Contribution ID: **548** Type: **Paper**

Evaluating Software Defined Networking Solutions to Reduce the Digital Attack Surface of Nuclear Security Systems

Most nuclear security systems in place today were not designed to address the current threat environment. Systems that were originally intended to be stand alone are now interconnected. Devices that have a single purpose are built on multi-purpose platforms and use communication protocols that, while effective, have no ability to authenticate authorized versus unauthorized commands. These attributes provide an attacker significant ability to affect the system, pivot throughout the interconnected networks, and remain undetected if he or she can compromise a single node.

Software defined networking (SDN) has been used for years by information technology cloud service providers to quickly provision or remove servers or other systems to meet changing demand. The same concept has recently been applied to operational technology systems to enable very fast failover on critical systems that have stringent and deterministic (<5ms) transmit/receive times. Using software defined networking, the communication flows through a network are carefully engineered using preplanned routes and specific pathways. This networking approach makes it possible to achieve deterministic and extremely reliable message delivery, even when components fail. The engineering approach for software defined networking has added numerous security benefits, including but not limited to: securing the networking control plane, eliminating network scanning and mapping, inhibiting Address Resolution Protocol (ARP) spoofing and host masquerading, eliminating unauthorized network pivoting, and enabling greater situational awareness on the network.

Software defined networking in operational technology environments is a relatively new concept. Early testing conducted in electrical power and other critical infrastructure, however, has proven it to be a very effective tool for building reliable networks and reducing the digital attack surface of the network. Researchers at the Pacific Northwest National Laboratory and Idaho National Laboratory are testing software defined networking technologies on a radiation portal monitor system and physical protection system to validate its effectiveness in these common nuclear security systems. In these tests, researchers establish a baseline using existing networking equipment, then replace and configure the existing networking equipment with software defined networking equipment. Once the software defined networking equipment is in place, the team reruns the same tests used in the baseline.

In this paper, we will explain the concept of software defined networking in greater depth and provide an overview of the tests conducted on nuclear security systems and the results achieved. We will also discuss the security benefits of software defined networking in the context of nuclear security systems and consider other nuclear security applications beyond those that have been tested.

State

United States

Gender

Author: CLEMENTS, Samuel (Pacific Northwest National Lab)

Co-author: NICKERSON, Charles (Idaho National Laboratory)

Presenter: CLEMENTS, Samuel (Pacific Northwest National Lab)

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