Contribution ID: **616** Type: **Paper**

A cyber-capability model for compromise of I&C system functions at nuclear facilities

IAEA Nuclear Security Series No. 33-T provides an ordered list of the four potential consequences of a compromise on I&C system function are arranged from worst to best case. These potential consequences are the basis on which to define the computer security requirements for the I&C system functions. IAEA NSS 20 details the need for risk informed approaches to take into account a current assessment of nuclear security threats (i.e. threat actors having intent, motivation, opportunity, and capability to attack a State's nuclear security regime). This need requires understanding of the cyber-capabilities on which to perform a detailed analysis to determine the security requirements.

This analysis can be supported by modelling threat actor capabilities required to compromise I&C system function via cyber-attack. This paper will propose a three-level capability model for use in evaluation of potential consequences and their likelihood of occurrence.

In this model, the threat actor capabilities lead to a classification into one of three "hacker"groups. They are IT hackers, ICS hackers, and nuclear process hackers. IT hackers have knowledge and understanding on how to compromise information technology and could initiate or target cyber-attacks on I&C systems that are likely to be more disruptive (i.e. failure) than causing more severe consequences. This is due to the attribute that IT hackers are not aware of the specialized characteristics of industrial control systems.

On the next level representing increasing threat, ICS hackers have the same capability as IT Hackers (having acquired the general knowledge of information technology) but they also have acquired the specific knowledge of industrial control systems.

On the level representing the highest threat, nuclear process hackers have the same capabilities as ICS hackers, but also have gained the access and understanding of the detailed information about I&C systems at nuclear facilities that they have targeted.

In this model, the different types of attacks are associated with each of the different types of threat actors. Application of this model, reveals that consequences increase in severity as the threat actor behind the compromise progresses from lower threat level (i.e. IT hackers) to the highest threat level (i.e. Nuclear Process Hackers). The three-level model proposed in this paper could also be utilized in development of a more sophisticated model used to develop the cyber design basis threat (cyber-DBT) of nuclear facilities.

Gender

State

China

Authors: LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University.); ROWLAND, Michael (Practical Reason Incorporated); HEWES, Mitchell (IAEA)

Presenter: LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University.)

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