Survey of Cyber Security Intrinsic for a Nuclear Power Plant

Yoo-Rark Choi [a*], Jae-Cheol Lee [a]
KAERI, P.O.Box 105, Yuseong Daejeon Korea
yrchoi@kaeri.re.kr

1. Introduction

Federal agencies are facing a set of emerging cyber security threats that are the result of increasingly sophisticated methods of attack and the blending of once distinct types of attack into more complex and damaging forms[1].

Spam, phishing, and spyware, while once viewed as discrete consumer challenges, are being blended to create substantial threats to large enterprises, including federal systems and digital I&C of a NPP (Nuclear Power Plant) is one of them.

The cyber security policy for a NPP has been established for years by KINS, but its scope is very broad and conceptual.

We will describe several important cyber security issues for a NPP in the applicative boundary.

2. Cyber Security Factors

Cyber security plays an integral role in a wide range of areas - from protecting personal information to protecting a nation's critical infrastructure.

2.1 Data Security

A data breach occurs when unsecured personally identifying information held by an individual, company or government agency is mishandled, lost or stolen - resulting in confidential information falling into the wrong hands. Personally identifying information is most commonly defined as any data that links an individual's name with his or her Social Security, driver's license, financial account, medical or other confidential personal information.

Data breaches occur in a variety of ways. One common thread is the data lost is in a format easily read by thieves. Some of the most common include[1]:

- Lost, stolen or misplaced computers, laptops, computer storage (USB) or backup devices
- Tapes containing data backups or transfers that disappear in transit
- Information inappropriately transferred or sent out via e-mail, Web mail, file transfers or instant messaging
- Data inappropriately removed via USB ports to, as an example, USB drives
- Data stored on network, file or email servers that is remotely accessed by hackers or accessed by employees without authorization
- Hackers exploiting viruses, Trojan horses, weak passwords or security loopholes to harvest information
- Improper destruction of information - both physical (dumpsters) and electronic (laptops)
- Poor business practices such as sending postcards that include Social Security numbers

2.2 Foreign Access

Foreign Access includes remote access and all finds of sniffing. Remote access provides flexibility in locations where employees may perform their jobs and allows them to work at home, at an alternative office or other location.

Developed in the early 1970s, remote access is widely used in private industries. Remote access is popular with employees because it frees them from the drudgery of commuting and provides flexibility for personal activities. Employers also like remote access because it helps to keep workers happy, increases productivity, reduces overhead and saves money. Society also benefits from reduced traffic congestion and pollution.

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic.

Two types of security are crucial for securing foreign access[1,2]:

- Network security for intra-agency communications and connections used by remote workers.
- Data fabrication.

2.3 Other factors

Virus and spyware are critical threats in a cyber network. They can be used to break down important computer systems that are controlled by government. Spread of the virus and spyware causes crash of the national security. Almost contamination of virus and spyware are incurred through portable storage devices and network data transmission.

DDOS(distributed denial-of-service) is an attempt to make a computer resource unavailable to its intended users.

Physical cyber security is a important factor, too. But it is not our concern in this paper.

3. Cyber Security in SCADA

SCADA stands for Supervisory Control and Data Acquisition. SCADA systems are computer-based monitoring tools that are used to manage and control critical infrastructure functions, such as the transmission and distribution of electricity, pressure and proper flow of gas pipelines, water treatment and distribution, wastewater collection, chemical processing and railway transportation systems control, in real time. They are just one implementation of Process Control Systems (PCS), a term commonly used in conjunction with SCADA.

Because today's SCADA systems are completely computerized and located on centralized networks, they are a tempting target for a major physical or cyber attack. SCADA equipment often covers large geographical areas with some equipment residing in remote locations. These remote areas are an easy target for intruders or vandalism. Protecting these vital plants from system failures, intrusions or terrorist attacks is critical to the viability of overall critical infrastructures. A major physical or cyber attack on the control and data systems of electric power plants, or oil and gas refineries and pipelines could potentially bring a country to a halt. The problem is compounded because private companies control 85 to 90 percent of critical infrastructures, leaving governments few avenues to ensure that IT systems are secure.

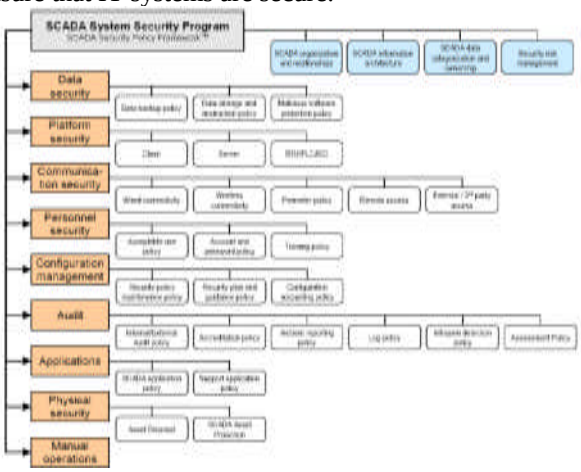

Fig. 1. Cyber Security Policy for SCADA

SCADA systems, like all computer networks, are vulnerable to hacking, intrusions, viruses, data loss, data alteration and the like. There are four main threat categories to consider[1]:

A. Malware – SCADA systems are vulnerable to various forms of malware, including worms, viruses, Trojans and spyware.

B. Insider – This internal threat can be accidental or intentional; however, the latter is the greater threat and is commonly referred to as the "disgruntled employee" scenario, where a knowledgeable insider may be motivated to damage or corrupt the system.

C. Hacker – This is an outsider who is interested in probing and breaking into a SCADA system because of the challenge it presents.

D. Cyber Terrorists – A SCADA system is a very appealing attack target for a well-funded terrorist group that seeks to cause widespread damage to a large portion of the population. Al Qaeda is one organization that has demonstrated increased interest, for example, in U.S.-based SCADA systems.

4. Cyber Security Issues in a NPP

There are many kinds of threat to a NPP in term of cyber security but the corresponding solutions are developed to confront with them.

The networks in a NPP are forced to have isolation concept. It includes the methods of how to protect the safety I&C between the safety and non-safety I&C networks. The NPP I&C networks must be isolated with any other networks, but it does not keep up.

Virus contamination of the digital I&C system was occurred in Japan and America. The foreign access(sniffing) with infected portable computer, network data transmission and non-isolated network are the cause of it. The possibility of foreign accesses and spread of virus and spyware always exist.

KINS/GT-N27, the regulations for cyber security for the Korean NPPs that is announced by KINS includes all of the IT cyber security concepts. It requires authentication and authorization, access control, cryptography, Data validation, intrusion detection and defense, logging, training, audit, verification/validation, and response against the threats in term of technical aspect.

It is clear that the threats to a NPP's cyber security must be eliminated, but the costs for the elimination may incur critical failure to the digital I&C network. The NPP's I&C network must keep severe time limitation rules. But the time costs for the elimination of cyber security threats conflict with the time limitation of the digital I&C network[2].

5. Conclusion

Many kinds of cyber security technologies that are developed in the IT industry may be applied to the digital I&C network that is used in the nuclear industry.

But all of the network systems and their components always have holes and they will act as a potential cause for cyber security disturbances.

Cyber security activity for a NPP must be performed but the cost efficiency must not give critical effect to the performance of the digital I&C network and systems.

Network isolation, maintenance of data integrity and the monitoring of foreign accesses are the intrinsic issues in a NPP. When an invasion accident happens in a NPP digital I&C system, the activities such as a detection of the invasion and preventing data manipulation by the invader must be executed at least. The authority control, data transmission flow control, data cryptography and network access control must be executed to achieve them, too.[2].

REFERENCES

[1] Cyber security industry alliance, cyber security issues, CSIA, http://www.csialliance.org

[2] Y.R. Choi, S. B. Hong, I.S. Koo, and J.C. Lee, A state of art of IT secutiry technologies for cyber security, KAERI/AR-784/2007, 2009.