BNL-112742-2016

An Approach for Assessing Consequences of Potential Supply chain and Insider Contributed Cyber Attacks on Nuclear Power Plants

Tsong-Lun Chu, Athi Varuttamaseni, Joo-Seok Baek and Susan Pepper

2016 ANS Winter Conference
Las Vegas, NV

November 2016

Nuclear Science & Technology Department

Brookhaven National Laboratory

U.S. Department of Energy
Office Of Science
American Nuclear Society

DISCLAIMER

An Approach for Assessing Consequences of Potential Supply Chain and Insider Contributed Cyber Attacks on Nuclear Power Plants

Tsong-Lun Chu, Athi Varuttamaseni, Joo-Seok Baek and Susan Pepper

Brookhaven National Laboratory, 33 N. Renaissance Road, Upton, NY 11973, chu@bnl.gov

I. INTRODUCTION

The Stuxnet attack at the Natanz facility is an example of a targeted and successful cyber attack on a nuclear facility. Snowden's release of National Security Agency documents demonstrated the consequences of the insider threat. More recently, the United States tried to attack North Korea but failed, South Korea was attempting to attack North Korea, and both applied Stuxnet-like approaches. These sophisticated targeted attacks differ from web-site hacking events that are reported almost daily in the news mainly because targeted attacks require detailed design and operation information of the systems attacked and/or are often carried out by insiders. For instance, in order to minimize disruption of facilities around the world, Stuxnet remained idle until it recognized the specific configuration of the Natanz facility, demonstrating that the attackers possessed extremely detailed information about the facility. Such targeted cyber attacks could become a national-level military weapon and be used in coercion of hostile countries.

While U.S. nuclear power plants (NPPs) are well designed and protected and not easily attacked through internet hacking, there have been a few digital-system-related incidents. For example, in 2003, the Slammer worm breached the private network of the Davis Besse plant[1]and disabled a safety monitoring system for almost five hours. The breach did not pose a safety hazard because the plant was offline, but it demonstrates the vulnerability of NPP systems. The worm did not enter the plant systems directly; it began by entering the systems of a Davis Besse contractor, and entered through the T1 line bridging the contractor's computer and Davis Besse's corporate networks. The T1 line was not protected by the plant's firewall.

The success of the Stuxnet-Natanz case demonstrates that supply-chain level attack (i.e., physically tampering with digital systems to install undetectable malware for the purpose of bringing harm to a player further down the supply chain network) plays a crucial role in a successful attack. Although attacking an NPP naturally requires more complex strategies and tactics than internet hacking, NPP's have a variety of sophisticated and possibly sensitive systems that may be attacked. Previous studies, for example, Baylon[2], have identified and confirmed that such attack strategies and tactics can be designed and could produce severe damage to an NPP.

Current NPPs were designed according to design basis accidents that predate use of the internet by the general public and did not take into consideration potential cyber attacks that could be carried out by state-sponsored attackers and malicious insiders. To date, no detailed engineering analysis has been performed to realistically examine the consequences these attacks may have on the plants. In this paper, we discuss an approach for assessing the potential consequences of Stuxnet type of attacks. We will examine the engineering criteria used in designing the plants, develop possible attack scenarios in terms of the structures, components, and systems (SSCs) being controlled by digital systems at the NPPs, perform engineering analysis to determine if the attacks would impose conditions that are beyond design bases, and categorize the consequences of the potential accidents.

II. SUMMARY OF THE APPROACH

II.A. Identification of Potential Attack Scenarios

NPPs in the United States have converted many of their non-safety-related Instrumentation and Control (I&C) systems (i.e., balance of plant systems that are used in normal operation of the plants) from analog to digital, while only a few plants have replaced some of their analog safety-related systems (that are used in mitigating accidents). The identification of potential scenarios starts with an inventory of digital I&C systems used at NPPs[3] which determines the systems that can potentially be attacked. Potential attacks may also involve attacks on combinations of digital I&C systems. Design information of the I&C systems and the SSCs that they control will be collected such that the extent of potential attacks can be determined. Design basis accidents that were used in designing the NPPs provide design requirements of the SSCs at NPPs. They also serve as potential events and accidents that can be caused by cyber attacks. Potential attack scenarios can also be identified by reviewing known safety concerns/issues (e.g., turbine missiles, water hammers, low temperature over pressurization, and reactivity accidents) of NPPs. Current probabilistic risk assessments (PRAs) of NPPs do not include risk from

cyber attacks, but provide scenarios that may be caused or made worse by cyber attacks.

Potential consequences (e.g., long term reactor shutdown, accident initiating events, and core damage) will also be identified. The scenario developments will be supported by engineering analyses of Section II.B to ensure the scenarios are realistic.

II.B. Engineering Analysis of Attack Scenarios and Their Consequences

The objective is to realistically assess the consequences of the attacks. The engineering analyses may include informal back-of-the-envelope calculations or detailed analyses using tools in thermal hydraulics, neutronics, and structural analysis (e.g., RELAP5 and TRACE). The engineering analyses will take into consideration the design basis of the NPPs, e.g., the safety margins that were built into the design. In some cases, releases of radioactive materials and health effects on the population also may need to be analyzed.

II.C. Categorization of Consequences of Attacks

The engineering analysis will provide detailed information on the consequences of the attack scenarios. The direct consequences of the attacks may include unexpected reactor trips, long-term unavailability of the plant, unavailability of safety systems, and damage to the reactor core. In addition, those attacks that may lead to breach of containment and public health effects can be identified. The risk significance of the attacks can be examined from the perspective of PRAs of the NPPs.
turbine overspeed protection,

III. AN EXAMPLE SCENARIO: TURBINE OVERSPEED PROTECTION FAILURE

Steam turbine generators are used at nuclear power plants as well as non-nuclear power plants. Turbine over-speed can lead to a catastrophic failure of the turbine, with resulting fires, explosions, and missiles that can further damage the equipment at the plant. Turbine overspeed accidents had occurred and are an important issue for the plants.

In recent years, many nuclear power plants have replaced their analog electro-hydraulic control systems with digital ones that also perform turbine over-speed protection functions. The protection function is needed when there is a generator trip. The digital systems may be more accurate but are susceptible to supply chain and insider attacks. An attack that disables the protection function would result in a turbine overspeed accident. It may cost a hundred million dollars to replace the turbine and repair the damages.

IV. CONCLUSIONS

This paper provides an approach for developing potential attacks on I&C systems of NPPs and assessing their consequences. An important concept is that the NPPs were not designed to cope with Stuxnet-type of attacks (and any other cyber attacks). That is, the plants were only designed for design basis accidents. The safety margins and redundancies built in the design are all based on design basis accidents. They may be helpful in mitigating cyberattacks, but may not be adequate.

In our approach, the attack scenarios are defined in terms of the I&C systems at the NPPs and how the systems may be used to manipulate the SSCs at the plants to create accidents. An assumption was made that the attackers have full access to the digital I&C systems at NPPs and are knowledgeable of the design details of the plants. The approach does not take into consideration how attackers would gain access to the systems and knowledge of the plants.

In order to fully assess cybersecurity risks of NPPs, modeling methods for the likelihood of cyberattacks need to be developed. Then an overall model for supporting risk-informed decision making can be developed.

REFERENCES

1. U.S. Nuclear Regulatory Commission, “Potential Vulnerability of Plant Computer Network to Worm Infection,” NRC INFORMATION NOTICE 2003-14, August 29, 2003.

2. C. BAYLON, R. BRUNT, and D. LIVINGSTONE, “Cyber Security at Civil Nuclear Facilities - Understanding the Risks,” Chatham House Report, ISBN 978 1 78413 079 4, September 2015.

3. R. T. WOOD, R. A. JOSEPH III, K. KORSAH, M. D. MUHLHEIM, J. A. MULLENS, “Classification Approach for Digital I&C Systems at U.S. Nuclear Power Plants”, Oak Ridge National Laboratory, LTR/NRC/RES/2012-001.