Establishing an Information Security System related to Physical Protection

Sung Soon Jang [a *] and Hosik Yoo [a]
[a]*Korea Institute of Nuclear Non-proliferation and Control 573 Expo-Ro, Yuseong, Daejeon, Korea, 305-732*
[*]*Corresponding author: ssjang@kinac.re.kr*

1. Motivation

A physical protection system (PPS) [1] integrates people, procedures and equipment for the protection of assets or facilities against theft, sabotage or other malevolent attacks.

In the physical protection field, it is important the maintain confidentiality of PPS related information, such as the alarm system layout, detailed maps of buildings, and guard schedules.

In this abstract, we suggest establishing a methodology for an information security system. The first step in this methodology is to determine the information to protect and possible adversaries. Next, system designers should draw all possible paths to the information and arrange appropriate protection elements. Finally he/she should analyze and upgrade their information security system.

2. Protect what from whom?

In establishing an information security system, the first thing is to classify the information that needs to be protected. According to the IAEA technical guidelines, TECDOC-967 [1], confidential information includes information on the *design basis threat*, the specific targets to be protected, physical protection plans; site specific maps that represent the design features of a physical protection system, alarm system layouts, details of on-site and off-site security communications systems, *guard* procedures; schedules and itineraries for specific *transport* shipment, and response emergency plans. This information might be stored on an internet accessible computer or in printed materials.

Also, the capabilities of an adversary should be considered before making a security system. An adversary might have computer hacking skills and might have a collaborator inside the target facility. In the case of an insider threat, giving authorization to access secrets should be carefully thought out.

3. How to protect?

Security system designer draws path diagrams to the information and arranges appropriate protection elements. For example, firewalls and virtual private networks (VPN) are on-line information protection elements. A safe box, entry control system, and security guards are defined as off-line protection elements. The confidential information could be stored electronically, as hard copies, or both. Thus, there are several paths that an adversary could take in order to obtain vital information.

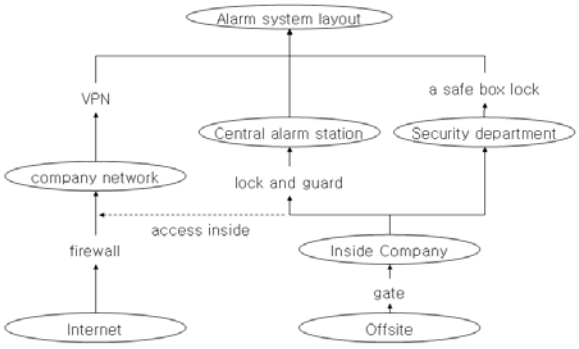

Fig. 1 Path Diagram of Adversary Intrusion

Figure 1 shows a path diagram to secret information with protection elements. In this figure, ellipses represent an area and words without borders stand for protection elements. The target is an alarm system layout which has three forms. The layout is on-line accessible through a virtual private network (VPN), which is only accessible from a company network with password and a specific USB token. Printed protection plans including the layout, are contained inside a safe box in the security department. It is also displayed in the main screen of the central alarm station (CAS), where guards perform their observations.

An adversary could choose three paths to the target, which is represented by arrows in Fig. 1. Through the internet, he/she can penetrate a firewall and a VPN. He/She also could go inside the company, passing the main gate and go to the key locked CAS where guards resident 24 hours a day. Alternately, after passing the gate he/she could go to security department and open a password locked safe box. Interestingly, after passing the gate he/she can access the company network by using a computer inside the company and attack VPN (on and off-line attack), which is shown as a dashed arrow in Fig. 1.

In the case of an insider threat, many of the protection elements could not work. Thus, the late protection elements (VPN, a locked safe box, locked CAS) are very critical.

4. How to measure protection effectiveness?

4.1 The effectiveness of protection elements

The effectiveness of protection elements can be measured by three factors: authentication, authorities,

	Low	Medium	High
Authentication	No features or weak password, simple lock	Strong password or complicate lock	Two-factor (key and password)
Authorization	Any employee	Permission to related groups	Graded permission according to trust level
Audit	No features	Required, analyze if incident occurs	Required, analyze periodically

Fig. 2 Relative Information Protection Effectiveness

and audits [2]. Authentication is the process of establishing the validity of a person's identity. The most frequently used authentication method is the password. Smart cards or tokens are used to strengthen the password use. An ID card is one of the authentication methods for off-line access. Authorization is the process of determining what actions a person is allowed to perform, depends on his/her working field and position. Auditing is the process of recording the actions or attempted actions performed by a person. For example, all on-line systems log security significant events, and the entry/exit log of the CAS is recorded. Also, lists are made of accesses to classified documents.

Based on these three functions we can determine the effectiveness of a protection element. Figure 2 shows the criteria to determine this effectiveness.

4.2 Measure of information protection effectiveness

For example, we investigated the on-line intrusion path of an adversary shown in Fig. 1. There are two protection elements, a firewall and a VPN. Figure 3 describes features for protection elements. According to the description, authentication for firewall is *Low*, authorization is *Low*, and audit is *Medium*. The overall effectiveness of firewall is *Low*, because it has weak authentication and a lack of authorization control. By a similar process, the protection effectiveness of the VPN is judged as *Medium*.

Effectiveness of the cyber intrusion path penetrating a firewall and a VPN is judged as *Medium*. We choose a higher value because where firewall fails, there is still the possibility that the VPN will be successful in defending the valuable information.

5. Conclusion

To protect information related to physical protection, we present a process for building an information security system. A security designer should determine the information to protect, predict possible adversaries, design an adversary's path to access the information, and arrange protection elements along those paths.

	Authentication	Authorization	Audit
Firewall	Restriction from outside access	Any employee	Yes, analyze if incident occurs
VPN	Smart card and password	Graded permission according to trust level	Yes, analyze if incident occurs

Fig. 3 Features of Protection Elements

	Authentication	Authorization	Audit	Overall
Firewall	L	L	M	L
VPN	H	H	M	M
Effectiveness of the path	M			

Fig. 4 The Results of Protection Effectiveness

Finally, a designer should assess every path and upgrade it according to the results. This information protection methodology will strengthen physical protection and nuclear security.

REFERENCES

[1] IAEA, INFCIRC/225/rev. 4 *The Physical Protection of Nuclear Material and Nuclear Facilities* (1999);
IAEA, TECDOC-967 (2000).
[2] Betty E. Bringer et. al., *Security Risk Assessment and Management*, John Wiley & Sons, Inc. (2007).