Seminar 4 – Nuclear installation and materials security – Session 1

Chaired by M. Pelzer (GRS) / L. Mandard (IRSN)

10:00 - 10:30 | No. 401

Insider threat and computer security, is there a specific profile?

O. Fichot (IRSN)

In the infosec community, insider threat is a “buzzword” which covers several different meanings.

However, in the nuclear field, IAEA has precisely defined it as “an adversary with authorized access to a nuclear facility, a transport operation or sensitive information”. Because many functions in nuclear facilities are now digitalized, computer networks are natural targets for a malicious actor and the agency’s definition of an insider can be applied to computer security. In that aspect, “authorized access” can be broken down into two distinct domains:

- Physical access to a network equipment.
- Logical access to accounts/network functions.

Of course, to be able to generate a significant impact like a major denial of service, extraction of sensitive data or takeover of the industrial process, an adversary must gain a high level logical access (in technical terms, he basically needs at some point to become “root” or “admin”), hence the widespread belief that insiders, in the computer security field, must have a deep computer and network knowledge and a high level of access rights, which can only be found in a small group of IT specialists like administrators, IT architects, maintenance or computer security engineers.

Insiders could be found in this population but real life has shown something very different. By analyzing TTP’s (Tactics, Techniques and Procedures) of past cyberattacks, some use cases with insiders can be highlighted.

Indeed, for targeted attacks on critical or high value networks, the threat actor will tend to use an insider to bypass the defensive measures in place, either an airgap or a hardened outside perimeter. This insider has just a very basic and one-time role to execute a single action, generally to plug a device in the targeted network. This device will establish a covert communication channel (either through the Internet or more probably through mobile networks) with the main team waiting discreetly and anonymously outside the network. This team will then proceed to the following steps of the attacks by escalating privilege and moving laterally,

Seminar 4 – Nuclear installation and materials security – Session 1

Chaired by M. Pelzer (GRS) / L. Mandard (IRSN)

without the insider's help, to gain better logical access until they reach their goal and strike. In short, the insider just needs a physical access to the targeted network.

In conclusion, insider threat covers a short but essential and critical phase in the overall computer attack and there is indeed no specific profile for insider in computer security : unskilled individuals with the right physical access to network or terminal devices represent a real danger if they act with malicious computer security experts outside the facility.

We should consider two criterias when assessing this threat:

- Physical access to an element of the network with which an insider can interact. That could be an endpoint, switch, firewall…. Or a simple ethernet plug.
- Possibility of setting up a covert communication channel between the outside team and the tool left behind by the insider.

Seminar 4 – Nuclear installation and materials security – Session 1

Chaired by M. Pelzer (GRS) / L. Mandard (IRSN)

10:30 - 11:00 | No. 402

Experimental Testing and Modelling of Radiation Portal Monitors

C. Deyglun (IRSN)

Each year, radioactive materials are lost, stolen or discovered as material out of regulatory control. Most incidents are minor, but material is potentially available for criminal acts. The ability to detect illicit transport of radiological or nuclear material is important to reduce the threat.

Fixed installed pedestrian Spectroscopic Radiation Portal Monitors are designed to be used at checkpoints to detect an increase of the level of ambient radiation in order to alert of the presence of nuclear or radioactive material. Because testing nuclear security equipment on site can be difficult and restrictive, IRSN developed a process to evaluate the performances of a pedestrian portal, based on a combination of experimental data and simulation.

Experimental data are collected within the laboratory using platforms designed for testing pedestrian Spectroscopic Radiation Portal Monitors. Two platforms are used: a static test platform with a pop-up design and a dynamic test platform with a conveyer-rail design. Many scenarios were tested with different sources using realistic setups and many experimental data were collected using radioactive and nuclear material available in IRSN nuclear security laboratory.

Based on the data provided in the user manual and the standards found in the industry, MCNP simulations were performed to calculate the detection probability and the false alarm rate for different measurement scenarios. The MCNP model of the portal and its surroundings were adjusted to be as realistic as possible based on measurements performed with americium, caesium, cobalt, barium and europium reference sources. Once the model validated, all variables inherent in the measurement, such as background fluctuations, source locations, etc, were considered. Their relative contributions were identified and quantified, then propagated to predict an overall uncertainty on the number of gamma-rays counted by the portal.

The results were then used to test the sensitivity of Spectroscopic Radiation Portal Monitors to special nuclear materials for different alarm thresholds. This process applied to different scenarios according to defined targets should help in the selection of operating characteristics of the portal.

Seminar 4 – Nuclear installation and materials security – Session 1

Chaired by M. Pelzer (GRS) / L. Mandard (IRSN)

11:00 - 11:30 | No. 403

Evolution of security systems during decommissioning of nuclear power plants in Germany

P. Terberger (GRS), M. Pelzer (GRS) and U. Weizel (GRS)

The German decision to phase out of the use of nuclear power following the 2011 Fukushima nuclear disaster led to the ongoing process of deactivation and decommissioning of all nuclear power plants in Germany. During decommissioning of a nuclear power plant, the inventory of radioactive materials changes continuously as components are processed and removed from the plant. This may affect the level of both security and safety measures, while the general aim of protecting persons, property, society, and the environment remains unchanged.

In this presentation experience gained recently from the decommissioning of German nuclear power plants regarding the security systems and their interface with safety is shown and discussed. Starting from an integrated, synergetic set of security measures and safety measures the security level may decrease as the inventory of radioactive materials decreases. The feasibility of a graded security approach depending on the inventory of radioactive materials is examined using examples derived from practice. In the course of the decrease of the necessary security level, in some cases safety measures may already be sufficient to meet security requirements. This is especially the case for radiation protection measures, e. g. access control and radiation monitoring of personnel at exits. Security may also be relevant if certain infrastructure (e. g. air locks) is added to the power plant buildings. In this context it is discussed how a decrease in security level may promote inconsistencies in the implementation of certain security measures.

The decommissioning of nuclear power plants in Germany has shown, that it may be practical to construct separate support facilities for dismantling or on-site storage of radioactive materials. Security measures for those facilities need to be defined individually in advance, depending on the intended inventory of radioactive materials. These measures may differ significantly from those for the actual power plant. When planning the security system, radiation protection measures are taken into account. The general aim of both safety and security to protect persons, property, society, and the environment remains unchanged for the support facilities.

Seminar 4 – Nuclear installation and materials security – Session 1

Chaired by M. Pelzer (GRS) / L. Mandard (IRSN)

During decommissioning of a nuclear power plant and the resulting decrease in inventory of radioactive materials, deterioration of security and safety culture may occur due to several reasons. A smaller inventory appears a lot less dangerous, therefore power plant staff may be less eager to comply with safety and security regulations. Also, the absence of proceeds after deactivation of the plant may increase pressure on managers to minimize expenses. Managers might be tempted to cut funding for safety and security measures. Therefore, adequate levels for security and safety culture need to be defined and may be adjusted, as the risk potential slowly decreases.

Seminar 4 – Nuclear installation and materials security – Session 1

Chaired by M. Pelzer (GRS) / L. Mandard (IRSN)

11:30 - 12:00 | No. 405

Blast effects: A small-scale experimental approach for nuclear security

S. Trélat (IRSN), M. Sturtzer (ISL), J. Legendre (ISL) and F. Braina (IRSN)
A. Tournier (IRSN)

Precise determination of blast characteristics is critical in the field of sensitive infrastructures (nuclear plant for instance) global security as a direct impact may lead to catastrophic damages in certain conditions.

IRSN conducts and analyzes experimental studies in order to improve the scientific knowledge on blast characteristics in free-field and phenomena governing its propagation around obstacles, useful in the context of its position of technical support to the French nuclear security authority.

A well-described literature technique consists in performing experimental simulations on a smaller scale. This technique provides easier access to a large amount of experimental data at a reduced cost, but it however requires the validation of the scaling laws necessary to extrapolate conclusions for larger or full scale configurations.

In this regard, IRSN has designed and built an experimental set-up dedicated to hemispherical blast effect assessment using down-scaled plastic explosives charges (ranging between 10 and 100 g in TNT equivalent). The set-up consists of a modular table and non-deformable mock-ups, both being equipped with pressure sensors. The modularity of the blast table enables to place the explosive charge at any location on its surface.

The present work summarizes the development of this set-up as well as some tests that have recently been performed in two geometrical configurations in cooperation with the French German research institute of St-Louis: 50g (IRSN configuration) and 400g (ISL configuration). TNT equivalent charges were respectively detonated, on ground level, in the vicinity of a reference solid hemi-cylinder, representative of considered convex structures.

Seminar 4 – Nuclear installation and materials security – Session 1

Chaired by M. Pelzer (GRS) / L. Mandard (IRSN)

The objectives addressed by this experimental approach are the following:

- at first, the provision of extensive experimental data on the interaction of blast with reference targets,
- the better understanding of the wave reflection phenomena and the improvement of current analytical prediction methodologies,
- the contribution to numerical codes validation and the identification of the most adapted tools or methods for blast effects assessment,
- a critical input for numerical simulation of different structures resistance.

These results will finally provide design guidance for small scale blast experiments and real critical infrastructure for government agencies in addition to other classic tools able to predict average loading on blast exposed surfaces.