Contribution ID: **643** Type: **Paper**

Scenario Development Through Mapping Transitive Digital Trust Relationships in Computer-based Systems

In 2016 the International Atomic Energy Agency (IAEA) launched a Coordinated Research Project (CRP) on Enhancing Computer Security Incident Analysis at Nuclear Facilities (J02008). One of the major activities undertaken within the CRP was the development of threat scenarios demonstrating the progression of an adversary through the digital systems used within a Nuclear Facility. Another activity undertaken in parallel by the IAEA's division of Nuclear Security, the development of working material for a non-serialised nuclear security publication to assist member states in conducting Computer Security Exercises for Nuclear Security.

Both activities provoked the question - how best to define a scenario that demonstrates the progression of an adversary through interconnected computer-based systems within a nuclear facility with the goal of creating a compromise that results in nuclear security consequences. The adversary would need to progress through multiple levels of computer-based systems and human operators arranged in and supporting a facilities Defensive Computer Security Architecture (DCSA) to achieve this goal, representing the technical specificities of such an approach was seen as a non-trivial exercise.

This paper will explore a methodology implemented and demonstrated through a software application arising out of the combined discussions of the CRP and development of the Computer Security Exercises for Nuclear Security to articulate such a scenario in a clear, flexible, and concise manner. This methodology is provided from a single philosophy: the foundation of security is trust and the reliance of reprogrammable computer-based systems implies a broadly accepting degrees of imperfect digital trust.

Through treating computer-based systems as another form of trusted insiders the methodology provides for the modelling of scenarios by defining elements (people, information, digital assets, and processes) within and external to a facility. The trust relationships that span a facility can then be defined between each of these elements and then the following rules scenarios can be mapped:

1. Trust is imperfectly applied, there exists trust relationships between some elements and adversaries.
2. Adversaries undertake actions to compromise trust relationships held with a connected element.
3. Once an element itself is compromised it becomes adversarial and the trust relationship it holds in turn can be targeted by an adversaries subsequent actions potentially resulting in further compromise.

Using these simple rules the most advanced computer security scenarios to be expressed effortlessly leveraging multi-disciplinary knowledge held throughout an organisation by reducing the technical specificities typically associated with computer security to a simple question that can be posed to anyone: What do we, and the computers we are responsible for, really trust?

Keywords: IAEA, Computer Security, Instrumentation and Control, Nuclear Facilities, Exercises, Trusted Insider, Software, Scenario

Gender

Male

State

Australia

Authors: HEWES, Mitchell (IAEA); Mr BARRY, Adam; PETERS, Joshua (Australian Nuclear Science and Technology Organisation); ESKANDER, Javan (Australian Nuclear Science and Technology Organisation)

Presenter: Mr BARRY, Adam

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