The purpose of this document is to describe measures that should be taken to ensure that NPP simulators maintain a strong security posture, without having to be classified as a critical digital asset. Most of this paper was discussed in Bernard Gagnon's presentation at Power Plant Sim, 2017, titled *Minimizing Cyber Security Threads to the Simulator* [3]. As incidents like what happened in Ukraine continue to happen around the globe, it is vital that industry adhere to a common practice of protecting their simulator infrastructure.

This document will discuss the following:

- Why a simulator would be targeted by an adversary

- Simulator attack surface and vectors
- Mitigations and controls
- Conclusions

Targeting a NPP simulator

NPP simulators are extremely useful in that they represent the actual control room as close to reality as possible, including housing the same type of equipment and controls. Because the simulators are so well represented, an adversary could use this less controlled area as a target for multiple reasons. Some of the information that could be useful to an attacker wanting to eventually target the regular NPP CR includes:

- Piping & instrumentation diagrams
- Training data, such as exams, lesson plans, test results
- Simulator information that could provide PLC logic, databases, or source code
- Electrical diagrams
- Operating procedures
- Safety analysis reports

Were an adversary to collect the piping and instrumentation diagrams, he or she would have an excellent blueprint of the plant's infrastructure. This creates an advantage to an attacker by taking the guessing game out of how particular components might be organized and structured, as well as detailing which instruments can communicate with one another. The information available in those diagrams should be treated as 'need-to-know' as only those who are involved in the operations of the plant should have access to those documents.

Training data would also harvest a lot of useful information to an adversary, providing ample information on techniques and abilities of the operators. Further, test scores and shift schedule could offer information to an advanced attacker that could exploit those correlations.

There is also the potential for an adversary to attack programmable logic controllers (PLC) or other controls residing in the simulator. The risk is that one of these control systems is compromised, and when a replacement cannot be found for the critical CR, it is taken from the simulator. This attack would be advantageous, as the adversary doesn't necessarily have to make his way into a control room; he or she simply needs to find a way to compromise the business network of the corporation.

Other important assets that should be considered proprietary and unknown to an adversary include the simulator servers, engineering workstations, instructor stations, classroom simulators, and controller boards. Should one of those systems

become compromised, the attacker gains unnecessary information of not only the layout of the control room, but the logic behind the controls.

The simulator environment also contains third-party software that is often installed off-the-shelf, with full trust that the software does not contain any adverse malware that might be used to infect the network. This software often times does not get vetted for scope of control and is installed with blind trust that the vendor has no mal intent.

Simulator control rooms can also be host to devices like cameras, microphones, printers, projectors, smart TVs, and cell phones. As the list of devices increases, so does the attack surface, especially if all of the devices are on the same network. Knowing this, an attacker has a lot of vectors that could be compromised, providing full access to a plethora of items with potential vulnerabilities.

Simulator attack surface

While great effort is put into securing the main CR, the simulator is often regarded as another business network asset, sometimes even managed by corporate IT. Previously, most simulators were on an isolated (or air-gapped) network, while considered safer, does not necessarily mean it is protected from Internet threats. This was evident in the "air-gapped" Natanz Nuclear Facility, in which the attack affected centrifuges used to enrich uranium, as well as the Korea Hydro and Nuclear Plant attack that lead to the public release of their blueprints.

Simulators reside on various networks in the industry: business, isolated, or in separated enclaves within the business network. With the advent of Internet of Things, digital control systems, plant PCs, and human-machine interface devices that all communicate over a network protocol, the isolation method has changed and has become more intertwined with connectivity. As technologies advance, the simulator is left with a hodge-podge range of equipment, both legacy and current, all of which needs to communicate in some way. For example, it isn't uncommon to have a rev-locked XP machine that serves to control a legacy, proprietary system while on the same network as a current version of Windows Server. If an intruder were to see an XP machine on the network, he or she is going to take the path of least resistance and likely target that machine first.

In the past, simulator networks still utilized less-than-observant practices of cyber security. Several of these practices would take very little effort of an adversary to wreak havoc on nearly all of the systems. These practices included, but were not limited to:

- Standalone or islanded environment (previously considered safe)
- No patching systems in place
- Single administrator accounts with a common, weak password

- Open SQL databases (non-password protected)
- No simulator network monitoring
- Little to no IT management or maintenance
- Basic recovery mechanisms

These techniques do not take into consideration intellectual property protection, personable identifiable information, exam security, simulator stability, network security or any other forms of risk that may be introduced.

Mitigations and controls

As the simulator control rooms and networks advance in technology, the vectors for potential breech should be scrutinized for vulnerabilities and other areas of attack. The general idea is to lessen the attack surface so that an adversary cannot infiltrate the environment, extracting sensitive information that could potentially harm the NPP.

Some potential entry points include:

- Smart devices
- USB and other mass storage devices
- Bluetooth
- Wireless Internet
- Audio and visual equipment
- IP Cameras
- CD and DVD media
- Software vector
  - Unsupported Operating Systems (Windows XP)
  - Use of unapproved freeware (screen capturing, editing utilities, steam tables)
  - Unknown source software (firmware, embedded software)
- Lack of training to personnel regarding risks of viruses, phishing attacks, visiting suspicious websites, or downloading software from unknown or nefarious sources
- Mandatory reporting of cyber related incidents

Smart devices should be controlled or not permitted into the simulator environment. The risk is that the phone or smart device could contain malware, controlling the device without the user's knowledge. As recently as 2016, ransomware malware has started infecting smart TVs, rending them useless to the user; however, not all malware is designed to make a device inoperable [3]. There are several benefits to an adversary to being able to turn on a microphone or activate a camera without being detected.

Ideally, USB and mass storage devices, once scanned for viruses and malware, and introduced to the simulator environment, should not leave and only be accessed by lock and key by proper personnel. CD and DVD media should be held to the same standard, as well. At the very least, these devices should be scanned routinely or every time they go in and out of the facility. Equally important is ensuring that the device doing the scanning has the latest virus definitions from the vendor, as this can change on a daily basis.

Wireless, albeit convenient, normally presents an unnecessary risk to a network; however, given the relative physical isolation of a NPP, it is not at risk to drive-by or wardriving wireless attacks. An attack on a NPP wireless network would need proximity to be a factor, therefore most would be okay in this regard. However, strong encryption (or other techniques, such as RADIUS or WPA2-Entperise) should be implemented. Further, if no mobile device management is in place, no personal or otherwise non-business devices should be allowed to connect to this network as it usually ties in with the corporate network.

A network strategy that would mitigate threats to the communications infrastructure should include the deployment of a firewall that has control over inbound and outbound connections, even if the termination point is to nothing. Utilization of this technique could also enforce the use of multi-factor authentication for remote access to the simulator, even if coming in from the corporate network. Access from the Internet is highly discouraged, as it broadens the attack surface.

Other devices in the simulator control room include audio and visual equipment. One popular device includes IP cameras, which should not be powered on when not in use, and ideally not be allowed to be awakened via magic packet (Wake-on-LAN). Further, all default usernames and passwords should be changed to complicated, even randomly generated characters and numbers. If possible, ensure that they cannot be logged into via HTTP (port 80) and, if available, only allow logins from HTTPS (secure) connections. This prevents the credentials from being easily obtained from an adversary on the network.

While several devices on the network remain rev-locked, meaning they cannot be upgraded because they control legacy equipment, they should be handled with caution. For example, if an XP device is used to communicate with a PLC, the XP machine should not be able to talk to any other device on the network and vice-versa. Accomplishing this can be done via the implementation of a firewall that can control communications between devices on a network. Further, these rev-locked devices should have their own firewall systems in place between their communication needs and the SCADA network. This mitigation prevents the devices from being manipulated from an unrecognized device that should not be able to control it. Access to these devices should be as tightly controlled as possible in order to prevent the possibility of not only malfunctions, but also a potential attacker who has compromised the network.

Mandatory reporting of cyber security incidents enables those in positions to mitigate risks to better understand what kind of posture the network maintains. This allows for dynamics to be controlled for, and also shows what kind of further steps should be taken to better mitigate against these incidents. It can also provide an example of how much training individual employees may need in order to prevent future cyber security-related events. Even with all mitigations and controls in place in the NPP simulator environment, one vulnerability in particular is the human.

Despite the constant training employees often receive from their IT department about the dangers of visiting questionable sites, downloading unapproved software, or clicking on attachments in links, there are still multiple incidents of people doing this daily. Proper training needs to be not only implemented on the corporate network, but it needs to be conducted for SCADA or simulator environments as well. Adhering to best practices, training, and mitigation is vital to the infrastructures in which we operate.

Conclusions

Cyber security threats are a moving target, constantly evolving and showing themselves in new ways every day. It is prudent to recognize that every industry is vulnerable to the security risks and its potential economic, physical, or safety impacts.

Training simulators hold sensitive information that could be useful to an adversary, so it is important to keep all assets protected. Simulator environments need to be kept with the same care and caution that is held to the corporate IT network, and potentially managed by personnel familiar with cyber security. This can be accomplished by leveraging in-house experts in security and infrastructure that are currently enforcing policies within the corporate environment.

Employees in both environments should welcome the idea of enhanced cyber security precautions in order to protect information from getting into the wrong hands. Implementing a strong security posture benefits everyone involved, except perhaps those illicitly wanting to extract this protected information.

As the world moves into a more digital direction, the nuclear industry will be right alongside, bearing the brunt of bad guys and evil-doers along with everybody else. It is wise to begin ramping up security sooner than later, as the longer it is put off, the more difficult it will be to implement.

References:

1. EPRI, Implementation Guideline for Wireless Networks and Equipment Monitoring, R. Rusaw, December 2009

2. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.152, Rev. 2, January 2006.

3. Android Ransomware Infects LG Smart TV, Retrieved from https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv/ April, 2017

4. Minimizing Cyber Security Threats to the Simulator, Gagnon, B., Presentation from PowerPlant Sim, January 2017