Transactions of the Korean Nuclear Society Autumn Meeting
Jeju, Korea, October 21-22, 2010

Cyber Security on Nuclear Power Plant's Computer Systems

Ickhyun Shin
[a]*Korea Institute of Nuclear Nonproliferation and Control, Expo-ro 573, Yusung-gu, Daejeon, Korea 305-348*

1. Introduction

Computer systems are used in many different fields of industry. Most of us are taking great advantages from the computer systems. Because of the effectiveness and great performance of computer system, we are getting so dependable on the computer. But the more we are dependable on the computer system, the more the risk we will face when the computer system is unavailable or inaccessible or uncontrollable. There are SCADA, Supervisory Control And Data Acquisition, system which are broadly used for critical infrastructure such as transportation, electricity, water management. And if the SCADA system is vulnerable to the cyber attack, it is going to be nation's big disaster. Especially if nuclear power plant's main control systems are attacked by cyber terrorists, the results may be huge. Leaking of radio-active material will be the terrorist's main purpose without using physical forces.

In this paper, different types of cyber attacks are described, and a possible structure of NPP's computer network system is presented. And the paper also provides possible ways of destruction of the NPP's computer system along with some suggestions for the protection against cyber attacks.

2. Types of Cyber Attacks

There are many different types of cyber attacks with many different types of purposes. And it has a trend.

In early 21st century and late 20th, when the internet was beginning to popular among people, hackers tended to show their computer skills or ability by breaking down computer systems operated for the industrial or organizational purpose. One of the methods is to make malicious codes including virus, worm which uses the network to send copies of itself to other nodes without any involvement from a user. And some virus such as Trojan programs circumvent confidentiality or control objectives and can be used to gain remote access to systems, gather sensitive information, or damage systems and data.(Juniper). One of the severely damaged cyber attacks in Korea was the Slammer worm happened on January 25th of 2003 from 14:10 pm to 23:00pm. People were not able to access the most electronic shopping malls and online game sites. It resulted great damage of 150 Billion Won. The hacker who developed the slammer worm took advantage of the vulnerability of MS-SQL. The Microsoft released the patch of the MS-SQL 6 months prior to the accident . The severe accident would not have happened if IT managers patched the MS-SQL Software when it came out.

When hackers became more skillful on cyber attack and hacking technology became more general, their purpose of hacking changed toward the information gathering rather than just ostentation. Hacking of Auction.com was the one of such cyber attack which happened on 2008. About 18 million account information of auction.com member leaked to Chinese hackers. This information leaking accident was caused by the human factor; one of the IT managing personnel opened up the suspicious email which had a malicious code.

Latest cyber attacks are mostly related with money. DDoS is commonly used for making profit from attacking illegal online companies running adult-entertainment business such as illicit sex service and gambling. DDoS, Distributed Denial-of-Service, attack is an attempt to make a computer resource unavailable to its intended users.(Wikipedia). People can't access the websites when Zombi PC's infected by malicious code occupied all the resources of the target websites. The cyber commercial agencies providing hacking service are also growing fast as companies, especially in the field of electronic market, are competing with each other. They will do anything if it is profitable.

And there are also international cyber terrorists whose job is to gather nation's secret information and intrude nation's important system such as NPP. Physical invading on highly secured facilities is very difficult compared with the cyber invading. Because the nuclear power plants hold the highest physical protection standards of any industries and the cyber security of the NPP is not considered as important as the physical protection.

3. Possible Structure of NPP's computer systems

NPP's computer systems are generally composed of two types of network system which are as follows ;

1) Internet : The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite to serve billions of users worldwide.(Wikipedia). Representing homepage of NPP's must be connected to the internet so that people can access the homepage to get general information

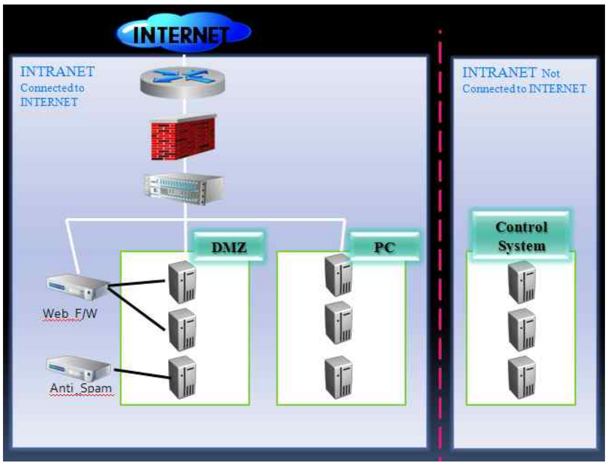
about the NPP. There are also some other information systems which are publicly open for the purpose of taking applications from job-seekers or contractors.

2) Intranet : An intranet is a private computer network that uses Internet Protocol technologies to securely share any part of an organization's information or network operating system within that organization(Wikipedia). Actually there are two types of intranet; one is that the private network is connected to the Internet but it is protected by information security systems such as Firewall or Intrusion Protection System. The other one is that the private network is physically isolated from outside network. The IT systems in the former network are as follows; ERP, Enterprise Resource Planning, which is used to manage the resources and functions of a business, KMS, Knowledge Management System, which used for sharing information, experiences and practices, within the organization. Those systems are accessible from outside of company in case for traveling employees. In order to access remotely, they need a authentication which is usually a SSL, Secure Socket Layer, certificate. And the IT system in the latter network is the NPP's control system which controls operation, management and so on.

4. Methods of Attacking the NPP's computer system and Suggestions of its Security

There are many ways to attack the representing homepage of NPP through internet, since the site is open to everybody and has lots of web-vulnerabilities. Some of the methods for cyber-attacking the homepage are as follows; DDoS which makes the homepage unavailable or inaccessible, SQL-Injection and XSS, Cross Site Scripting, which used for gaining access to the managing page of the site, which the hackers can do anything they want; manipulating the information or shutdown the system and so on. To protect the homepage system, some security information systems are needed along with the continuous monitoring of the system. Firewall is the very basic device for the access-control of visitors of homepage. And the IPS, Intrusion Protection System, is also needed to probe what the visitors have in their pockets. The Web-Firewall is the necessary system for preventing from web-vulnerability attacks such as SQL-Injection.

With the case of NPP's control system which is not connected to the internet, hackers are not able to access to it no matter what, unless they visit the facility of NPP. Therefore, controlling and monitoring the actual visitors of facility are more important than monitoring the cyber visitors.



"General Structure of Information Security System"

5. Conclusion

The greatest threat of all is the lack of understanding within the industrial organizations—in both operations and IT departments—as to the seriousness of the problem. Even control system vendors still are not designing technologies for security. In fact, many are instead including vulnerable applications and technologies such as Microsoft IIS, Bluetooth wireless communications, and wireless modems in their latest offerings. But the policy makers are gradually focusing on cyber security of NPP. And it's great to see that the NRC, Nuclear Regulatory Commission, of U.S.A issued Nuclear Regulations 10 CRF 73.54 "Protection of digital computer and communication systems and networks." This rule states "By November 23, 2009 every one of the 104 U.S. plants and companies seeking to license new plants must submit a comprehensive cyber security plan."

REFERENCES

[1] Juniper Networks.(2009). Nuclear plant control system cyber vulnerabilities and recommendations toward securing them. Retrieved from http://www.juniper.net/us/en/local/pdf/whitepapers/2000338-en.pdf

[2] www.wikipedia.com