Advancing Computer Security for Radiation Detection Systems through IAEA Coordinated Research Project

Rodney Busquim e Silva
International Atomic Energy Agency (IAEA)
Email r.busquim@iaea.org

Michael T. Rowland
Sandia National Laboratories (SNL, USA)
Email: mtrowla@sandia.gov

Gregory White
Lawrence Livermore National Laboratory (LLNL, USA)
Emial: white6@llnl.gov

José Roberto Castilho Piqueira
University of Sao Paulo (USP, Brazil)
Email: piqueira@lac.usp.br

Jianghai Li
Tsinghua University (THU, China)
Email: lijianghai@tsinghua.edu.cn

Tamas Holczer
Budapest University of Technology and Economics (BME, Hungary)
Email: holczer@crysys.hu

Khalil El-Khatib
Ontario Tech University (OT, Canada)
Khalil.el-khatib@ontariotechu.ca

Abstract

This work presents the results of the on-going International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) J02017 entitled Enhancing Computer Security for Radiation Detection Systems. Radiation detection systems are comprised of a large number of fixed and mobile radiation detectors used for safety and security purposes for nuclear power energy production, nuclear fuel cycle activities, nuclear research reactor operation, medical applications, transportation of nuclear material, environmental monitoring, border control and major public events (among others). The signals generated by radiation detection and physical protection systems produce alarms (and information) that are transmitted and monitored locally or remotely and additional alarm monitoring centers. The transmission of this information across a diverse range of communication channels increases the effectiveness of radiation monitoring and detection systems, and the timely responses to alarm conditions. During signal generation and transmission, processing or storage of information, there is the possibility of compromise and manipulation of data, requiring computer security measures to protect and preserve the confidentiality, integrity, and availability of the information being transmitted, assessed, and stored. The research also includes the physical protection systems that protect other radioactive material from theft or sabotage.

The objective of the IAEA CRP on Enhancing Computer Security for Radiation Detection Systems is to develop methodologies and techniques to improve computer security of radiation detection equipment, physical protection systems, associated computer-based systems, data communications protocols and the network infrastructure that supports the use of these systems. This panel will discuss the ongoing IAEA CRP research addressing computer security issues related to radiation detection equipment, the need of cybersecurity capacity in specific nuclear security domains; the specific challenges involved with researching cybersecurity for nuclear security; and it will summarize key projects within the IAEA CRP J02017 and their potential benefits to capacity building efforts in Member States with mature nuclear security programs and newcomer countries.

1. INTRODUCTION

Operations of nuclear and other radioactive material facilities, along with systems and measures for the detection and response to nuclear and other radioactive material out of regulatory control, rely on real time detection of radiation. The signals generated by radiation detection systems produce information that are transmitted and monitored in central alarm stations and additional alarm monitoring centers. This information is transmitted across many different communication channels increasing the efficiency of monitoring and detecting radiation, and the timely application of security responses to alarm conditions. As the processes of signal generation and information transmission are vulnerable to data compromise and manipulation, it is essential to implement robust computer security measures to ensure the confidentiality, integrity, and availability of the transmitted, assessed, and stored data.

The IAEA CRP J02017, titled Enhancing Computer Security for Radiation Detection Systems, aims to improve the computer security of Radiation Detection Systems (RDS). The project's research focuses on ensuring the secure operation of RDS in nuclear security and safety applications, including during Major Public Events (MPE) [1] and in the detection and response to nuclear materials and other radioactive materials outside of regulatory control (MORC) [2]. To achieve this, the project is developing innovative methodologies and techniques to enhance the computer security of radiation detector equipment, associated computer-based systems, communication protocols, and network infrastructure.

The researchers this project have multidisciplinary expertise and have been working in cooperation to advance the research on computer security for radiation detection used in nuclear power plants (NPPs), nuclear fuel cycle activities, nuclear research reactor operation, medical applications, transportation of nuclear material, environmental monitoring, border control and major public events among others. A multidisciplinary research team, from many participating institutes from ten IAEA Member States is working in a coordinated way in several aspects:

- Defining strategies for connecting radiation detectors sensors.
- Exploring cyber-security of wireless detector networks.
- Developing models for propagation of malwares in distributed radiation detector networks.
- Identifying anomalies during radiation detection system’s operation.
- Developing virtual test-beds simulating the radiation detection architecture.
- Exploring the application of data encryption in radiation detection networks.
- Studying the cybersecurity resilience in radiation detection data transmitted or stored in the cloud.

This work summarizes the ongoing CRP J02017 activities.

2. PARTICIPATING INSTITUTES

Operations of nuclear facilities such as NPPs and research reactors, of installations, such as ionizing radiation and border monitoring control facilities, and secure operations during MPE and during transport of nuclear material [3], require real time detection of radiation level. The four basic radiation detection devices (RDDs) are:

- Fixed radiation portal monitors (RPMs).
- Personal radiation detectors (PRDs).
- Hand-held gamma and neutron search detectors (GSDs and NSDs).
- Hand-held radionuclide identification devices (RIDs).

The critical function of a radiation detection equipment is the identification of radioactive materials for the safety and security of the public, workers and environment. This project brings together 11 participating institutes from 10 IAEA Member States, all of which are actively contributing to this initiative:

- Austrian Institute of Technology GmbH (AIT, Austria), with the project "Threat Analysis and Anomaly Detection for Next Generation Radiation Monitoring System Computer Security".
- University of São Paulo (USP, Brazil), with the project "Cyber Security Assessment of Radiation Detection, Associated Systems and Networks".
- Tsinghua University (THU, China), with the project "Cyber-Physical Approach to Enhance Computer Security of Radiation Detection Systems"
- Ontario Tech University (OT, Canada) with the project "Building Resiliency in Sensor Cloud for Radiation Detection System (RDS)".
- Egyptian Atomic Energy Authority (EAEA, Egypt), with the project "Interference Management and Advanced Encryption Techniques Application in Radiation Detection Systems".
- Nuclear Regulatory Authority (NRA, Ghana), with the project "Improving Computer Security of Radiation Detection System".
- Budapest University of Technology and Economics (BME, Hungary), with the project "Virtualized Networks and Automatic Scenario Generation for Enhancing Computer Security of RDSs".
- National Research and Innovation Agency (INS, Indonesia), with the project: "Security Consideration in the Design and Implementation of LoRaWAN-based Radiation Monitoring System".
- National Centre for Nuclear Research (NCBJ, Poland), with the project "Testing the Cybersecurity of Wireless Communication Between Remote Radiation Detection Systems and Dosimetry Centre".
- Georgia Tech (GTU, USA), with the project "Development of Cyber-Attack Detection Systems for Radiation Detection Systems".
- Sandia National Laboratories (SNL, USA), with the project "Analysis of Defensive Cyber Security Architecture (DCSA) Effectiveness Analysis for the Physical Protection of Radiological Material".

3. SUMMARY OF CURRENT STATUS OF THE PROJECTS

Radiation detectors equipment usually have a small signal processing unit that allows for data processing, handles sensor data and communicates with other sensors in a time-driven or on-demand way, and allows for self-configuration. In a bi-directional communication channel, technical mechanisms must guarantee that the radiation detection equipment, which process and store the collected data, is secure against compromise. Moreover, the detection radiation equipment must be properly calibrated to ensure appropriate handling [4] in order to identify material that pose risks to public safety and security. For example, bi-communication protocols must ensure that an adversary will not change the equipment configuration, which includes the calibration or background radiation levels.

The following summary outlines the status of the current research by the participating institutes involved in this project. This overview provides a concise snapshot of the ongoing research activities, highlighting the key contributions of each institute:

- AIT
  AIT research activities leverage the artificial intelligence-based security tool, ThreatGet [5] to conduct a comprehensive analysis of a refence RDS architecture:
  - Established a ThreatGet server and provided access to select CRP participants.
  - Created and distributed Digital Asset Datasheets to select project partners for information gathering, to be used in Threat and Vulnerability assessments using ThreatGet.
  - Developed and investigated of use cases and threat scenarios against RDS
  - Conducted an analysis of threat vulnerability of RDS from open source data.

- USP
  USP is currently developing two main research sub-projects leveraging the modeling and simulation experience after the IAEA CRP J02008 [6] and modeling activities for virus propagation:
  i) Model Development:
    - A code has been prepared for simulating clustered propagation models in large-scale systems of any arbitrary order.
    - Stability analysis of the model is ongoing for order 3 and higher.
    - A dynamic model for malware propagation is being developed.
    - A reference model for MPE is being developed.

  ii) Virtual Testbed Development:
    - The testbed framework has been defined.
    - The simulation tools have been selected and the coding started.
    - Basic and general virtual nodes have been developed using a Docker/container approach in a Linux deployment.

- THU
  The research activities undertaken by THU comprehends:
  - A network architecture model has been developed for radiation monitoring systems in AP1000 NPPs, featuring connections between various radiation monitors via RS-485 and Ethernet communication.

- A test bed has been built to simulate the system, including radiation data generators, signal splitters, programmable logic controllers (PLCs), gateways, and an anomaly detection system.
- An Operation Technology (OT) Intrusion Detection System (IDS) with Security information and event management (SIEM) has been containerized using Docker and Linux Core, enabling the capture and analysis of network traffic, anomaly detection, and security log generation. The SIEM aggregates and correlates events, triggering alerts when certain conditions are met.

- OTU

  OTU is currently developing two main research sub-projects:

  i) Development of an efficient IDS:
     - This sub-project aims to create a robust intrusion detection system for radiation detection systems. Currently, OTU is conducting experiments to assess the performance of the machine learning models developed.

  ii) Threat Analysis of Radiation Detection Systems:
     - This sub-project involves a comprehensive threat analysis of radiation detection systems to identify potential vulnerabilities and risks.

- EAEA

  The research activities undertaken by EAEA are related to Wireless Sensor Networks (WSNs):
  - EAEA is developing a solution to mitigate channel jamming or interference in WSNs by calculating interference temperature using the Channel Availability Metric (CAM) and switching channels as needed.
  - To address the vulnerability of WSNs to internal node compromise, a two-step approach is proposed: first, an anomaly detection step is conducted to identify unusual patterns in sensor readings, using mean and standard deviation calculations for each node.
  - In the second step, a reputation-based algorithm is employed to determine the cause of the anomaly, whether it's a fault, malicious activity, or false data injection attacks.

- SNL

  The research activities undertaken by SNL, in collaboration with Lawrence Livermore National Laboratory (LLNL), comprehends:
  - Development of physical protection system (PPS) and RDS simulator.
  - Specification of technology stack: Unity Engine, MATLAB/Simulink [7], MiniMega [8], and Open-Source Relational Database.
  - Specification of MATLAB/Simulink functional blocks for PPS. Including:
    - Interior Sensors
    - Access Control System
    - Biometrics
    - Exterior Sensors
    - Radiation Detection Systems.
  - Release of Gula Regional Hospital 3D Model.
  - Development of simple demonstration of the technology stack.

- NRA

  The research activities undertaken by NRA are related to RDDs:
  - RDDs (i.e. identiFINDER and Polimaster) have been analyzed in terms of their architectural components and functions.
  - The impact of known classes of malware on the component architecture of the identified RDD has been assessed.
  - Vulnerability scenarios considering attack pathways and defensive considerations have been developed from the observed impact of malware on the component architecture of the RDD for defensive capability development.
  - Investigations of the impact of malware on cloud data acquisition, data processing and data distribution radiation detection data are on-going.

- INS

  The research undertaken by INS comprehends activities on Long Range Wide Area Network (LoRaWAN):
  - Prototype of RDD utilizing LoRaWAN and PIN-Photodiode detector based on Arduino platform, and communication module for integrating commercial RDD have been developed.
  - Architecture of Private LoRaWAN-based radiation monitoring system was proposed. Setup of outdoor and indoor LoRa Gateway (concentrator) was done. Network coverage around the gateways has been tested using developed LoRa node.
  - Conducted assessment of possible security threats mainly for LoRa Gateways.
  - Real measurements of radiation dose rate were collected using developed node. Radionuclide spectrum data for Co-60, Cs-137, Cs-134 were collected and can be used to develop data communication format, synthetic data generation algorithm, and algorithm to detect radiation and cyber events.

- BME

  The research undertaken by BME comprehends the following activities:
  - A country-wide early warning system was chosen as our test scenario, featuring two distinct RDDs. We analyzed the systems and implemented a virtual topology using the infrastructure as coding approach, leveraging Ansible [9] and Terraform [10] for rapid, reproducible, and easy deployment.
  - To address the lack of synthetic data generation methods for RDDs research, a system based on generative neural networks was developed.
  - A comprehensive model was developed to handle various devices, services, operations, and connections, serving as the foundation for a threat scenario.
  - An evaluation of cyber-security of back packs has been conducted. A set of exercises tailored to these devices are under development.

- NCBJ

  The research undertaken by NCBJ comprehends the following activities:

- Designed of virtual private network (VPN) and consulted it with Polish regulator and country-wide Radiation Emergency Centre CEZAR, taking into account a possibility of a dual system consisting of wired and wireless systems, complementing each other and giving possibility for redundancy increasing the system resilience to possible attacks.
- Started testing the functionality of the cybersecurity test bed and development of measurement procedures, which includes state of the art encryption technologies.

- GTU

  The research undertaken by GTU comprehends the following activities:
  - Development of a RDS text bed with hardware in the loop capabilities.
  - Investigation of cyber threat vectors for RDSs by attempting to exploit various communication channels.
  - Development of fault and cyber-attack detection models capable of identifying when a radiation detection system is operating outside of a given tolerance.
  - Development of machine learning classifier for cyber-attacks.

4. FINAL REMARKS

In conclusion, the CRP on Enhancing Computer Security for Radiation Detection Systems (J02017) brings together 11 organizations from 10 Member States to advance the secure use of radiation detection systems. Through their research, the participating institutes have explored various topics, including defensive computer security architecture, anomaly detection techniques, malware propagation in RDDs, sensor cloud computing, wireless technologies, PPS-RDS coupled simulation, and threat modeling. These efforts aim to improve the computer security of radiation detection systems in various security and safety nuclear applications.

In the first year of the project, the IAEA hosted a research coordination meeting at LLNL (November 2023) to discuss research plans, cooperation opportunities, and project facilitation. A consultancy meeting was also held at USP (June 2024) to advance research on testbed development, network integration, cloud computing, threat modeling, and synthetic radiation data generation. During this meeting, researchers defined a common reference model based on a major public event. This model will facilitate the integration of all techniques and methodologies under development. In addition, the CRP's contributions to the IAEA International Conference on Nuclear Security: Shaping the Future (ICONS2024) provided a platform to share the project's results and outcomes with nuclear community.

To summarize the project results to date, the participating institutes collectively agreed on reference models for synthetic radiation data and cyber data. The institutes developed and tested various anomaly detection techniques, conducted vulnerability assessments of RDDs, and created prototypes of test beds (virtual and hardware in the loop) and simulators, including a PPS-RDS simulator featuring a 3D model of a hospital. Additionally, the propagation of malware in a virtual network was explored, and the cyber-security of wireless networks for transmission of radiation data has also been investigated.

As this coordinated project continues to progress, the collective efforts of the participating institutes will have a significant impact on enhancing the computer security of radiation detection systems, contributing to ensure the confidentiality, integrity, and availability of the transmitted, assessed, and stored radiation detection information.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for Major Public Events, IAEA Nuclear Security Series No. 18, IAEA, Vienna (2012).

[2] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev. 1), IAEA, Vienna (2020).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Combating Illicit Trafficking in Nuclear and Other Radioactive Material, IAEA Nuclear Security Series No. 6, IAEA, Vienna (2007).

[5] THREATGET - THREAT ANALYSIS AND RISK MANAGEMENT. https://www.threatget.com/. Accessed on 30 June 2024.

[6] CRP Success Story: Enhancing Computer Security Incident Analysis at Nuclear Facilities (J02008). https://www.iaea.org/newscenter/news/crp-success-story-enhancing-computer-security-incident-analysis-at-nuclear-facilities-j02008. Accessed on 30 June 2024.

[7] MathWorks. https://www.mathworks.com/products/simulink.html. Accessed on 30 June 2024.

[8] What is minimega? https://www.sandia.gov/minimega/ Accessed on 30 June 2024.

[9] Ansible Collaborative. https://www.ansible.com/ Accessed on 30 June 2024.

[10] Automate infrastructure on any cloud with Terraform. https://www.terraform.io/ Accessed on 30 June 2024.