Cyber Threats in the Nuclear Sector

Tudor Radulescu
UTI Grup

04 November 2015
Nuclear engineers focus on safety...

... terrorists focus on killing people
Reasons to protect nuclear facilities

Critical infrastructure

• Nuclear power plants generate significant power levels, hence a high impact on the available power in case of unplanned shutdown

Nuclear material

• Attractive targets for terrorists
• Can become weapons of mass destruction
• Potential environmental effects
Timeline of the nuclear sector

1950
- 1st nuclear power plant connected to grid (1954, Obninsk, Russia)

1960
- Chernobyl accident (1986)

1970
- 1st physical protection guide (1972)
- Introduction of DBT for physical protection (1979)

1980
- September 11th Twin Towers attack (2001)

1990
- Fukushima accident (2011)

2000
- 1st PP regulation in Romania (2001)
- First serious cyber incident in a nuclear plant (2003, Davis Besse, USA)
- Cyber-physical vulnerability proof of concept - project Aurora (2007)

2010
- 1st guide on CS for nuclear installations (2009)
- Stuxnet (2010)

2020
- Introduction of CS regulations in Romania (2014)
Game-changing Cyber Security Events

Slammer Worm

• Fast spreading (75,000 computers in 10 minutes)
• In 2003, SQL Slammer worm **infected the Davis Besse nuclear power plant** in Ohio, USA
• It created a disruption in operation of
  • Safety Parameter Display System
  • Plant Process Computer
• Multiple points of entry
  • including remote connections by contractors
• No radiological consequences
Game-changing Cyber Security Events

**Stuxnet**

- Produced **physical damage** to industrial infrastructure (kinetic effect)
  - Destroyed more than 1000 centrifuges for uranium enrichment in Natanz plant in Iran
  - 60% of the cases of infection in Iran
- Aimed at PCs running WinCC/Step 7 control software (industrial automation)
- Able to use network for propagation, but was introduced by USB flash drives
- Complex
  - 4 zero-day vulnerabilities
  - two compromised digital certificates
Game-changing Cyber Security Events

Flame

- Discovered in 2012, in Iran
- One of the most complex pieces of espionage software
  - 20MB in size (Stuxnet was only 500kB)
- Able to perform complex intelligence gathering
  - audio recorded through computer’s microphone
  - keystrokes
  - screen captures
  - network traffic sniffing
  - nearby Bluetooth devices monitoring
- Referred as “cyber weapon”
Credibility of Cyber Threat in the Nuclear Sector

• Cyber-attacks have been proven effective in obtaining physical effects
• This can result in the undesired release of radioactivity, without any need for physical attack
• Cyber-attacks can be used to prepare and assist a physical attack by
  • disabling or denying the service of physical security systems
  • interfering with nuclear accountability databases
  • disabling safety mechanisms
• Alteration of information in nuclear materials accountability databases can facilitate nuclear material theft
Shift towards Cyber Security

Regulatory bodies start to perceive the threat

• In 2009 NRC published a chapter in Title 10, Code of Federal Regulations, Part 73, called “Protection of digital computer and communication systems and networks”.
  • “the licensee shall review the cyber security program as a component of the physical security program”

• In 2010 NRC published the Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities

• In 2011, IAEA published the “Computer Security at Nuclear Facilities”

They are developed as “patches” to an existing traditional body of knowledge and practice of physical protection
Threat Actors

Recreational hackers
• Closest similarity in the physical world: casual vandalism
• Low resources
• Minimal access to information

Disgruntled current/former employees
• Aim towards
  • obtaining revenge by sabotaging the installations
  • damaging the image of the employer or
  • assisting external factions that have interests against the employer
• Attitude
  • passive
  • active
Threat Actors

**Activists and extremists**
- Driven by ideological motivations
- Aim to create a strong media coverage of an attack
- Cyber-attacks – embarrassing the nuclear site operator or public authorities

**Organized crime**
- Involved for financial gain
  - directly (theft of material for contraband or theft of information)
  - indirectly (blackmail, holding the site hostage)
- High level of resources
- Professional expertise
Threat Actors

Terrorism
- Plays on building fear in the public, so terrorists rely on massive media coverage
- High level of resources
- Trained personnel
- Highly skilled members recruited for specific tasks

Covert agents
- Aim to steal information on either industrial or intellectual property
- Insiders, with either physical access to the plant or some sort of legitimate remote access
- Included in the program for protection of classified / confidential information in the past

State Actors
Potential targets

Nuclear reactors
• Nuclear power plants, research reactors

Nuclear materials processing and storage facilities
• Uranium mines, nuclear fuel production plants, enrichment plants, fresh and spent fuel storage

Radioactive sources
• Relatively small quantities of nuclear materials used in medicine and research

Nuclear materials in transit
• Fresh and spent nuclear fuel, radioactive sources transport

Information on any of the above
• Design documentation, specifications, logs, credentials of the nuclear installation and
• Nuclear material inventory databases
• Information on personnel with legitimate access
Information and computer systems security

Aspects that can be compromised

• Confidentiality
  • Public disclosure aimed at affecting the operator or the industry
  • Information leak in preparation for an attack
  • Real-time information in support of an attack

• Integrity
  • Altering the information to cover material theft
  • Spoofing attacks intended to mislead operators and allow other attacks to go undetected

• Availability
  • Disabling the safety systems
  • Altering the functioning of the security systems
  • Power supply cuts
Categories of systems

Systems in the scope of regulation
- Nuclear security systems
- Physical protection systems
- Nuclear accountability systems
- Emergency response systems

Other systems
- Classified information systems
- Business network
- Online public systems (public website, environmental reporting)

Networks
- Designed or rogue
- Sneakernet (use of portable media)

“Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway”
(Andrew Stuart Tanenbaum, in Computer Networks, 1989)
Cyber Security of the Physical Security System

Trends...

• IP connectivity
• Virtualization
• Internet of Things
• Full integration – all access management

... that bring new challenges

• Securing the physical protection network
• Resilience of the security system (segmentation, redundancy, diversity)
• Ensuring the availability of the response
Supply chain security

Counterfeit equipment

• Apart from the IPR problems, it introduces major security issues

Backdoors and time bombs

• Cause premature equipment failure or unpredictable failures
• Allow remote control of equipment
• Propagate attacks within secure networks
• Collect information
• Exfiltrate information
About UTI

- **Civil Infrastructure & Security**
  Improve your business processes and technologies through our civil infrastructure, security and facility management solutions and services.

- **Critical Infrastructure Security**
  Integrate complex systems for critical security areas based on comprehensive risk analysis and threat assessment services.

- **Traffic Management**
  Benefit from a complete range of urban and interurban traffic management systems, solutions and services, assuring mobility and traffic safety.

- **IT & C Solutions**
  Leverage integrated systems and services for IT, information security and business solutions, delivering increased added value, productivity and progress.
Cyber Security Solutions

IT Infrastructure Management
- IT Asset Management, IT Vulnerability Management

Network Security
- Firewall/NGFW/UTM, Threat Prevention Platform, IDS/IPS, VPN/Encryption, Web Application Firewall

Process Computers Security
- Specialized SCADA / DCS solutions

Communication Security
- Mail Server Security, Web Gateway Security

Data Security

Collaboration Security

Endpoint & Mobile Device Security

Threat Monitoring

Integrated in a comprehensive security plan
Cyber Security Services – first Private CERT in Romania

Consulting
- Vulnerability Assessment
- Security validation (Pentesting)
- Security Policy Design
- Network Security Design

Managed Services
- Monitoring (SIEM)
- Network Security
- Communication Security
- Data Security
- Endpoint Security

CSIRT
- Alerting Services
- Incident Handling
- Vulnerability Handling
- Data Forensics
- Malware Analysis

Special Services
- Cyber Investigation
- Threat Intelligence
- Advanced Correlation
- Vulnerability Analysis
International coverage

IT and Cybersecurity

• International presence in 10 countries
  • Digital tachograph cards provider: Romania, Bulgaria, Finland, Moldavia, Norway, Tajikistan, Serbia, Croatia, Ukraine and Uzbekistan
  • PKI solutions delivered in Albania and Azerbaijan
  • Mobile security for Azerbaijan e-Government services
• International interoperability tests
• Partnerships and strategic technology alliances
Thank you!