SAND2018-13446C

Security Enhancements to the Leksell GammaKnife®

A collaborative project between the
Office of Radiological Security and Elekta Instrument AB

Per Kjäll, Michal Kuca

ORS
Office of Radiological Security
Protect · Remove · Reduce

Elekta

IAEA, Vienna, 3-7 December 2018 International Conference on Security of Radioactive Material Contribution ID :138

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Agenda

- Background
- Project Overview
- Design Challenges
- As-built Security Solution
- Project Experience

ORS and IDD

ORS
Office of Radiological Security
Protect · Remove · Reduce

- The U.S. Department of Energy (DOE) National Nuclear Security Administration (NNSA) Office of Radiological Security (ORS) works with governments, law enforcement, and businesses across the globe to protect radioactive sources.

- The In-Device Delay (IDD) program supports ORS's Protect mission.
  - Partners with manufacturers to incorporate engineered security enhancements into device or facility designs that will make illicit removal of sources difficult.
  - Incorporate detection components as well as delay where possible to increase time for local law enforcement to respond.
  - Existing devices/facilities retrofitted with enhancements; new devices/facilities incorporate enhancements into manufacturing process.

IDD provides substantial delay time against an adversary that attempts to remove the source from the device, thus buying time for off-site responders to arrive at the site to contain the adversary.

Elekta Instrument AB

- Manufacturer of equipment to treat tumor diseases and brain disorders
- Focus areas:
  - Radiation therapy
  - Brachytherapy
  - Stereotactic radiosurgery
- Leksell GammaKnife®
  - Utilizes Co-60 for stereotactic radiosurgery
  - Treats disorders and tumor diseases in the brain

The Project

- Initial engagement in 2010
    - Nondisclosure Agreement
    - Requirements Specification Development
    - Vulnerability Assessment
    - Design and Testing
    - Implementation
- Design Objectives:
    - Access Delay
    - Intrusion Detection
    - Meet or exceed potential adversary capability
    - Ability to re-load sources periodically
    - Patient and staff safety
    - Clinical throughput

Design Challenges

- LGK is required to conform to applicable medical standards and requirements
    - Security solution cannot interfere with these requirements
    - i.e. Electromagnetic Compatibility (EMC)
- Must not effect device maintenance and service
- Device must be accessible at all times during treatment
- High patient treatment throughput

System Design

- Security system design is proprietary however…
- Delay enhancements cover most likely points of access
  - Delay hardware exceeds design goal
  - Increases time required for source reloading however within acceptable design limits
- Detection solution integrated into delay components
- Utilized common physical security design principles
  - Detection before delay
  - Defense in Depth
  - Layered Approach
- Removed elements that might aid adversary

Implementation

- Some design modifications made at the factory
- Delay and detection elements installed at licensee (end user) site during:
  - Initial Device Commissioning
  - Source Re-loading
  - Maintenance/Service visits
- Intrusion detection elements integrated into medical facility alarm system
  - Coded as critical alarm
  - Staff/response training

- Pilot installations started in 2016
- ~60% of all eligible LGKs in U.S. completed
- Some LGKs upgraded in Europe

Lessons Learned

- Elekta/ORS needed to agree on Potential Adversary Capability (PAC)
- Ensure device compliance is not violated
- Inclusion of all stakeholders (especially end users) is critical
- Requirements Specification
- Run security design through desktop simulations
- Pilot installations provided valuable data:
  - Logistics
  - Technician training
  - Coordination with end users and response entities

Questions