Information Assurance Evaluation for Network Information Systems

Xin Lü[1] and Zhi Ma[2]

[1] State Information Center, No. 58 Sanlihe Road, Beijing, 100045, China
lux@cei.gov.cn
[2] Department of Information Research, PLA Information Engineering University, Zhengzhou, 450002, China
muzinihao@hotmail.com

Abstract. In both the public and private sectors, organizations have become significantly depend over on the proper functioning of information systems. As security spending continues to rise, organizations contend that metrics initiatives will become critical to managing and understanding the impact of information security programs. This paper reviews information assurance (IA) conceptions from viewpoint of system science and analyses the construction of IA systems. An IA evaluation model is addressed in this paper, which is depicted by IA capability index, IA countermeasure index and IA cost index. This evaluation model can be used for organizations to assess their IA strategies and analyzes their security state.

1 Introduction

Rapidly advancing information-based technologies and increasingly competitive global environment have drive information into the center stage in society, government now. Information becomes the important national and organizational resource, which has natural and social properties independent of matter and energy. The most popular definition of information is a message or communication. However, a message is not information because the same message can contain information for one person and no information for another person. In 1928, Hartley defined information as the eliminated uncertainty [1]. Information can also be defined as the eliminated uncertainty or reflected variety [2]. These definitions are based on Shannon's information theory, which represents a statistical approach to information. Warren Weaver gave the three levels of problems in communication, which can be described as the technical problem, the semantic problem and the effectiveness problem. The technical problem cares about the accuracy that the symbols of communication be transmitted. The semantic problem cares about the precise that the transmitted symbols convey the desired meaning. The effectiveness concerns the pragmatics and the use or function of language. The broad research object of information science is the information acquisition, information transformation, information processing, information decision and information effectiveness.

Y. Wang, Y. Cheung, and H. Liu (Eds.): CIS 2006, LNAI 4456, pp. 869–877, 2007.

Information security is one of the cornerstones of the Information Society. Confidentiality within a virtual enterprise, integrity of financial transactions, authenticity for electronic signatures, privacy of personal information, reliability of critical infrastructure, all depend on the availability of trustworthy security mechanisms. In a popular view, information security has experienced communication security phase (COMSEC), information security phase (INFOSEC) and information Assurance phase (IA) [3,6,7,8,9]. Information assurance is about protecting information assets from destruction, degradation, manipulation and exploitation by an opponent. DOD perspective, JP 3-13 provides a widely accepted definition of IA. IA protects and defends information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation [10,11]. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IA employs technologies and processes such as multilevel security, access controls, secure network servers, and intrusion detection software. IA's Goals and Objectives are to minimize the probability of information assurance vulnerability, to minimize the damage if vulnerability is exploited and to provide methods to recover efficiently and effectively from the damage.

More important, security evaluation provide a mechanism for information systems security management and feed a process toward continuous security improvement. In section 2, we define IA model based on system science methodologies and describe the key security services, IA risks and IA countermeasures. Section 3 propose an IA evaluation model and metrics indices. Conclusions are made in section 4.

2 IA Model and IA Systems

2.1 IA Model

Information security theoretical models have been intensively studied in the last thirty years. The Bell-LaPadula Model (BLM), also called the multi-level model, was addressed by Bell and LaPadula, is one of the fundamental models of computer security, which was designed for enforcing access control in government and

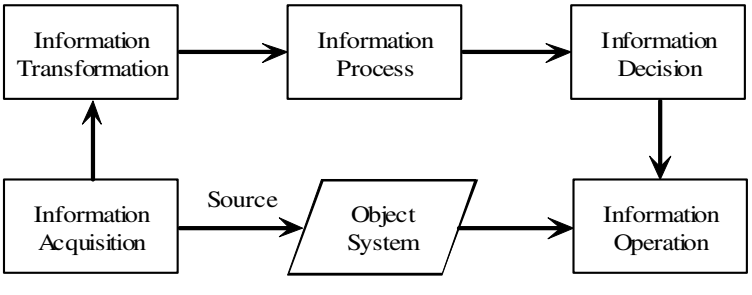

Fig. 1. Information flow in an information system

military applications [4]. In this model, subjects and objects are often partitioned into different security levels. A subject can only access objects at certain levels determined by his security level. David *et al*. proposed a very interesting and intriguing commercial security model, the Chinese Wall model [5], and showed that it couldn't be correctly represented by a Bell-LaPadula model. McCumber presented an INFOSEC model, also known as McCumber Cube model, which is always used as a structured methodology to assessing and managing security risk in IT systems [6,7]. However, McCumber Cube model is not enough to be used as an IA model because it concerns only about the states and security characters of "information". In IA model, both information and information system are the protected objects.

The word "system" is used to describe any "experience-cluster" that we can map as a set of interacting elements over time. Information system includes the entire infrastructure, personnel, organization, and components that collect, store, transmit, disseminate, and act on information. Typically a system is mapped by identifying the pathways of information flow, as well as possibly the flow of energy, matter and other variables. The information flow of an information system can be depicted as Fig.1.

In this paper, an IA system is defined as a system to provide security technology, security management and personnel to protect information and information system from destruction by all kinds of threat, such as natural threat, intentional threat and unintentional threat (see Fig.2.).

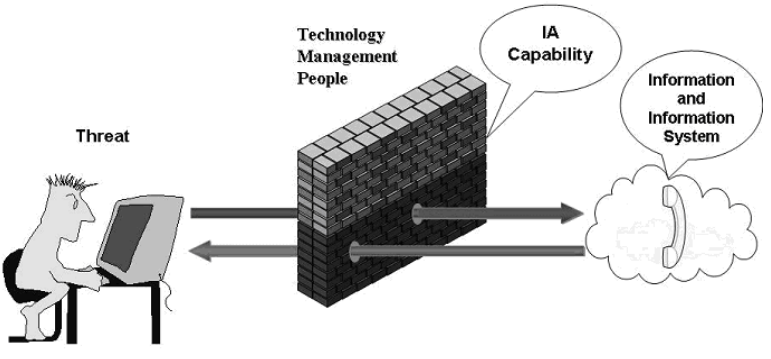

Fig. 2. IA systems

2.2 The Security Services for Information and Information System

The main object of an IA system is to provide five security services for information and information system: confidentiality, integrity, availability, authenticity and non-repudiation.

Confidentiality ensures that information is not available or disclosed to unauthorized individuals, entities, or processes.

Integrity means that data has not been altered or destroyed in an unauthorized manner.

Availability means that the information and information systems can always be timely and reliable accessible by authorized entities. Availability is regarded as a function, which is not entirely security.

Confidentiality, integrity, availability are the basic security service for an information system, which are also know as CIA model.

Authenticity indicates the corroboration that the source of data received is as claimed.

Non-repudiation requires the recipient of data to provide proof of the origin of data.

2.3 IA Risk

As is well known, information security risk of computer systems is tied to two factors: internal vulnerabilities and external threats. The internal vulnerabilities are flaws or weakness that expose the system to harm. The external threat is a intentional or unintentional event, which could destroy the system by employ one or more vulnerabilities.

2.3.1 Vulnerabilities

Vulnerability is defined as the degree to which a software system or component is open to unauthorized access, change, or disclosure of information and is susceptible to interference or disruption of system services. Fig.3 illustrates the increasing trend in Vulnerability reported by the Computer Emergency Response Team Coordination Center (CERT/CC).

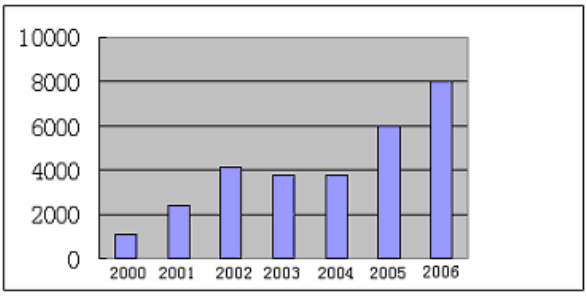

Fig. 3. Vulnerabilities reported from 2000 to 2006 by CERT/CC

2.3.2 Threat

In the context of information assurance, a threat to a system can be defined as: “a circumstance or event that has the potential to cause harm by violating

security of an information system". There are several types of threat in the information world includes: the insider, the hacker, the criminal, industrial or economic espionage and the terrorists.

Recently, botnet, social engineering, phishing and Zero-day are new rising type of attacks which challenge the network protection policies and the traditional information security products.

Botnet attacks take advantage of programs that secretly install themselves on thousands of personal computers and use them to commit Internet crimes.

For a social engineering attack, an attacker uses human interaction to obtain or compromise information about organizations or their computer systems. The attackers may claim to be a new employee, repair person, or researcher and even offering credentials to support that identity.

Phishing is a form of social engineering, which is a technique used to gain personal information for purposes of identity theft and seeking financial benefits. Symantec detected 157,477 unique phishing messages in the first half of 2006, up 81 from the last six months of 2005. Home PCs were targets of 86 of security threats in the first six months of 2006, according to the Symantec report.

Zero-day attack can be defined as a virus or other exploit that takes advantage of a newly discovered hole in certain program or operating system before the software developer has made a fix available, or before they are even aware the hole exists.

2.4 IA Countermeasures

(1) Technique
Technology, in a security context now includes access control, identification and authentication,crypto systems, , system and communication protection audit and accountability, physical and environment protection, security protocols etc.

(2) Management
IA management is the process of achieving objectives using a given set of security resources. IA management includes risk assessment, planning, system and services acquisition, certification, accreditation, maintenance, policy, standards, law, procedures and so on.

(3) People
People are the most critical link in the information assurance program. This aspect of IA includes security personnel and the security of personnel. People require security awareness, education and training when designing, using, managing the information systems. IA awareness is very important in the IA process due to that most of attacks and incidents, according to FBI, are form the internal of the organizations. IA training and education is also the fundamental to development IA technology in companies and construct complete IA management systems.

3 Evaluation of IA Systems

3.1 IA Evaluation Indicator Systems

The proposed IA evaluation model includes IA capability index, IA countermeasure index and IA cost index , which is described in Fig.4.

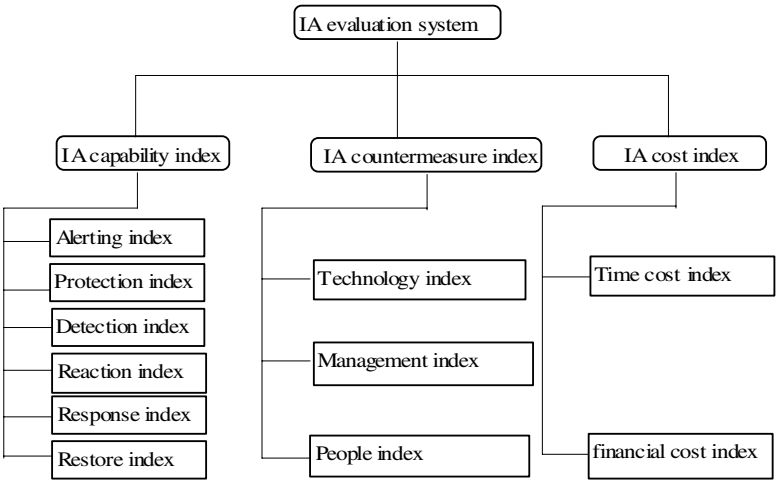

Fig. 4. IA evaluation indicator systems

3.1.1 IA Capabilities Index

In many professionals' views, information assurance can be regarded as one complete system or a process. The Alerting-Protection-Detection-Response-Restore-Counterattack (APDRRC) capability model is a true system, which is a holistic approach to deal with IA problems.

(1) Alerting, noted as *al*, means that preventing an accident or eradicating an attack before they comes. Security warning procedure and alerting organization, such as US-CERT and CN-CERT, should be established. These organizations alert users to potential threats to the security of their systems and provide timely messages about how to avoid, minimize, or recover from the damage.
(2) Protection, noted as *pr*, deals with the issues of ensuring the confidentiality, integrity, availability, authenticity and non-repudiation of information and the survivability, reliability of information systems from destruction and intrusion.
(3) Detection. Timely and exactly detection of the existence of attacker and incidents is the key to initiating restoration and attacker response. Regardless of the type of attack, the earlier an intrusion is detected, the quicker a appropriate response can be initiated. Detection can be noted as *de*.

(4) Reaction. The first task of organization, when attack is detected, is to stop the attack and to mitigate the risk to a low and accepted level. The second task is to collect evidence to facilitate legal action. The third task is to set up formal reporting procedure. Security incidents should be reported through appropriate channel as quickly as possible.Reaction can be noted as rea.
(5) Restoration. The objective of an effective reaction is to restore the availability, confidentiality, and integrity etc. of information and information systems to their original or accepted state. It requires backup strategy based on its ability to meet the organization's needs in terms of time required to restore the data and return the information system to an operational state. Restoration can be noted as res.
(6) Counterattack, by attacking the peacebreaker's system or take the legal steps to hold the peacebreaker accountable, is part of IA in some cases. Counterattack can be noted as ct.

3.1.2 IA Countermeasure Index

The IA countermeasure can be obtained from IA technology index, IA management index and IA people index.

3.1.3 IA Cost Index

In the process to build IA system, cost must be taken into account because almost all the organizations aim at obtaining the greatest return on investment. In this research, IA costs can be classified into three categories: time cost, personal cost and financial cost.

3.2 IA Evaluation Model

Following the general system theory used in Bell-La-Padula security model [12], we regard IA capability as IA, IA cost as CST, IA countermeasures as C and note time as T. Thus the state of an information system's IA state can be written as

$$y = (IA, CST, C, T) \in Y \tag{1}$$

where, $IA \in (al, pr, de, rea, res, ct)$ represents IA capabilities for certain information system, al, pr, de, rea, res, ct denote the capability of alerting, protect, detection, response, restore and counterattack respectively. $CST \in (tc, wc, fc)$ represents IA cost, which includes time cost, personal workforce and financial cost for IA system. $C \in (t, m, p)$ represents IA countermeasures, t, m, p denote technology countermeasures, management countermeasures and people countermeasures respectively.

A system's IA baseline describes the basic requirements for IA capabilities, IA cost and IA countermeasures (see Fig.5), and the baseline equation can be written as

$$f_B = F(IA_B, CST_B, C_B) \tag{2}$$

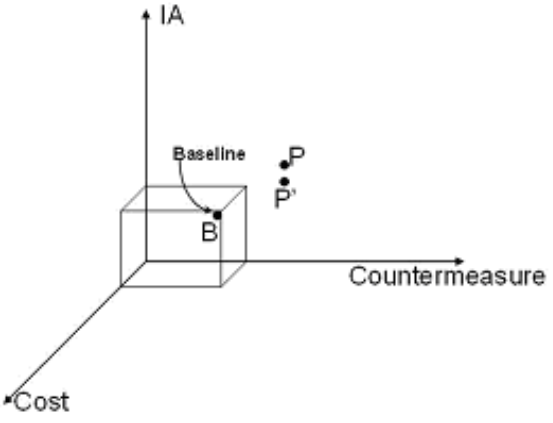

Fig. 5. IA evaluation indicator systems

When a system's IA state is P, which satisfies $f_P \geq f_B$, we say that the system satisfies the baseline requirements. Otherwise, the system does not meet the basic security requirements. For IA strategies P and P' within the same information system, if $IA_P = IA_{P'}$, $C_P = C_{P'}$ and $CST_P < CST_{P'}$, then we say that the IA strategies of P is better than the IA strategies of P'.

4 Conclusions

Along with the rapid breakthrough of information applications and the increase of information sharing, the problem of information security has become a main issue of the whole society. Theoretical model for information assurance is studied in this paper, which can be used in information security policy design for organizations. This paper proposed an IA evaluation model which is described by IA capability index, IA countermeasure index and IA cost index. This evaluation model can be used for an organization to devise IA plan and assessment the IA strategies of its information systems.

Acknowledgments. This work was supported by the Postdoctoral Science Foundation of China under Grant No.20060400048 and the Natural Science Foundation of China under Grant No.60403004.

References

1. Hartley R.V.L.: Transmission of Information. In: Bell System Techn. vol. 1928(3) 535–563
2. Shannon, C.E.: Mathematical Theory of CommunicationBSTJ1948
3. British Standards Institute, Code of practice for information security management, BS 7799, London (1999)

4. Bell, D., Padula, L.: Security Computing Systems: Mathematical Foundation and Model. MITRE Report, Bedbord, MA (1975)
5. David, F.C.B., Michael, N.: The Chinese Wall Security Policy. In: IEEE Symposium on Research in Security and Privacy, pp. 206–214 (1989)
6. McCumber, J.: Information Systems Security: A Comprehensive Model. In: Proceedings 14th National Computer Security Conference. National Institute of Standards and Technology. Baltimore, MD (October 1991)
7. Maconachy, W.V., Schou, C.D., Ragsdale, D., Welch, D.: A Model for Information Assurance: An Integrated Approach. In: Proceedings of the, IEEE Workshop on Information Assurance and Security United States Military Academy, 2001, pp. 306–310 (2001)
8. ITU X.800. Security Architecture for Open Systems Interconnection for CCITT Applications (1991)
9. National Security Agency. National Information Systems Security Glossary. NSTISSI 4009 Fort Meade, MD (Septemper 2000)
10. Information Assurance Technical Framework, National Security Agency Information Assurance Solutions Technical Directors (September 2002)
11. Zhao, Z.S.: Lectures on Information Assurance. State Key Lab of Information Security, Chinese Academy of Sciences (In Chinese) (2005)
12. Chen, X., Zheng, Q., Guan, X. et al.: Multiple behavior information fusion based quantitative threat evaluation. Computers and Security 24, 218–231 (2005)