Nuclear Cyber Security Case Study and Analysis

Sunae Park[a*], Kyung doo Kim[b]
[a]*ChungNam National Univ., 99 Daehak-ro, Yuseong-gu, Daejeon, 34134, South Korea*
[b]*Korea Atomic Energy Research Institute, 1045 Daedeok-daero, Yuseong-gu, Daejeon 305-353, South Korea*
[*]*Corresponding author: sapark@kaeri.re.kr*

1. Introduction

Due to the new trend in cyber attacks, there is an increased security threat towards every country's infrastructure. So, security measures are required now than ever before.

Previous cyber attacks normal process consists of paralyzing a server function, data extraction, or data control into the IT system for trespassing. However, nowadays control systems and infrastructures are also targeted and attacking methods have changed a lot.

These days, the virus is becoming increasingly serious and hacker attacks are also becoming more frequent.

2. Nuclear Power Plant Security Cases

2.1 Stuxnet Virus

In the past, viruses only attacked hard disk data, deleted information, extracted data, via malware, but now Stuxnet virus has potential which can result in a much more serious situation.

Since 2011, Stuxnet was termed Called “cyber sniper” and it has the ability to destroy critical infrastructure. One example of a critical infrastructure attack was the paralyzing the operation of centrifuges Iran's nuclear facilities.

So the question becomes: who made this virus? The answer is not clear, but many people assume that they were made from Israel and America. People are not able to know for sure if this is true though, because it is open source, so everyone can use and modify it freely.

This virus is a computer virus produced for the purpose of destroying the infrastructure, such as power plants, airports, railways June 2010, and it was first discovered in Belarus.

Israel, the US, and other countries are believed culprits behind Stuxnet attacks on other nations such as Iran.

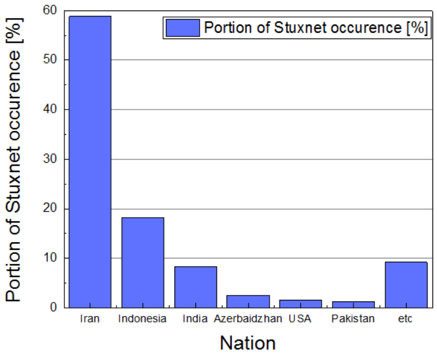

Fig. 1. Portion of Stuxnet Occurrence

If the virus discovers an attack goal, then it can hijack the process control signal and perform a man-in-the-middle attack to send a false signal. This signal prevents software from being able to stop the system and detect malfunctions. The software cannot detect the malfunction and the signal controls the system to not shut down. If some conditions are satisfied, this virus attacks the system otherwise it won't.

The potential threat of Stuxnet virus is one to be wary of. Extremely specialized knowledge-based industries’ functions and facilities are known by potential hackers. Development and gathering of knowledge about the vulnerability of power plants or other industrial facilities have been prioritized by the attackers.

The fact that there is no way to know when you have malware or a virus or how much damage is possible, makes it a top concern for people today.[1]

2.2 Case Study

One major security threat is in nuclear power plant reactors. Where the power supply can be cut off, and it can seriously affect the reliable operation of the nuclear power plant instrumentation and control systems.

A nuclear safety threat can undermine the stability in the reactor protection system in normal operation.

In addition, safety and non-safety system malfunction can occur in plants such as hacking prevention, and disruptions in power supply may occur.

Moreover, if you can’t control the system it causes technical problems, such as data modulation and outflow, transfer delay, a malfunction of the nuclear power instrumentation and control system may cause enormous damage.

Table I : Nuclear Power Plant's Cyber Attack Cases

Nuclear Power Plant	Year	Results
US Davis-Besse Nuclear Power Plant	2003	Stopped for 5 hours
US Hachi Nuclear Power Plant	2008	Emergency Shutdown
Iran Bushehr Nuclear Power Plant	2010	Stopped for 2 years
Japan Monju Nuclear Power Plant	2014	Leaked Personal Information to Employees
Korea KHNP Hacking Accident	2014	Infected the 8 PC's, leaked Nuclear Power Plant Blueprint

Looking at the nuclear power plant cyber security cases in the United States two plants were halted. On January 2013, Davis-Besse nuclear power plant in Ohio was attacked by a Slammer worm and it penetrated private computer networks.[2] Another case occurred in 2008, where security surveillance systems of Hachi's nuclear plants were stopped for 5 hours and the power plants were not updated resulting in an emergency shutdown.

Japan's last suffered attack occurred on January 2014. In Fukui, Monju nuclear power plant was infected with malware. An infected computer operator performed video playback program updates. This attack was attempted more than 30 times and obtained the playback performed for 5 days. E-mails, training records from more than 42,000 employees. Also documents that were leaked were reported to have personal information.

Up till now, the worst nuclear power plant accident in Cyber security occurred in Iran in 2010. Due to malicious code, 1,000 centrifuges at Natanz uranium enrichment facility was destroyed, thus stopping the operation of the Bushehr nuclear power plant.

In case of Korea, a hacking incident occurred at the Institute for Agency for Defense Development(ADD) and Korea Hydro & Nuclear Power Co. Ltd.(KHNP).

ADD was reported to have confidential information leaked in April 2014. Leaked materials were relevant reports and data analysis. Also in December 2014, KHNP was exposed revealing the Korean nuclear plans and state secrets. In the process of hacking, the hacker stole nuclear power plant data and publicly disclosed the documents five times.

Also, sent mail was hacked including seven thousand documents infected with malware which was sent to KHNP staff to penetrate the nuclear power plant control network. The hack targeted PC hard disks and 8 personal computers were infected. As a result, five hard disks were formatted. Hackers made the command not to attack and destroy the system recovery.

Fortunately, even though the potential threat of these hacks was big, nuclear or radioactive leakage did not occur. However the threat is evolving further and it is increasing the psychological insecurity that people are feeling towards cyber terrorism.

3. The Emergency Accident Response Measure

Since the cyber attacks towards Iran, the possible threat of whether this can destroy real facilities or not has stirred much controversy.

The accident caused a physical blow to the national infrastructure program and nuclear physicist's for the first time were shocked and saw physical damage.

Hackers who attacked Iran have infiltrated a system for power generation through USB. Also weapons were Stuxnet virus called "Cyber Sniper".

Table II: Cyber Attack Cases

Nation	Year	Cyber Attack Cases Explains
US	1994	Roosevelt Dam exposed by a 12-year-old hacker who can adjust the Roosevelt management network control system
US	2000	Hacking of a wastewater treatment control system leaving one insider intrusion to the wireless network.
		Approximately 800,000 liters was discharged via unauthorized access from a total of 46 hacking attempts
Russia	2000	Gas pipeline control system was hacked
America	2003	CSX railroad that operates in the eastern United States was exposed by the Sobig. F virus. Where the transport control system was discontinued and operation ceased in the Southeast Amtrak and commuter trains in the Washington area.

KHNP took an emergency action after malware mail was received on December 9 last year.

For the first action, detected malware immediately results in the blocking of all incoming mail, full Internet e-mail messages, including an outgoing Blocked Sites. After requesting and analyzing malware, antivirus company servers and PC latest security updates for all employees took action, such as the full inspection.

Since the hacker distribution of data relating to nuclear power plants, KHNP shut down and blocked any providing external services. A change of the whole system ID/PW and virus scanning, log analysis, and cut off the network and the Internet network data transmission services and USB connection also were used a countermeasures. Also KHNP, strengthened and reinforced the urgency of cyber security monitoring system and block network of domestic and overseas offices.

In addition to technical advancements to security, other protective measures have been placed. Such as a contact zone of vulnerability checks ensuring the safety of the nuclear power plant control systems and confirming that it is impossible to connect the control system on the network services again. Also a dedicated organization was established to build a management system for information and technology. This organization was aimed to strengthen technical data, drawings, important asset classification, and rating systems security.

Thus KHNP is also scrambling to actively diagnose the level of data protection across the enterprise in order to fundamentally improve the security system, benchmarking information security system of leading companies.[3]

As such KHNP is intended to further strengthen the nuclear safety operations in the wake of the terrorist attacks and cyber upgrade the security system at the highest level. Originally hacking was merely just a skill and not so much a threat however, each country has hackers that are already in the war in the cyber dimension. The national aptitude of cyber warriors are used to realize political goals.

These days, nations are also facilitating and accelerating development of new cyber weapons like Gauss or Stuxnet to perform cyber war.

According to an EU report, it was said that there are a presence of 6 million botnets worldwide. If you mobilize these botnets, a spiral of cyber-attacks is expected to launch at one point and it could end in a catastrophe.

If one were to grasp this opportunity, at any moment the nature of cyber war may take place. The biggest weakness of a social network in the Internet is its network.

When any one of the networks is attacked, the entire network can fall like dominoes in a crisis. It is connected to network outlets and they are affected directly to ancestor according to one of the hub. Cyber war can destroy and create an instant major national infrastructure problem such as declaring war without a word grid, network, transport, financial networks, pipelines and gas lines, water and sewage. Some have come out to say that a cyber-war has the same or more magnitude of danger to that of a nuclear war.

Michael Hayden, former director of the US CIA said "There is no network connected to the Internet that is safe." Also, cyber-war has showed and warned it could happen anywhere, anytime without choosing a target.

If a hacker attacks the network and its operation is stopped and it can paralyze a country, leaving state secrets to be leaked and the harness of the national security will be threatened.

4. Conclusions

Recent malware distribution, such as website hacking threat is growing. In surveys today one of the most long-term posing security threats is from North Korea.

In particular, North Korea has been caught launching ongoing cyber-attacks after their latest nuclear test. South Korea has identified national trends regarding North Korean nuclear tests and analyzed them in order to catch disclosed confidential information.

Especially, many nuclear power plants in the world are found to be vulnerable to cyber-attacks.

Industrial facilities should be more wary of the risk of a serious cyber attack in the middle is going to increase the reliance on universal and commercial digital systems (off the shelf) software, civilian nuclear infrastructure.

Senior executives’ current risk rate levels are increasing. Digitalization of the perception of risk is lacking in nuclear power plants and workers are creating prevention methods to make them fully aware of the risks of cyber-attacks. It is suggested that it may be inappropriate to assume we are prepared for potential attacks.

Due to advances in technology, a warning that the growing sense of crisis about the cyber-attacks targeted APT(Advanced Persistent Threat) risk its own computer network or infrastructure which is heightened among government was pointed out that urgent protective measures laid one after another.

The South Korean government has enforced security by forcing public institutions to operate in a closed-network. But recent advice from the experts is that APT attacks are increasing both at home and abroad to evade large-scale infrastructure and there is a need for strong protective measures.

Especially with the possibility of cyber terrorism expanding, the Terrorism Act was enacted in order to protect from APT's. Also already in Russia and China, South Korea has cyber-attack prevention capabilities that are rated amongst the best in the world.

The United States has increased its focus in the cyber war by expanding training at the cost of reducing the defense budget, and each year about 4.5 trillion won is budgeted towards cyber war training.

In addition, Israel has been operating the most powerful cyber force, called 8200 troops. Korea also comes off in a 'defensive need, as well as hackers "aggressive hackers' cyber war against the positive pace with the times.

In the modern world, networks have created a tightly woven connection between everything and everyone. Between these connections lies the ability of countries to use cyber warriors. Between nations the cyber war has already started.

Now is the time required massive investment and human resources development at the national level.

REFERENCES

[1] http://egloos.zum.com/garisangod/v/11155585
[2] NRC Information Notice 2003-14, "Potential Vulnerability of Plant Computer Network to Worm Infection,' Nuclear Regulatory Commission, Mar., 2003.
[3] http://khnp.co.kr