Contribution ID: **82** Type: **Paper**

Evaluation of the appropriateness of Trust Models to specify Defensive Computer Security Architectures for Physical Protection Systems

Monday 10 February 2020 11:30 (15 minutes)

Defensive Computer Security Architectures (DCSA) are a vital element in the application of computer security to nuclear facilities. The DCSA should provide higher degrees of protection to digital assets performing more significant functions. This will increase the difficulty to the adversary as they will need to overcome multiple, diverse, and independent measures to successfully complete an attack.
Basing the DCSA specification on a well-established trust model, allows for effective application of good computer security practices in . Current US Regulation mandates a trust model similar to Biba which prioritizes reliability (e.g. integrity and availability requirements) over confidentiality. This leverages the existing Nuclear I&C architecture for safety which allows for measures such as data-diodes, and restrictive procedures (such as requiring independence and channelization) to be put into place. Implementing a DCSA can be very effective against a cyber attack that could result in sabotage potentially leading to unacceptable radiological consequences (URC).
Current DCSA and its underlying trust model does had not been applied sufficiently to physical protection systems (PPS) where the current practice is to assign all devices to a single security level and apply a 'large zone'around all the components of the PPS. This requires extra effort to physically protect networks and components, as well as provide administrative controls to control access.
PPS contain both personally identifiable information (biometrics) and other confidential information as well as have to operate reliably. With these requirements on the system, the trust model in use for Nuclear I&C (Biba), with its emphasis on integrity and availability is unsuitable.
This paper will aim to propose use of well-established trust models to apply to the DCSA specification for PPS. The trust models to be considered are (1) Biba; (2) Bell-LaPadula; (3) Clark Wilson; and (4) Brewer and Nash. The comparison will (1) identify significant functions performed and/or sensitive data managed by an example PPS; (2) identify the underlying tasks or activities that are required to be successfully achieved to delivery the security function or to protect the data (information); (3) indicate the priority of the Confidentiality, Integrity and Availability (CIA) requirements for each task; and (4) for each task, evaluate each trust model as to whether the information flows they allow are effective or ineffective in providing security.

Gender

Male

State

Canada

Author: Mr SLADEK, John (John Sladek Enterprises Inc.)

Co-authors: ROWLAND, Michael (Practical Reason Incorporated); NICKERSON, Charles (Idaho National Laboratory)

Presenter: Mr SLADEK, John (John Sladek Enterprises Inc.)

Session Classification: Identification, Classification, and Protection of Digital Assets in a Nuclear Security Regime

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