Learning Objectives

After completing this module, you should be able to:

• Identify information systems associated with nuclear materials, nuclear facilities, and physical protection systems

• Be familiar with threats against information systems including adversary goals and potential attack points

• Understand process and guidelines for establishing Computer and Information Security
Motivation

- Daily, we hear of new, successful cyber attacks - the threat is active and evolving. Also, best practice requirements dictate [1]:

  “**Computer-based systems used for physical protection, nuclear safety and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the threat assessment or design basis threat.**”


---

Types of Information Systems

**Systems where information is stored, used, or transmitted**

<table>
<thead>
<tr>
<th>Mode</th>
<th>People</th>
<th>Physical</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types</td>
<td>Knowledge, Skills</td>
<td>Paper, Equipment</td>
<td>Networks, Communications, Stored Data, Digital Control Systems</td>
</tr>
<tr>
<td>Examples</td>
<td>Where are materials located, How to handle nuclear materials</td>
<td>Policies, Procedures, Entry control lists, Security plans, System design, Schedules (i.e., material movements)</td>
<td>Sensor network systems, Entry control system, Material inventories, Safety control systems, Plant configuration, Smart cameras / motion sensors</td>
</tr>
</tbody>
</table>
Computer Systems in Nuclear Facilities

**Safety Systems**
- Protection systems for automatically initiated reactor and plant protection actions
- Safety actuation systems (initiated by protection systems)
- Emergency power

**Safety-related Systems**
- Process control
- Control room - controls and alarms
- Fuel handling and storage
- Fire protection systems

**Non-Plant Equipment**
- Office automation
- External connectivity

**Security-related systems**
- Access control systems
- Voice and data communication
- Clearance database
- Alarm monitoring and control
- Computer and network security
- Nuclear accountancy

[3] Compiled from NSS-17 (Section 5)

Common Features

- Central servers and workstations
  - Usually run Windows operating systems current as of installation, rarely receive security updates, and are not always in protected zones

- Field Panels
  - Usually run embedded operating system, rarely receive security updates, and may be physically accessible

- Communications Network
  - Moving almost exclusively to Ethernet and IP, for which a wide variety of attack tools already exist (and require little knowledge)

How are these located and protected?
An attacker that gains access at any point can use well-known tools to manipulate or deny monitoring
Remote, Protected

Information Security

Supply Chain Attack Model

Untargeted attacks possible

Component designers

Foundries

Suppliers

Designers

Contracted manufacturers

Assemblers

Physical Product

Specific attacks possible

Firmware and software developers

Firmware/Software Storage & Mfg Installation Network

Integration & Testing

Warehousing (Vendor or Contract)

Attractive, targeted attacks

Firmware/Software Storage & Mfg Installation Network

Integration & Testing

Existing Installation

The Twenty-Sixth International Training Course
Page 4
Potential Adversary Goals [4]

- Information gathering for planning further malicious acts (reconnaissance)
- Attack disabling or compromising computers or security / safety control systems
  - For example, adding an identity
- Compromise of computers or digital control systems combined with other modes of attack, such as physical intrusion
  - For example, degrading a sensor sensitivity

[4] Discuss threats to information systems based on NSS-17

Computer Attack Phases [5]

- Goal identification
- Reconnaissance
- System access / compromise
- Attack execution
- Covering of tracks to maintain deniability


Not within the awareness / control of the defender so active defense must anticipate adversary and limit information

Increasingly, control system attacks and tools are becoming more sophisticated
Energy Companies Compromised

- Dragonfly / Energetic Bear [6]
  - Windows-based but targeted energy companies
  - Successfully exploited thousands of power plants
  - Install malware, steal data, run executable files
- Blackenergy [7]
  - In development since 2007!
  - Trojan malware and root kit (gain foothold and download other malware, such as KillDisk)
  - Linked to wide-scale power outages in the Ukraine
- Nuclear Power Plant Target [8]
  - December 14, South Korea’s Korea Hydro and Nuclear Power (KHNP) successfully hacked. Nuclear power plant design information stolen

Not New, Not Hypothetical!


Attacker Tools

- Attack tools can be purchased openly [9]
- Malware targets control systems
- Agora Software – offers “unpatched” vulnerabilities, not detectable by existing virus scanning or malware protection

Stuxnet – Advanced Attack Sophistication [10]

- Successful attack against the "closed" network of a nuclear facility
- Targeted specific machinery, so it was informed by insider reconnaissance
- Software used encrypted network traffic for external command and control
- Software passed standard trust policies (used driver signing keys of two companies)
- Self-propagation - infects additional hosts via 3 alternate paths


- Follow national legal and regulatory requirements
- Apply relevant IAEA and other international guidance
- Ensure senior management support and adequate resources
- Define a computer security perimeter
- Identify interactions between computer security and facility operation, nuclear safety and other aspects of site security
- Create a computer security policy
- Perform risk assessment
- Select, design and implement protective computer security measures
- Integrate computer security within the facility’s management system
  - Regularly audit, review and improve the system.

[11] Key steps in Chapter 5 of NSS-17
Defense in Depth [12]

• Protection requirements should reflect the concept of multiple layers and methods of protection (physical, technical, and administrative)

[12] NSS-17, Section 2.3.3

Fundamental System Architecture and Design Principles

• Prevent loss of integrity
• Maintain availability
• Ensure confidentiality

Design Considerations

• Protection Levels
• Access Levels
• External Connectivity
• System Interfaces

- Zone borders enforced with decoupling mechanisms (e.g., air gaps and data diodes) to prevent unauthorized access and error propagation
- Technical and administrative measures ensure decoupling
Protection Measure Options

- Administrative Controls
  - Training
  - Policies and procedures (example, password management)
  - Principle of Least Privilege
- Physical Protection of Information System Assets
  - Lock rooms or cabinets where computer systems or digital control systems are located
  - Limit access to areas where computer systems or network components, particularly servers, are located, such as outdoor wiring cabinets
- Mitigation / Recovery
  - Periodic backups made and protected at the same level as the original
  - Recovery from backups is tested

Technical Controls

- Network design and configuration management
- Detection and logging
- Firewalls and routers
- Zone enforcement with firewalls, data diodes or air gap

**Virus Protection** – For analyzing data for malicious signature

**Encryption** – For data in storage and during transport

**Authentication** – For knowing who is doing what and attribution

**State of Health** – Validating technical controls are functioning as expected
Summary

• Various types of information systems exist and all of them need to be protected
• Adversaries can use a number of different tools to attack an information system
• Access to any part of the system can cause systems to not function as intended
• A graded approach – to require different sets of protection measures to satisfy the security requirements for information system in a given level – should be created