International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.225-230
http://dx.doi.org/10.14257/ijsia.2014.8.1.21

Study on Accurate Calculating the Risk of the SCADA

YoungIn You and KyuongHo lee

Korea University Graduate School of Information Security
(crenius, kevinlee)@korea.ac.kr

Abstract

Starting with the discovery of Stuxnet SCADA systems have been the target of cyber threats. Original SCADA system is operating in closed-independent structure is safe from outside attacks, but by the development of IT industry With the advent of the Internet as a connection point is always exposed to hacking threats. As a result, if cyber attacks occur in the SCADA system as a national major economic and social problems will occur. So in this study, Accurate and concise risk calculation propose. And this formula is can be that indicator of new system's efficiency

Keywords: *SCADA; RISK; Security; Solution*

1. Introduction

SCADA system was essentially complete closed network. However, for ease of connection with other networks began as a problem has occurred. The following is a diagram of the power IT. These environments are vulnerable to hacking and viruses. Mentioned earlier, the openness and scalability of the network is cause.

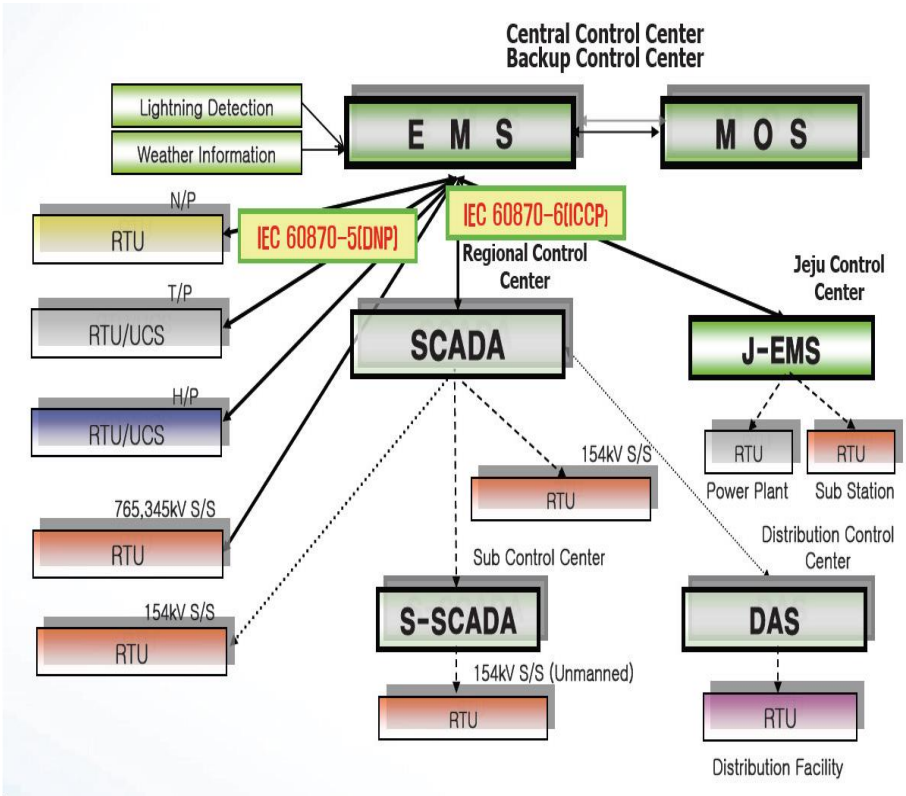

Figure 1. Diagram of the Power IT

ISSN: 1738-9976 IJSIA

Therefore, risk management for SCADA systems is required. In this study, SCADA system with the characteristics of the threat to the existence of substantial consideration to derive quantitative models for risk is proposed. IT and SCADA system there are many differences. So also different vulnerabilities and threats. Therefore redefinition of security priority is needed. Has been a lot of research on this topic. This considers the probability that the defense applied to the security system based on the unemployment risk is to calculate the value. Calculation of the first to define general security risk. Next, defense in the event of a security incident considering the probability and the value of each weight is defined. And using these values to calculate the final risk value to evaluate.

2. Main Discourse

First output introduces security risks. Second caculating threat value considering the chracteristic of SCADA system. Finally, the risk calculations are derived.

2.1. Security Risk Calculation

Security threats Vulnerability, Threat, Asset of the three components is determined by. Threats, vulnerabilities, assets are combined definition of risk is practically possible. Vulnerability, Threat, Asset, respectively, V, T, A, as indicated by the following formulation can be.

$$R = T * V * A$$

However, the characteristics of each sector of companies and organizations that are important when considering the security of the property will be different. Defined vulnerability to the threat does not exist, or if the vulnerability exists does not exist as a threat. In this study, we consider the characteristics of each system against the threats that exist on the importance weights and the security system used to calculate the risk is considered.

2.2. Defense against Security Attacks Calculated Risk with Probability

The primary goal of the general information security, confidentiality, integrity, and availability is defined as the net. However, in the case of energy availability, integrity, confidentiality, in order of importance is the re-definition. Considering the characteristics for the risk weighting in the calculation will be calculated. An attack on the existing IT system, as shown in Table 1 of the three part SCADA system (SCADA server, communications network, RTU and terminal equipment) can be classified as.

Assorted types of attacks that do not apply to the SCADA System is also the threat items are painted in the Table below. Back three categories (Confidentiality, Integrity, Availability) are classified as. And the threats to secure control of the system completely if (Availability) partial control or data that can be changed if (Integrity), but if possible, get information (Confidentiality) considered to be weighted. Availability attack has the highest degree of difficulty. However, when the gain control SCADA system to attack the most dangerous, because the nature of the weight was 0.6. Otherwise, seized control of the part you want, or that interfere with the operation if the weight was 0.3. Finally, in the event of information disclosure has a weight of 0.1.

The more you have the appropriate type of attack is a powerful attack. So SCADA system configuration that corresponds to the ratio of the proportion depending on the type of attack was given.

Table 1. System Components by Cyber Threats, Vulnerabilities, Weight and Component Ratio

System Configuration / Kinds of threats		SCADA server	network		RTU and End point machine	Weight	C.R
			TCP/IP	Serial			
Confidentiality	Eavesdropping	V(01,01)	V(01,02)	V(01,03)	V(01,04)	x0.1	0.0166x4
	Traffic Analysis	V(02,01)	V(02,02)	V(02,03)	V(02,04)		0.0166x2
	EM/RF Interception	V(03,01)	V(03,02)	V(03,03)	V(03,04)		0.0166x1
	Indiscretions by Personnel	V(04,01)	V(04,02)	V(04,03)	V(04,04)		0.0166x1
	Media Scavenging	V(05,01)	V(05,02)	V(05,03)	V(05,04)		0.0166x1
Availability	Trojan Horse	V(06,01)	V(06,02)	V(06,03)	V(06,04)	x0.6	0.0166x2
	Trapdoor (Backdoor)	V(07,01)	V(07,02)	V(07,03)	V(07,04)		0.0166x2
	Service Spoofing	V(08,01)	V(08,02)	V(08,03)	V(08,04)		0.0166x2
	Denial of Service	V(09,01)	V(09,02)	V(09,03)	V(09,04)		0.0166x2
Integrity	Masquerade	V(10,01)	V(10,02)	V(10,03)	V(10,04)	x0.3	0.0166x1
	Bypassing Controls	V(11,01)	V(11,02)	V(11,03)	V(11,04)		0.0166x1
	Authorization Violations	V(12,01)	V(12,02)	V(12,03)	V(12,04)		0.0166x2
	Physical Intrusion	V(13,01)	V(13,02)	V(13,03)	V(13,04)		0.0166x4
	Replay	V(14,01)	V(14,02)	V(14,03)	V(14,04)		0.0166x1
	Theft & Illegitimate Use	V(15,01)	V(15,02)	V(15,03)	V(15,04)		0.0166x1
Total						1	0.45(/1)

Applied security system not be able to prevent security attacks that occur Let's take a look at the probability. In order to calculate the following two definitions of the variables are required.

E_s : 's' security system to safeguard the security target event

E_a : 'a' security attack incidents occur

The applied security system not be able to prevent security attacks that occur odds are as follows:

$$\mathrm{P}(E_s) = \sum_{a \in A} P(E_s|E_a) \times P(E_a)$$

$P(E_a)$ is attacked a security represents the probability, $P(E_s|E_a)$ is a security attack happened when the security system, s is the probability of fail on defense. Where the probability $P(E_a)$ with the following results can be derived.

$$P(E_a) = P_1 \times \text{C.R(composite ratio)}$$

P_1: 15 kinds of security attacks, the probability of one year of experience

Cyber security of SCADA systems and related statistical data so that this does not exist there, and even if the public is difficult. Furthermore, the closed network SCADA system has been maintained for quite a long time. So, in this study, assume that there is no real data. Thus, the configuration is applied to the ratio of the SCADA system to estimate the number of risk factors P_1 value was assumed to be 10%. For example, to calculate the

probability of occurrence of Eavesdropping is as follows.

$$P(E_{\text{Denial of Service}}) = 0.1 \times 0.0332 = 0.00332$$

As above, calculating the value for each item. In order to calculate $P(E_s)$, the probability of defense is needed. Table2 is an example of the probability of defense.

Table 2. Example of the Probability of Defense

Security Technology / Security Attacks	IDS	Firewall	Vaccine
Virus and worm infections	0	0	0.9
Denial of Service	0	0.8	0

When the Firewall is installed on the system to defend against Denial of Service attacks, let's look at the probability of failure.

$$P(E_s) = 0.1 \times 0.0332 \times (1\text{-}0.8) = 0.000664$$

The value of the above seems quite small. However, the absolute value is not important. Because it is for comparison between the effect of the security system.

In conclusion, considering the weight final formula are as follows:

$$T * V = \sum_{s \in S} P(E_s) = \sum_{s \in S} \sum_{a \in A} P(E_s | E_a) \times P(E_a) \times W_a$$

This formula is designed for SCADA system characteristics. And this formula is can be that indicator of new security system's efficiency.

3. Conclusion

In this study, we use the threat of a SCADA system on the basis of the security system was applied to the variable. This formula is designed for system characteristics. Thus, the risk more accurately identify and briefly can be calculated. The study of the relationship between SCADA systems and security systems and is working to quantify. In this study, up to now failed to apply the value of the statistic, the variable was unified. In the formula field, but using the exact figures will be able to find a reliable value. This study future attacks on the security of SCADA system, the expected loss calculated in accordance with the new security system installed in effect is the basis of a formula that can calculate. Finally, according to the SCADA system security investments return on investment (ROI) of it will be calculated by the formula. The development of a new security system is also important. However, the quantification of the return on investment for this work is considered to be very important.

References

[1] Study on power applied for improving IT security study **(2012)** June.
[2] S.-W. Seo, Pf of Seoul national University, The economics of information security **(2012)** April.

Authors

YoungIn You, is now a Master Course in Graduate School of Information Management and Security at Korea University since 2013.

Kyoungho Lee, received his Ph.D. degree from Korea University. He is now a Professor in Graduate School of Information Management and Security at Korea University, and leading the Risk management Laboratory in Korea University since 2012. He has a high level of theoretical principles as well as on-site experience. He was a former CISO in NHN corporation, and now he takes as the CEO of SecuBase corporation. His research interests include information security management system(ISMS), risk management, information security consulting, privacy policy, and privacy impact assessment(PIA).