Contribution ID: **532** Type: **Paper**

The Application of a Systems-Based Approach to Computer Security at Nuclear Facilities

Many member states have chosen to adopt the use of compliance-based approaches when addressing the computer security of nuclear facilities. Such approaches typically mandate the application of a large set of generic security controls to protect every declared sensitive (i.e. critical) digital asset within a facility. The resulting volume of work has resulted in a significant challenge for some nuclear facility operators and competent authorities with respect to implementation and inspection activities.

Although there is merit in a compliance-based approach, it is important to be aware of potential drawbacks. One concern is that under a compliance-based approach, computer security engineers may need to spend a disproportionate amount of time preparing engineering justifications for why specific security controls cannot (or should not) be applied within the nuclear operational environment rather than working to secure sensitive systems from cyber threat. Another concern is the lack of a graded approach to the protection of sensitive systems related to safety, security, and emergency preparedness. If no grading criteria exists with respect to the relative importance of the system to the facility, then everything must be considered equally critical. This can result in applying the same time and resources to securing assets whose compromise poses little risk to the facility and those whose compromise poses much greater risk. There is also the concern that the compliance-based approach may lead to an asset-based mindset. This could result in a situation where the computer security analysis focuses so heavily on impacts to individual assets, it may fail to appropriately consider potential impacts to the design-based functions of the system that can arise when multiple assets are negatively affected by a given cyberattack.

An alternative or supplement to a compliance-based approach involves the use of a phased, systems-based approach that focuses on the protection of design base functions of sensitive systems. With this type of approach, systems are evaluated to (1) determine their relative level of susceptibility to compromise along identified pathways of communication and (2) the consequences resulting from a successful cyberattack. A risk-informed analysis in the systems-based approach provides the technical basis for the selection of security controls to mitigate consequences of cyberattacks.

This paper will report on some of the issues nuclear facilities and competent authorities have experienced with the compliance-based approach for computer security. The paper will identify where the appropriate application of a systems-based approach, as a supplement to (or modification of) the traditional compliance-based approach could improve computer security at nuclear facilities.

State

United States

Gender

Primary authors: LANDINE, Guy (Pacific Northwest National Laboratory); GLANTZ, Clifford (Pacific Northwest National Laboratory)

Presenters: LANDINE, Guy (Pacific Northwest National Laboratory); GLANTZ, Clifford (Pacific Northwest National Laboratory)

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