Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 30 (2008) 1 – 7
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

A study on e-Taiwan information system security classification and implementation

Kwo-Jean Farn *, Shu-Kuo Lin, Chi-Chun Lo

Institute of Information Management, National Chiao-Tung University, No. 1001, Ta Hsueh Road, Hsinchu 300, Taiwan, ROC

Received 13 September 2005; received in revised form 5 February 2007; accepted 2 July 2007
Available online 20 September 2007

Abstract

Information systems of Cyberspace offer attractive targets. They should be resistant to such as Active Attack, Passive Attack, Insider Attack, Close-in Attack, and Distribution Attack from the full range of threat-agents – from hackers to nation states – and they must limit damage and recover rapidly when attacks do occur.

According to Common Criteria (CC), Information Security Management System (ISMS) and the international standards of Information System Security (ISO/IEC 15408, ISO/IEC 17799, and ISO/IEC TR 19791) as well as the other international standards and guidelines such as the framework of Defense-in-Depth promoted by the U.S., in this paper we propose a new framework of information system security classification for e-Taiwan to reach the vision "information and communication network resources can be fully used in an obstacle free and secure environment by year 2008."

Keywords: Cyberspace; Defense-in-Depth; Information Assurance; Corporate governance; Organized attack

1. Introduction

The popularity of information technology overwhelms the whole world. This brand new technology leads human lives to the cyberspace of knowledge-based economy. The application of information technology causes tremendous changes to the working ways, living environment and even the concepts of human beings. Besides, it promotes the development of human society and the advancement of world civilization, which brings people into a new era. However, people also face the severe test when they enjoy the great benefits that cyberspace brings.

Information systems of Cyberspace offer attractive targets. They should be resistant to attack (show as Table 1.1) from the full range of threat-agents – from hackers to nation states – and they must limit damage and recover rapidly when attacks do occur.

Based on Common Criteria (CC) and the international standards of information security management (ISO/IEC 15408, ISO/IEC 17799, ISO/IEC TR 19791) as well as the other international standards and guidelines (i.e., Information assurance Technical Framework, etc.) [1–3], in this paper we propose the concept of implementation strategies for how to protect and strengthen the information system from organized attack in order to form the foundation of the classification and implementation framework targets of information system security in cyberspace.

Since the U.S. officially announced reliable computer system security evaluation criterion in 1985 (hereafter referred to as Orange-Book), it only considers that the traditional single computer is independent of the operation environment. With the upturn of information technology, the issues of information security have already started afresh. Using the scheme of Information Assurance (IA) Degree of Robustness, which was integrated with Strength Mechanism Level (SML) and Evaluation Assurance Level (EAL), is the new solution [3]. In light of

* Corresponding author. Tel.: +886 3 5712301; fax: +886 3 5723792.
E-mail address: kuo@iim.nctu.edu.tw (K.-J. Farn).

0920-5489/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2007.07.001

Table 1.1
Classes of attack [3]

Attack	Description
Passive	Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information (e.g., passwords). Passive intercept of network operations can give adversaries indications and warnings of impending actions. Passive attacks can result in the disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.
Active	Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These include attacks mounted against a network backbone, exploitation of information in transit, electronic penetrations into an enclave, or attacks on an authorized remote user when attempting to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.
Close-in	Close-in attack is where an unauthorized individual is in physical close proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close proximity is achieved through surreptitious entry, open access, or both.
Insider	Insider attacks can be malicious or non-malicious. Malicious insiders have the intent to eavesdrop, steal or damage information, use information in a fraudulent manner, or deny access to other authorized users. Non-malicious attacks typically result from carelessness, lack of knowledge, or intentionally circumventing security for non-malicious reasons such as to "get the job done."
Distribution	Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product such as a back door to gain unauthorized access to information or a system function at a later date.

this, we discuss the framework of the U.S. Information Assurance in Section 2. In Section 3, based on the Evaluation Assurance Level (EAL) of the CC standards [3–7], we propose the implementation framework of information system security classification for e-Taiwan. At last, we conclude this paper in Section 4.

2. Brief discussion of the U.S. IA framework

The Information Assurance Technical Framework Forum (IATFF) is a National Security Agency (NSA) sponsored outreach activity created to foster dialog amongst U.S. Government agencies, U.S. Industry, and U.S. Academia seeking to provide their customers solutions for information assurance problems. The ultimate objective of the IATFF is to agree on a framework for information assurance solutions that meet customers' needs and foster the development and use of solutions that are compatible with the framework. Furthermore, the Information Assurance Technical Framework (IATF) provides technical guidance for protecting information and information infrastructures [3].

Today, the information infrastructure processes, stores, and transmits information critical to the mission/business operations of the organization. Protecting this information is achieved through Information Assurance (IA) that addresses the full suite of security requirements for today's information infrastructure. Information assurance relies on the people, the operations, and the technology to accomplish the mission/business and to manage the technology/information infrastructure. Attaining a robust information assurance posture means implementing policies, procedures, techniques, and mechanisms at all layers throughout the organization's information infrastructure [3].

The IATF defines a process for developing a system with information assurance and the security requirements for the hardware and software components in the system. Applying these principles results in layers of protection in the information infrastructure are known as the Defense-in-Depth Strategy. Fig. 2.1 depicts an important principle of the Defense-in-Depth strategy: the achievement of IA requires a balanced focus on three primary elements — people, technology, and operations [3].

The process of IATF implementation includes: first of all, classifying the protected information asset by means of the

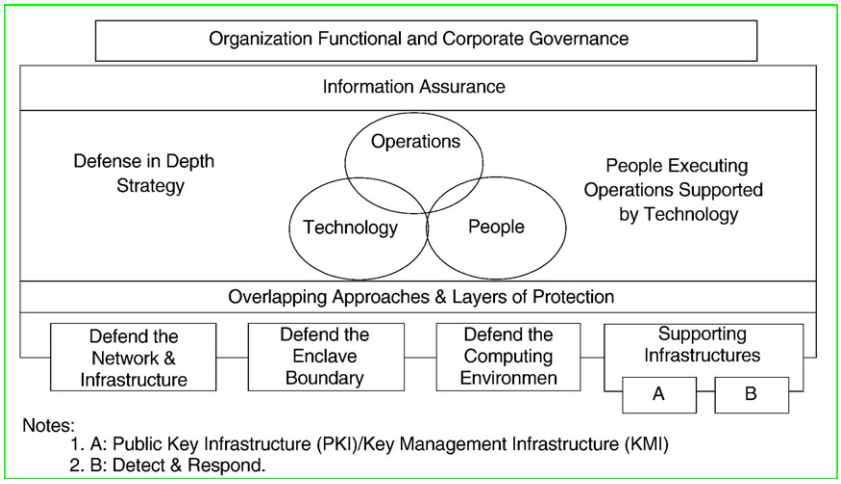

Fig. 2.1. Illustration of Defense-in-Depth [3].

Table 2.1
Definition of information value [3]

1. **V1**: Violation of the information protection policy would have negligible adverse effects or consequences.
2. **V2**: Violation of the information protection policy would adversely affect and/or cause minimal damage to the security, safety, financial posture, or infrastructure of the organization.
3. **V3**: Violation of the information protection policy would cause some damage to the security, safety, financial posture, or infrastructure of the organization.
4. **V4**: Violation of the information protection policy would cause serious damage to the security, safety, financial posture, or infrastructure of the organization.
5. **V5**: Violation of the information protection policy would cause exceptionally grave damage to the security, safety, financial posture, or infrastructure of the organization.

Table 2.2
Definition of information threat levels [3]

1. **T1**: Inadvertent or accidental events (e.g., tripping over a power cord).
2. **T2**: Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening).
3. **T3**: Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers).
4. **T4**: Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations).
5. **T5**: Sophisticated adversary with moderate resources who is willing to take significant risk (e.g., international terrorists).
6. **T6**: Extremely sophisticated adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation–state, international corporation).
7. **T7**: Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g., nation–states in time of crisis).

Table 2.3
Definition of Evaluation Assurance Level (EAL) [3]

1. **EAL1:** Functionally tested. Applicable where some confidence in correct operation is required, but when the threats to security are not viewed as serious.
2. **EAL2:** Structurally tested. Requires the cooperation of the developer in the delivery of design information and test results, but should not demand more effort (or substantially increased cost or time) than is consistent with good commercial practice.
3. **EAL3:** Methodically tested and checked. Permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.
4. **EAL4:** Methodically designed, tested, and reviewed. Permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require substantial specialist knowledge, skills, and other resources.
5. **EAL5:** Semiformally designed and tested. Permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices supported by moderate application of specialized security engineering techniques.
6. **EAL6:** Semiformally verified design and tested. Permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment to protect high value assets against significant risks.
7. **EAL7:** Formally verified design and tested. Applicable to the development of products to be used in extremely high risk situations and/or where the high value of the assets justifies the higher costs.

Table 2.4
Definition of Strength Mechanism Level (SML) [3]

1. **SML1** is defined as basic strength or good commercial practice. It is resistant to unsophisticated threats (roughly comparable to T1 to T3 threat levels) and is used to protect low-value data. Examples of countered threats might be door rattlers, ankle biters, and inadvertent errors.
2. **SML2** is defined as medium strength. It is resistant to sophisticated threats (roughly comparable to T4 to T5 threat levels) and is used to protect medium-value data. It would typically counter a threat from an organized effort (e.g., an organized group of hackers).
3. **SML3** is defined as high strength or high grade. It is resistant to the national laboratory or nation–state threat (roughly comparable to T6 to T7 threat levels) and is used to protect high-value data. Examples of the threats countered by this SML are an extremely sophisticated, well-funded technical laboratory and a nation–state adversary.

Table 2.5
Degree of robustness [3]

Information value	Threat levels						
	T1	T2	T3	T4	T5	T6	T7
V1	SML1	SML1	SML1	SML1	SML1	SML1	SML1
	EAL1	EAL1	EAL1	EAL2	EAL2	EAL2	EAL2
V2	SML1	SML1	SML1	SML2	SML2	SML2	SML2
	EAL1	EAL1	EAL1	EAL2	EAL2	EAL3	EAL3
V3	SML1	SML1	SML1	SML2	SML2	SML2	SML2
	EAL1	EAL2	EAL2	EAL3	EAL3	EAL4	EAL4
V4	SML2	SML2	SML2	SML3	SML3	SML3	SML3
	EAL1	EAL2	EAL3	EAL4	EAL5	EAL5	EAL6
V5	SML2	SML2	SML3	SML3	SML3	SML3	SML3
	EAL2	EAL3	EAL4	EAL5	EAL6	EAL6	EAL7

information value and threat in Table 2.1 and Table 2.2; then, according to the information value and threat, determining the required EALs (as shown in Table 2.3) and SMLs (as shown in Table 2.4) by the robustness table (as shown in Table 2.5).

Various risk factors, such as the degree of damage that would be suffered if the security policy were violated, threat environment, and so on, will be used to guide determination of an appropriate strength and an associated level of assurance for each mechanism. Specifically, the value of the information to be protected and the perceived threat environment are used to obtain guidance on the recommended SML and EAL. For example, one corporation with a large intranet that processes only unclassified data, and the corporation has stringent legal requirements for protecting its data from unauthorized access or modification, and off-line stand-alone access is required to view the protected data. Taking all of the abovementioned into consideration, the information value should be at the V3 level, and the perceived threat should be at the T4 level. Using the Degree of Robustness table, as shown in Table 2.5, the minimum SML and EAL recommended is SML2 and EAL3 based on the information threat and value levels [3].

After determining the required SML, the recommended mechanisms for establishing needed security management are depicted in Table 2.6.

The Defense-in-Depth Strategy has been broadly adopted. For instance, within the U.S. Department of Defense (DoD), the Global Information Grid (GIG) IA Policy and Implementation

Table 2.6
Security management mechanisms [3]

	Compromise recovery	System administration	Training	Operational security (OPSEC)	Trusted distribution	Secure operation	Mechanism management
SML1	Informal plan	FITSAF1~ FITSAF2	Training available at user's discretion	Implementing OPSEC at user's discretion	Direct vendor purchase	Informal plan of operation	Procedural, at user's discretion
SML2	Detailed plan that is reviewed and approved	FITSAF3~ FITSAF4	Formal training plan	OPSEC training required; implementation at user's discretion	Certificate of authenticity, virus scan, validation	Formal plan of operation	Procedural, reminders, at user's discretion
SML3	Detailed plan that is reviewed and approved	FITSAF4~ FITSAF5	Knowledge/ skill certification required	OPSEC training required, implementation required	Protective packaging, checksums, validation suite	Detailed, formal plan of operation	Automated support

Notes:
1. FITSAF: Federal Information Technology Security Assessment Framework.
2. SML: Strength Mechanism Level.

Table 3.1
Classes of information security operation service targets (government organizations) in Taiwan [8]

	National Defense Division	Administration Division	Academic Division	Business Division (1)	Business Division (2)	Business Division (3)	Business Division (4)	Sum
A	27	71	0	16	3	7	2	126
B	102	190	26	32	34	12	3	399
C	63	755	25	82	18	21	35	999
D		1261	837	71	14	0	6	2,189
Total	192	2277	888	201	69	40	46	3,713

Source: N.S. Chi (2003), A aide of Information Security in Taiwan—National Information and Communication Infrastructure Security Mechanism Plan, Journal of Information Security, Vol. 1, pp. 4–10, Table 2.

Guidance was built around the Defense-in-Depth Strategy. This departmental-level policy cites the IATF as a source of information on technical solutions and guidance for the DoD IA implementation [3]. Furthermore, the Defense-in-Depth also may apply into the implementation framework of information system security classification in other countries.

3. A framework of classification and implementation for e-Taiwan information system security

The National Information & Communication Security Taskforce (NICST) of Executive Yuan in Taiwan at the end of 2002 had set up an integral information and communication

Table 3.2
An integral information and communication security defense system for e-Taiwan [9]

	SML	Defense in depth	ISMS approaches	Audit method	Information security training (CEO, CIO, IT Technicians, General Officials)	Professional license
Class A	4	N-SOC/SOC, IDS, Firewall, Anti-virus	Passing third-party ISMS accreditation in 2007	at least 2 internal audit per year	at least 4, 6, 18, 4 h/year	2 Copies of information security certificate in 2007
Class B	3	SOC (Opt.), IDS, Firewall, Anti-virus	Passing third-party ISMS accreditation in 2008	at least 1 internal audit per year	at least 4, 6, 16, 4 h/year	1 Copy of information security certificate in 2007
Class C	2	IDS, Firewall, Anti-virus	Self-establishing ISMS working-group	Self-review	at least 2, 6, 12, 4 h/year	Information security professional training
Class D	1	Firewall, Anti-virus	Promoting ISMS concepts	Self-review	at least 1, 4, 8, 2 h/year	Information security professional training

Notes:
1. Classification of information security in government organizations includes 3713 units; however, after re-examining and increasing the Academic Division, it is estimated to become 7028 units.
2. Source: T.A. Wang (2006), The presentation of Executive Yuan Council Meeting No. 2993, 2006-06-14.

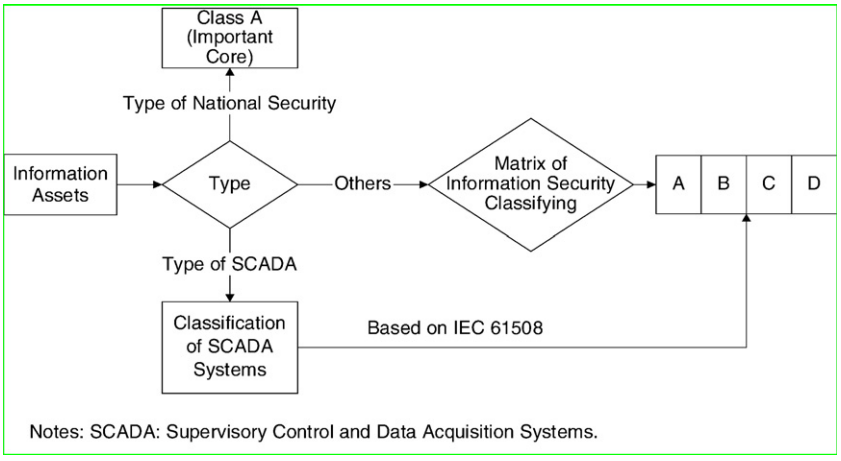

Fig. 3.1. Framework of information security classifying operation process.

security defense system for 3713 major government organizations, and also implemented strict control on twenty major national infrastructure information systems that affect national security and social stability for the purpose to continuously strengthen the implementation of information security operations. It vertically classifies the unit levels, the table of organization, and investment amount into four levels—A (important core), B (core), C (important), and D (general), and horizontally distinguishes the attribute of government organization into national defense, administration, academy and undertaking, and applies to all sorts of information security operations of our government organization as shown in Table 3.1. Besides, the integral information and communication security defense system is shown in Table 3.2.

The abovementioned information and communication security classes are based on "risk classification management" in BS 7799 Information Security Management System (ISMS). The security level is divided into four classes to facilitate emergency response and reflect the severity of impact when an incident is reported [10]:

- Class A: Affecting public security, social order and people's life and property.
- Class B: Mission critical systems come to a halt, business inoperable.
- Class C: Business interruption results in system inefficiency.
- Class D: Business operation temporarily interrupted and restorable momentarily.

Since the information and communication security classes had been implemented, many units proposed some suggestions of modulation like stipulating the classes based on the confidentiality of information or system; determining its security levels based on whether the information or system gets involved in data security (such as the individual privacy materials, etc.) or national security. However, the classification has not exchanged yet until nowadays.

Owing to the deficiencies of the old information and communication security classification, we propose a new framework of information system security classification for e-Taiwan as described below.

Firstly, the security level is redefined and divided into four classes to facilitate emergency response and reflect the severity of impact when an incidence is reported:

- Class A: It is resistant to the national laboratory or nation-state threat and is used to protect very high-value data.
- Class B: It is resistant to counter a threat from an organized effort (e.g., an organized group of hackers) and is used to protect high-value data.
- Class C: It is resistant to sophisticated attack actions from an individual person and is used to protect medium-value data.
- Class D: By way of the basic strength achieved by a good information security operation, it is resistant to unsophisticated threats and is used to protect low-value data.

Secondly, corresponding to the international standards of risk classification and the approaches of advanced countries, the information system should be divided into three categories:

- Information systems related to national security.
- Supervisory Control and Data Acquisition (SCADA) systems (e.g., the electric energy management system).
- The others.

Thirdly, proposing a new framework for information system security classification depends upon the information systems

Table 3.3
Example of information security class matrix [3]

Information value	Low	Medium	High
Antagonist			
Null	D	C	B
Personal	C	B	A
Organized group	B	B	A
Nation–state adversary	A	A	A

Table 3.4
Summary of the potential impact definitions for each security objective—confidentiality, integrity, and availability [11]

Security objective	Potential impact		
	Low	Moderate	High
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability: Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Source: NIST (2003), Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards (FIPS) Publication (PUB) 199, page 6.

categories as shown in Fig. 3.1. The information systems related to national security should be classed into Class A (important core); the SCADA system security level could follow the international standards such as IEC 61508, etc.; the other information system security level may follow the illustration of information security class matrix as shown in Table 3.3. The Table 3.4 is the definition of potential impact of the information asset security targets in Table 3.3.

In order to assure the information security of the information system, if the information systems belong to Class A, such as SCADA systems, we also recommend they should adopt such as physical isolation and/or compartmentalization of Defense-in-depth deployment [12,13].

4. Conclusion

Security is just like air. It is originally worthless, but its existence will not be painfully detected until it is lost. The outflow of private information causes unprecedented threat to e-Taiwan. The investigation wastes time and the forensic is difficult. Rumor has it that Mainland China has obtained the individual data (i.e., census register, military record and tax) of people in Taiwan. On March 27, 2004, the event of Trojan-Horse detecting e-bank accounts and passwords has been occurred in Taiwan. On April 14, 2004, it was even reported by mass media that "Mainland China hackers invaded the Presidential Hall." We should recognize how to ensure "when there is confidence that information and information systems are protected against attacks through the application of security services in such areas as availability, integrity, authentication, confidentiality, and non-repudiation. The application of these services should be based on the protection, detect, and react paradigm. This means that in addition to incorporating protection mechanisms, organizations must expect attacks and must also incorporate attack-detection tools and procedures that allow them to react to and recover from these attacks." The achievement of information security assurance is not only an important link to information security infrastructure in e-Taiwan but also public property that is worth of being treasured.

The purpose of ISMS is to assure the legal gathering of information resources and to provide complete, uninterrupted information system operation even when facing the intrusion [14]. According to IATF and the relevant guidelines of information security, in this paper we propose a new framework of information system security classification for e-Taiwan to reach the vision "Information and communication network resources can be fully used in an obstacle free and secure environment by year 2008."

Our country begins to concern the information security operation of cyberspace, and there is not much accumulation of time and experience. Everybody is trying to find out the value, idea, or system that should be set up. As information technology progresses rapidly and under the environment of information system security of cyberspace, the issue of information system security that is relevant to our country people's livelihood needs deeper thinking and discussion. As a member of digital era, we must not fail to live up to the opportunity that all the people participate in setting up the model of information society security.

References

[1] ISO/IEC, (2006), Information technology–Security techniques—Security assessment for operational systems, ISO/IEC TR 19791:2006(E).
[2] L. McCarthy, Intranet Security, Prentice-Hall, 1998.
[3] Frederick Cynthia, (2002), Information Assurance Technical Framework, Release 3.1, National Security Agency, http://www.iatf.net.

[4] ISO/IEC, (2005), Information technology–Security techniques—evaluation criteria for IT security (all parts), ISO/IEC 15408:2005(E).
[5] ISO/IEC, (2005), Information technology–Security techniques—methodology for IT security evaluation, ISO/IEC 18045:2005(E).
[6] ISO/IEC, (2005), Information technology—code of practice for information security management, ISO/IEC 17799:2005(E).
[7] K.J. Farn, S.K. Lin, A Study on the information security guideline and source of reference guidance, Information Security (Issue 38) (2007) 92–94.
[8] N.S. Chi, A aide of Information Security in Taiwan—National Information and Communication Infrastructure Security Mechanism Plan, Journal of Information Security 1 (2003) 4–10.
[9] T.A. Wang, The presentation of Executive Yuan Council Meeting No. 2993 (2006), 2006-06-14.
[10] http://www.nicst.nat.gov.tw/template/nics/content.pdf, (2004/08/01).
[11] NIST, Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards (FIPS) Publication (PUB) 199 (FIPS PUB 199) (2003).
[12] The Executive Yuan National Information Communication Security Taskforce (NICST) of Republic of China (R.O.C.), (2005), Information security dispatch document No. 0940100802, 2005-09-28.
[13] The Executive Yuan National Information Communication Security Taskforce (NICST) of Republic of China (R.O.C.), (2006), Information security dispatch document No. 0950100631, 2006-10-25.
[14] K.J. Farn, et al., A study on information security management system evaluation—assets, threat and vulnerability, Computer Standards & Interfaces 26 (No. 6) (2004) 501–513.

Kwo-Jean Farn is a part time associate professor of National Chiao Tung University (NCTU) in Taiwan. He received his PhD degree in 1982. During a 20-year career at Information Technology and about 10-year career at Information Security. He is chair of the Implementation National Critical Information Infrastructure Protection Project at Computer & Communications Research Laboratories/Industrial Technology Research Institute (CCL/ITRI) in Taiwan from Jan. 1999 to Sep. 2000. He worked at ITRI for more than 18 years until summer of 2001. He has 9 patents of information security area.

Shu-Kuo Lin received his MBA degree in Information Management from Tam Kang University, Taiwan, in 2001. Currently, he is a PhD student of the Institute of Information Management, National Chiao Tung University, Hsinchu, Taiwan. His research interests include information security and network management.

Chi-Chun Lo was born in Taipei, Taiwan. He received the BS degree in mathematics from the National Central University, Taiwan, in 1974, the MS degree in computer science from the Memphis State University, Memphis, TN, in 1978, and the PhD degree in computer science form the Polytechnic University, Brooklyn, NY, in 1987. From 1981 to 1986, he was employed by the AT&T Bell Laboratories, Holmdel, NJ, as a Member of Technical Staff. From 1986 to 1990, he worked for the Bell Communications Research. Since 1990, he has been with the Institute of Information Management, National Chiao-Tung University, Taiwan. At present, he is professor and director of the institute. His major current research interests include network design algorithm, network management, network security, network architecture, and wireless communications.