Legal Protection of Cyberspace Infrastructure and Information Safety in China -- A Response to Cyberspace Challenges to China's National Security

Hongyu Fu[1,a]

[1]Beijing Foreign Studies University School of Law, Beijing, China

[a]fhymars@163.com

Keywords: Network information security; insurance; strategy; risk

Abstract. In recent years, with the standardization of key infrastructure control system, intelligent, network development, the network attacks against the critical infrastructure is increasing. Electricity, petrochemical, rail transportation and other key infrastructure involving the national economy and the people's livelihood, once attacked, it is likely to have disastrous consequences. The key infrastructure information security has become the sword hanging in the heads of governments, taking measures to strengthen its information security capabilities is imperative. In this paper, we first introduce the critical infrastructure of the basic concepts and critical infrastructure applications typical industrial control system, analyzes the characteristics of critical infrastructure information security incidents, elaborated the industrial control system is facing the challenges of information security, and aimed at the challenge put forward corresponding measures and suggestions.

1. Introduction

With the continuous advance of information technology, network information security problems began to spread, according to statistics, the global average for each additional seconds once online intrusion event, at least a week nearly 80% of the company to be a large-scale invasion on the Internet [1]. America Federal Bureau of investigation report shows, the crime of computer security America every year there are about 75% the loss of the company. At present, small and medium enterprises European countries each year due to computer virus causes economic losses of up to 22 billion euros. Even at the height of the development of information security technology and American Europe, can not avoid the information security problem of economic losses caused by these data, let us feel the information technology products to the security threats extremely weak [2].

All kinds of information security technology and management methods have got extensive development and application, the security technology commonly used firewall technology, encryption technology, anti-virus technology, intrusion detection technology, VPN technology, network isolation technology and so on [3, 4]. Although the information security technology to a certain extent, a certain scope to solve the security problem, however security is a process of dynamic change, along with the continuous upgrading of information security threats, information security issues and relatively more and more difficult to eradicate, using technology to solve the problem of information security is not enough, can not really achieve the purpose of safety, even if these security techniques temporarily solved the problem, but the loss caused by the enterprises or individuals has been irreparable. At the same time the enterprise security problem has also weakened, unable to return to the previous operating state [5].

Network information security is affecting national security, social stability, economic development and people's lives. The development of network information technology, to the field of world politics, economy, military, science and technology, culture and social life brought profound changes and permeability of network openness, the spread of interactivity and technology affects people learn, work, all aspects of life. The economic and social development of the state is increasingly dependent on the network information. But at the same time, network attack, the spread of the virus, network crime, adverse information flooding and other serious threat to network information security; and domestic and foreign anti china forces utilizing the network to incite propaganda, intelligence surveillance and attack technology and other activities, a serious threat to the network information security in our country. The protection of the network information security is essential to China.. Therefore, the construction of network information security system based on the protection of legislation has become the consensus of the world.

2. Key infrastructure challenges of information security

2.1 Typical control system for key infrastructure

a. Monitoring and data acquisition system

SCADA system is used for data acquisition and control, and centralized management for the assets and equipments of large distance geographic distribution.. SCADA system is integrated with the data acquisition system, data transmission system and human-machine interface, in order to provide a centralized monitoring system for multiple process inputs and outputs.. The SCADA system is the wide area network size control system, which is commonly used in the process control of the electric power and oil pipeline.

b. Distributed control system

DCS is centralized LAN mode of production control system, through the control of the controller, so that they can work together to complete the entire production process; the modularization of production system, reduce the single point of failure of the whole system influence. DCS is mainly used for the decentralized control of various large, medium and small power stations, the transformation of power plant automation system and the process control industry such as iron, petrochemical, paper, cement and so on.

c. Programmable logic controller

PLC is a solid state equipment with the ability of computing, and has the function of independent, calculation, analysis and control of industrial equipment and industrial process.. PLC can also be directly used as a small scale control system for the production process control, as the entire system of the SCADA and DCS system as a whole system for local management. In the SCADA system, PLC can play a role in DCS, and in the RTU system, the function of PLC is local controller..

2.2 Data statistics and analysis

According to the site investigation, the questionnaire and interview, combined with the Ministry of public security in recent years to carry out the status of network security and computer virus outbreak investigation results, this paper on the requirements of the network security of enterprise, departments and insurance companies of the survey data were analyzed, statistics, sorting and summarized. Specifically as follows:

Table 1.The incidence of network security events

Year	2004	2005	2006	2007	2008
Event rate	58%	49%	54%	65.7%	62.7%
Occurred over three times	23%	15%	22%	33%	50%

From the perspective of the overall trend, although in recent years in our country, the problem of network security more and more attention, attention, and to take the measures to guard against the risk, network security technology continues to improve, constantly updated product safety, but the network information security incidents of an annual incidence on the rise, are becoming more and more serious. Network security interface and composition was shown in Figure 1.

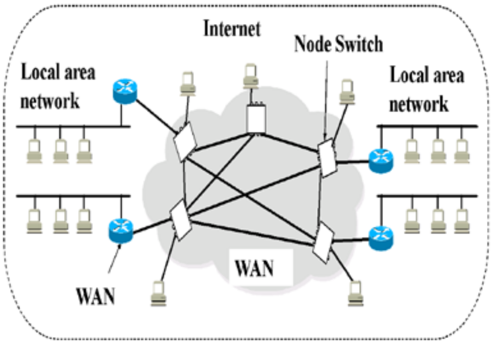

Fig. 1. Network security interface and composition was shown in

3. Experimental Results

3.1 Random access technology

In the early 1970s, the University of Hawaii for the first time successfully tested random access. This is to allow geographically dispersed users to use a central computer via radio. Since the radio channel is a common channel, a station can transmit the information received by a plurality of stations, each station is sent at random, so this system is a random access system. Early development of the University of Hawaii system called ALOHA, is Additive Link On-line system of abbreviations and Hawaii ALOHA just another dialect, Figure 2 represents an ALOHA system works.

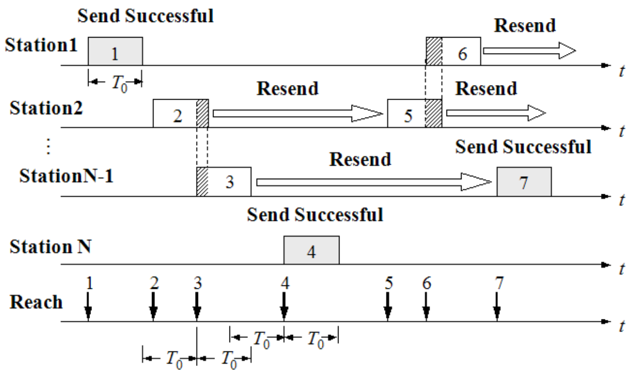

Fig. 2. Pure ALOHA system works.

When the network system reaches a steady state, at time T0, the average number of frames reach the network should be equal to the throughput S.

$$\mathrm{P[t]} = \frac{(2G)^k}{k!} \mathrm{e}^{-2G}, k = 0, 1, 2... \tag{1}$$

In the above formula, 2G in 2T0 mean arrival time frames. Then S = G ·P[t] = G ·P[2T0]

$$= G \frac{(2G)^0}{0!} \mathrm{e}^{-2G} \tag{2}$$

At this time, the network load reaches a great value. Continuously transmit data frames, collision, retransmission, but there is no useful output. Seen in pure ALOHA system, the network load G must not exceed 0.5.

$$D / T_0 = 1.5 + R + N_R [R + 0.5 + (K + 1)/2]] \tag{3}$$

As each station sends frames are independent:

$$S_j = G_j \prod_{\substack{i=1 \\ i \neq j}}^{N} (1 - G_i) \tag{4}$$

This is a limited number of stations ALOHA system throughput formula. Using the formula:

$$S = \lim_{N \to \infty} G(1 - G / N)^{N-1} = Ge^{-G} \tag{5}$$

Right (5) type S obtained when G = 1 time, S up to maximum value:

$$S_{\max} = (1 - 1/N)^{N-1} \tag{6}$$

3.2 Network security product defense function

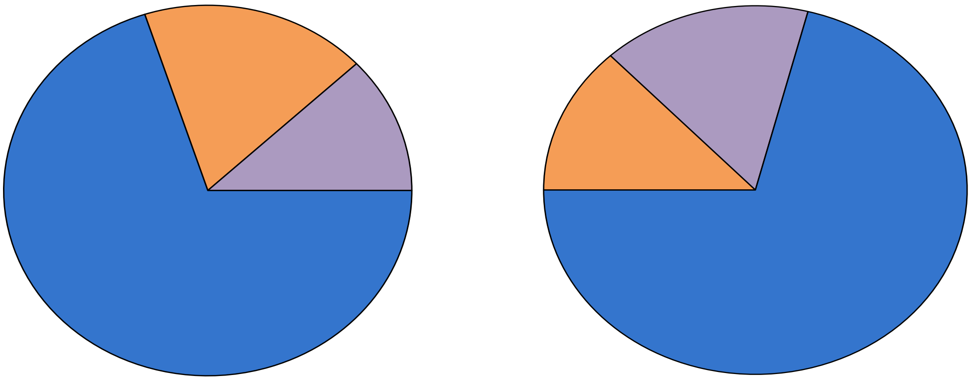

Fig. 3. Beforehand defense and post remedial function

Most believe that the network security products have a certain effect on the security, but the effect is not very satisfactory, but also can not completely solve the problem, the economic development of the enterprise or caused the loss. Beforehand defense and post remedial function was shown in Figure 3.

4. Summary

Operators of critical infrastructure units should strengthen management, mainly include: disconnect and public network between all unnecessary connection, connection of real need, to take the necessary protective measures, and risk assessment on a regular basis; strict control in the industrial control system and the public network between the cross use of mobile storage medium and portable computer; establish control server and other industrial control system key equipment configuration and security audit system, strict account and password management regularly to account, password, port, and service were checks and other measures.

References

[1] M Jachan,G Matz and F Hlawatsch. Vector Time-Frequency AR Models for Nonstationary Multivariate Random Processes[J], IEEE TRANSACTIONS ON SIGNAL PROCESSING, 2009, 57(12): 4646-4658.

[2] Xinyu Ma,C L Nikias. Parameter estimation and blind channel identification in impulsive signal environments [J]. IEEE Transactions on Signal Processing, 1995 ,43 (12) :2884 - 2897.

[3] M.shao.C.L.Nikias.singnal processing with fractional lower order moments instable processed and their applications[J].proceedings of the IEEE. 81(7):986-1010 1993.

[4] T.H Liu, J. M Mendel, A Subspace-Based Direction Finding Algorithm Using Fractional Lower Order Statistics[J], IEEE TRANSACTIONS ON SIGNAL PROCESSING, 2001, 49(8): 1605-1613.

[5] E N Kuruoglu. Signal Processing in α Stable Noise Environment: A Least lp-Norm Approach[D], Britai: Signal Processing and Communication Laboratory, Department of Engineering, University of Cambridge, 1998.