RIC 2011
Cyber Security – Licensing and Implementation at Nuclear Power Plants

March 9, 2011

1

Cyber Security – Digital Platform Cyber Vulnerability Research

Jeanne Dion
NRC Office of Research
March 9, 2011

2

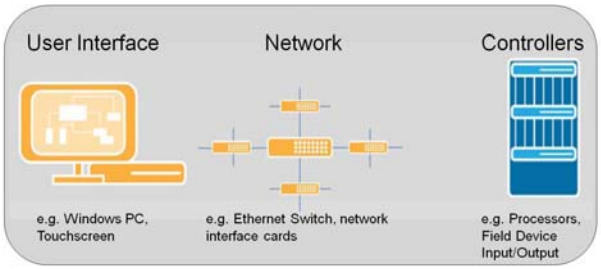
Introduction

- **Cyber Security for Nuclear Power Plants**
  - – Increasing trend to modernize Instrumentation and Control (I&C) systems
  - – Increasing emphasis on securing national infrastructure
- **NRC Cyber Research**
  - – Proactive effort to identify potential vulnerabilities in digital I&C systems
  - – Goal is to raise awareness about cyber security
  - – Findings will help to better understand how to protect digital I&C from computer-based threats

3

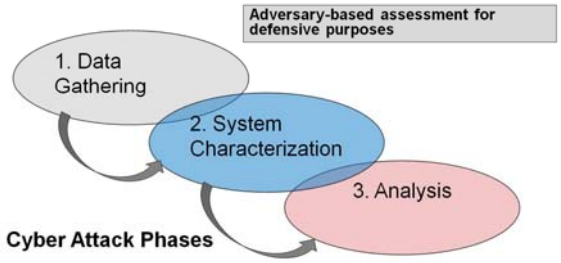
Platform Vulnerability Assessments

- **Multiple digital platforms assessed at the Sandia National Laboratories**



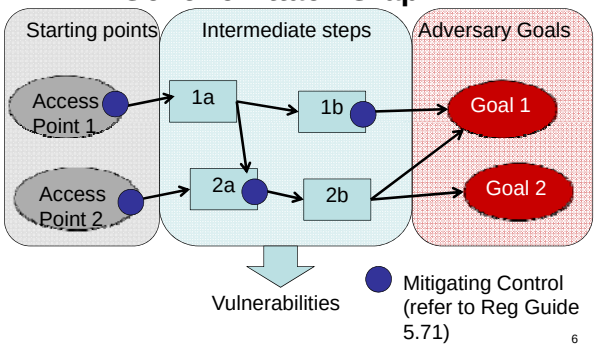
4

Red Teaming Assessment Methodology



5

Generic Attack Graph



6

Generalized Findings

- Engineering workstation vulnerabilities
  - Outdated operating systems
  - Unnecessary services or functions
  - Continuous connections to control systems
  - Multiple network interface cards
- Networking Elements
  - Open unused ports on ethernet switches
- Control System
  - Insecure communication protocols

7

Mitigating Controls

- Multiple approaches to mitigate vulnerabilities
- Some mitigating technical controls are not appropriate for control systems
- Implement alternative controls or countermeasures where appropriate

8

Observations from Assessments

- A targeted attack requires a lot of detailed information
  - Prevent adversary from creating attack by eliminating the opportunity to gather information
- Digital displays can be replayed or altered
  - Rely on hardwired alarms/indicators for critical information
- Important to correctly identify critical digital assets and ensure they are protected under cyber security plans

9

Conclusions

- **By identifying vulnerabilities from an adversary's perspective, we can understand how technical controls can be effectively applied**
  - **Controls listed in Regulatory Guide 5.71 are the cornerstone to protecting digital assets at plants**
- **Generalized findings**
  - **Informed NRC's cyber security inspection training**
  - **Lessons learned form all assessments to be summarized in a final report**

10