International Journal of Security and Its Applications
Vol. 9, No. 5 (2015), pp. 1-18
http://dx.doi.org/10.14257/ijsia.2015.9.5.01

Security Model for Sensitive Information Systems and Its Applications in Sensor Networks

Tianbo Lu[1,2], Xiaobo Guo[1], Lingling Zhao[1], Yang Li[1], Peng Lin[1] and Binxing Fang[1]

[1]School of Software Engineering，Beijing University of Posts and Telecommunications, 100876, Beijing, China
[2]Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada
lutb@bupt.edu.cn, gxbbest@126.com, wodepengyouzhao@163.com

Abstract

The study of security models for sensitive information systems has been taken on for years, but still lag far away behind the progress of information security practice. During this century, the thought of seeking the system security to the source of system development lifecycle received huge improvement in the system and software assurance domain. This paper firstly expounds the understanding of information security by illustrating information security study development progress since pre-computer age and presents a description of cyberspace and cyberization security by summarizing the status quo of cyberization. Then a security model called PDRL, which includes six core security attributes of sensitive information systems, is proposed to protect the security of sensitive information systems in the whole system life-cycle. At last, this paper probes into further discussion about controllability attribute and proposes a controllability model in sensitive sensor networks, followed by a probability computing formula and the example for computing the controllability of sensitive sensor networks. By dividing each single element of sensitive information and each element-related operation into a corresponding classification, this paper makes a reasonable description of the quantitative description about controllability.

Keywords: *Sensitive information system, sensor network, security model, control, security attribute*

1. Introduction

The rapid growth of information technology provides great convenience for our living, working, and recreating. Big data has been going through those infrastructures such as information system, Internet, sensor networks, and cyber-physical systems. Among these data, there is some sort of information that should be protected such as market information, financial information, trade information, medical information, human resource information and even national military information. Any kind of leaking, losing, misusing, modifying, destroying or unauthorized visiting of sensitive information can adversely affect the privacy or welfare of some individuals, trade secrets of a business or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information [1]. We define these kinds of information as sensitive information, and accordingly we name these systems as sensitive information systems.

However, as the information technology is expanding rapidly, many untested information systems with low security and confidence level are given to birth. Meanwhile, these systems are frequently updated, resulting in original vulnerabilities being covered

ISSN: 1738-9984 IJSIA

and succeeded. And robust network techniques and vulnerable network techniques are often integrated into one system, giving rise to new attack models, while at the same time, bringing new kinds of security problems and security risks. Therefore, the protection of sensitive information has become people's major concern. Proposed in 1970s, BLP model [2] and BiBa model [3] were raised to provide data confidentiality assurance and integrity assurance respectively by marking data or personnel into different security levels. Later, Clark-Wilson data integrity security model [4] was presented. Chinese Wall commercial security model [5], McCumber information security model [6], Reliability Assurance model [7] and Trust model [8]. Up to now, sensitive information security model and protection techniques have raised considerable concern and been developed gradually. However, the controllability of sensitive information system is rarely been noticed. The study of controllability is critical to sensitive information system security. If personal sensitive information is deleted by malware or stolen by spyware, the users are no longer in possess of this information and they no longer have the controllability of this information. Once a hacker steals this information, the controllability of this information will decline. This paper will take the guidance of seeking sensitive information system security to the system development life cycle, analyze the sensitive information system security framework, with the use of PDRL model, and probe into the attribute of controllability in sensor networks.

2. The Comprehension of Information Security

The connection of information security and the security attributes that it contains, are always coherent with the level or degree of informationization at that time. The progress of information security study can be divided into four phases. The initial phase was in 1950s, in which people believed that information security should focus on the study of cryptology and put emphasis on communications security. This period was called Communications Security (COMSEC) age and the key point was data security. The symbolic achievement was the publication of Communication in the Presence of Noise [9], which explored the cryptology on the sound basis of mathematics. The publication also indicated that cryptology and security communication had officially become independent disciplines. The next phase was in 1970s. People were more concerned about whether computer system was vulnerable to unauthorized access or not. This period was called Computer Security (COMPSEC) by the academic world. The main feature of this age was the Orange Book-- Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) [10] published in early 1980s. According to the definition of TCSEC, information security had three security attributes, namely security, integrity and utility. The third phase was in 1990s. With the application of computer system and computer network widened, people were more concerned about protecting the connected computers from network attacks. Academic world called this period as Network Security (NETSEC) age. Information security attributes had gained a few more members, such as information and system controllability, information non-repudiation. When we moved into 21st century, information security had moved to the fourth phase, people were more concerned about information assurance and information system assurance and how to construct integrated assurance systems in order to assure that information and information system worked normally. This period was called information assurance age by academic world. With the concept of information assurance, information security was regarded as a dynamic process, consisting of protection, detection, response and recovery dynamic progresses [11]. Information security had gained other security attributes from the prospective of information and infrastructure assurance, such as the reliability of network and information system [12], the survivability of network and information system [13]. Network security was a correlated concept of information security and the products of information security came to network age. Network security actually went across the third and fourth phase of information security development.

Recently, people are concerned much more about cyber security. Ahead of the discussion of cyber security, precisely understanding the meaning of cyberspace is essential. In 2008, Bush government issued NSPD-54/HSPD-23(National Security Presidential Directive 54/ Homeland Security Presidential Directive), and defined that cyberspace is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Usually this term also means the virtual environment in which information flows and people communicate. In 2011, Department of Defense of the United States presented that "Cyberspace is a defining feature of modern life. Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace" [14]. Our option for the description of national cyberspace can be expressed as:

The public environment, under the administration of the government, carries information and services as well as all the digital activities it contains. Public environment contains national infrastructure information network (including telecommunication network, public internet and broadcasting network), computer system, wireless sensor networks, the embedded processors and controllers in industrial infrastructure, all those connected infrastructures; Digital activities include the process of creating, modifying or using information and any other activities that happen in this environment. The government has the administration right in the cyberspace, as well as the obligation and responsibility to take actions to protect the national cyberspace.

For information security, people's concerns were targeted at the cyberspace, information system and the security of data itself, such as data leak, imitation, modification or denial those security issues. In recent years, information security has changed the focus to junk email and pornographic information and raises concern in cultural, propaganda, and educational world. The paper [15] advocated putting information assurance into the framework of information security and studying the assurance of information security and those security attributes it involved.

The questions of how many and what security attributes do the information security contain haven't been settled down. ISO/IEC 17799 defined that information security had three security attributes, confidentiality, integrity and availability [16]. These three attributes were called CIA by scholars. U.S. National Infrastructure Protection Center added authentication and non-repudiation to CIA [17], ITU-X.800 gave the description of those related attributes [18]. U.S. computer security expert Michael E. Whitman proposed a new security framework, including confidentiality, integrity, availability, authenticity, utility and possession [19]. We have proposed information security four elements theory, believed that among several attributes of information security, confidentiality, authenticity, controllability and Availability are four fundamental attributes and do not overlap or cover each other. The other attributes, like utility , integrity, legality, uniqueness, non-repudiation, specificity, possession, traceability, survivability, stability and reliability are side highlights of the above four basic attributes and can be attributed to the four fundamental attributes. We defined the concept of information security as that it was the process of attacking and defending the inner attributes of information system, information and information usage.

We portrait information security as, protecting the interests of individuals, society and the whole country in information area; maintaining the confidentiality, integrity, authentication, non-repudiation, controllability, availability of information and its source; fighting against all the threats that would harm the country' stability, or infect the countries' politic, economic, cultural and homeland security with all the technical and non-technical measures. As the information security threat evolves faster, new attacks become stronger and more targeted, security issues are deepened and widened and information security has extended from traditional information system to the devices or systems of information. We call it Cyberization security. Many well-known scholars and experts have their own study and reviews on Cyberization security, and we believe that the core issue of Cyberization Security is that it should not only contain the security of information system itself, but also should include the security of those entities that are manipulated and controlled by Cyberization - the security of manipulation; and should not only meet the needs of cyberspace security functional demands, but also the security assurance demands - measureable security.

The security of behavior includes the features as below: All kinds of behaviors (manipulation, transaction) do reflect the entities' being authorized to get access to the objective entity; Source of objective entities was defined and controllable; Identity of this entity is identifiable; Main entities' access to the objective entities' content is consistent with the security policy; Output of the access meets the expected outcome; Behavior is auditable; Violations of the policy are revocable.

3. PDRL Security Model of Sensitive Information System

The paper [20] in the first time put forward the concept of software assurance, and at that time, software assurance was confined in software quality assurance. After the coming of 21st century, software assurance applied to the assured security of software. In April 2005, the U.S. President Information Technical Consultant Committee (PITAC) issued Cyber Security: A Crisis of Prioritization [21], pointing out that software was the source of U.S. cyber system's and computing system's vulnerabilities and in the past 10 years, the work of U.S. protecting the national information technology basic construction was a fiasco. In order to change the defense policy of endless patching, and to solve this problem in overall system, they put forward 10 study projects of high priority, and the third project was software assurance. On April 2006, U.S. president Office issued National Science and Technology Council: Federal Plan for Cyber Security and Information Assurance Research and Development. This plan proposed 13 projects that needed to be supported, and software assurance was included [22].

Software assurance was the expected assurance degree of software non-vulnerability and software functionality [23]. Its principle was that in every phase of software lifecycle we should take security measures to assure the security of software. Academies further expanded the idea of software assurance and raised the concept of system assurance aimed at assuring the security of the products in every phase of system life cycle. The U.S. DoD gave the definition of system assurance as: "System Assurance is the confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted during the lifecycle".

In 2008, NDIA published the Engineering for System Assurance V1.0 Guidebook expressed the value of Assurance Case, requiring that the Assurance Case lie in the entire system lifecycle, being sustainable and maintainable[24]. Paper [25] pointed out the relationship of system assurance and software assurance: software assurance was in the core of system assurance.

Though information security has already been treated as a dynamic procedure consisting of protection, testing, responding, recovering and *etc.*, this dynamic procedure hasn't considered the system development phase. Based on PPDR (Policy, Protection, Detection, Response) model and PDRR (Protection, Detection, Response, Recovery) model, combining the concept of system assurance, we propose the Policy, Protection, Detection, Response, and Recovery in Lifecycle (PDRL), as shown in Figure 1. This model includes three dimensions: system state, security service and security measures. The main feature of PDRL is its emphasis that sensitive information system security should not be confined in passive protecting level, but strives for constructing a multidimensional and active defense system based on protection, detection, response and recovery and fully uses the guidance of information security strategies.

With careful analyses, PRDR and PDRR models both emphasized on the security protecting measures after the development phase and didn’t take the whole life cycle of information system into consideration. Compared with those models, the PDRL model proposed by this paper seeks the information security to the source and emphasizes on the protecting throughout the whole lifecycle of the system from information system demands to maintenance.

System states are phases of system life cycle, including concept, demand, design, test, integration, running and maintenance as well as recruitment. Again for each phase, we can divide it in more details. In different phases, what we care about and what measures we take are different.

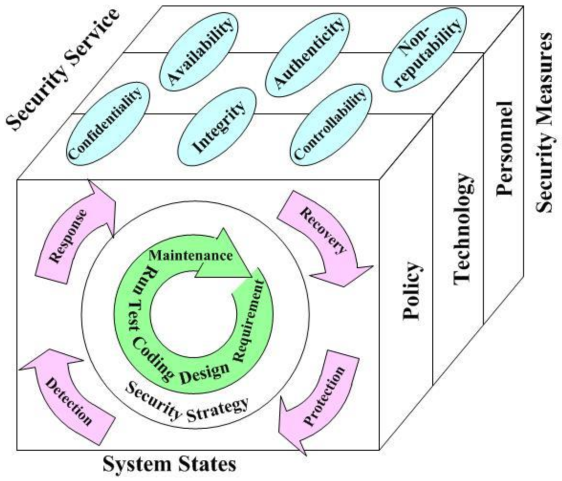

Figure 1. PDRL Model

Around system lifecycle concept, we need to develop sensitive information security strategies. It is the key of system security. With the guidance of security strategy, we should fully deploy actions combining protection, detection, response and recovery. Security protection is no longer confined in the protection of the on-run system, but also lies in every phases of system development. Detection is aimed at finding the security vulnerabilities and repairing them. Meanwhile, we should also be cautious on the invasions and thus take rapid actions to defend our system. After the invasion, there should be some measures in place to recover the system to normality. This is the so called all- round security protection.

Security measures have three key elements, personnel, policy and technology. As for personal, we should enforce the training and improve their security protection ability and security awareness. As for policy, it means law, regulation and management. As for technology, we should establish and improve graded information system security protection mechanisms, enforce both dynamic and static risk evaluation system, strengthen the development and deployment of cryptographic techniques, construct the information trustworthy system, build and improve information systems security monitoring system, and attach great importance to the work of information system security emergency response and the disaster backup of important information.

The security service layer sums up the main content of the information security and security attributes. We believe that the three attributes described by classical CIA security model, confidentiality, integrity and availability have already been out of date, and they cannot fully depict the security service. The U.S. DoD once proposed five security attributes of confidentiality, integrity, authentication, non-repudiation and availability [26]. Security expert Donn B.Parker extended the CIA model to six-key-elements model, as confidentiality, possession, integrity, authenticity, availability and utility in 1998 [27]. For example, unauthorized copy of software would not cause the loss of confidentiality, integrity, and availability, but only the loss of possession. Paper [28] believed that the six attributes were unaffected with each other and indispensable. In 2009, Doctor Wu Xianping from Australian Monash University analyzed the six attributes in his doctoral dissertation and pointed out that this model lacked the non-repudiation attribute, for example the legal user in bank system denied the transaction. Meanwhile in the other aspects, this model didn't solve the privacy problem, for example, in medical system, patients should be able to control his/her sensitive information, and decide who had the authority to access this information by themselves. So he proposed five-key-elements model, as "Authenticity & Authority, Integrity, Non-reputable, Confidentiality, and Availability" [29]. In 2013, based on the extensive literature analysis, Yulia Cherdantseva and Jeremy Hilton proposed a Reference Model of Information Assurance & Security (RMIAS) as an extension of the CIA-triad, which includes confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability [30].

In section 2, we listed the six attributes, confidentiality, integrity, availability, authenticity, non-repudiation, and controllability. We believed they were the principal attributes of sensitive information and were fundamental to sensitive information service. Among them, confidentiality means to assure that the sensitive information are accessed only by authorized users; integrity means ensure the accuracy and completeness of sensitive information; availability means the authorized users can access to the sensitive information when needed; authenticity refers to the effectiveness of information processing, and validation of the authorization; non-repudiation means the users cannot deny what they have done after the transaction or any other actions; controllability means to assure the user's control of sensitive information.

In paper [28], the utility was described as the information encryption key cannot be lost, when lost, the information was useless, thus lose the utility. We believe this feature can be covered by the availability, because the loss of key will lead to non-availability of the information. The possession was described as: the loss of the node, disk or other information container or the authentication information loss would lead to the possession loss. We believe that this is essentially a loss of control over the information and can be included in the scope of the controllability study.

In paper [31], two vulnerability aspects of SCADA systems were given: one is the threat of unauthorized access to the control software; the other is the threat of packet access to the network segments hosting SCADA devices, which is used to acquire information about the physical processes from sensors and so on. Paper [32] presents a new mathematical model and metric for quantitative information flow, as applied to confidentiality and integrity. Paper [33] tells how to make quantification of integrity respectively in the aspects of contamination and suppression. Contamination measures how much untrusted information reaches trusted outputs and suppression measures how much information is lost from outputs. In paper [34], the security intrusion and the response of an intrusion tolerant system to an attack is regarded as a random process, in which way security quantification analysis can be carried out for steady-state behavior. Paper [35] introduced a new kind of theoretical method to balance utility and privacy in sensor networks. With this method, raw sensor data could be transformed into a new form, which minimizes exposure of user defined private attributes while maximally exposing application-requested public attributes. Paper [36] proposes a framework for analyzing security in web protocols respectively in inference construction style and construction style.

On the controllability of information security, we discussed the proliferation of harmful information on the Internet in the paper [15]. We extracted some basic features of information broadcast in the Internet, and proposed a control model and evaluation structure of Internet information security. The former included the control model that based on the content, the control model based identity, and the control model based on behavior; the next one included the evaluation of the information accessibility, evaluation of information discover and the evaluation of information response ability. But, on the controllability of sensitive information, there are few reports.

4. The Controllability Model for Sensitive Sensor Networks

Before we put forward this model, we have to define the controllability of sensitive information. Cai, *et al.,* discussed the controllability of dynamical multi-agent systems [37]. In the discussion of information content [15], we considered that controllability is the control ability of information flow and to assure that some information can be accessed, and some information cannot be accessed. It indicates that the information flow and sensor network can be monitored by the controller. As for sensitive sensor networks, we believe the controllability means the ability of the users to control the flow of information in the sensor network, so that some information can flow out of the network and some can't.

Controllability, in sensitive sensor networks, is regarded as the users' authority which is the ability to control the outflow of information. It may allow some information flow out of the sensor network, while reject others, according to specific rules and conditions. In the condition that controllability is absolutely reliable, for some certain operation requests, if the sensor network allows the information to flow out and actually it will do, however, for other operation requests, if the sensor network rejects its flowing out, there will be no possibility that the information could leak out. As a matter of fact, sensitive sensor network is faced with some basic threats, which makes the leak of information possible, such as the uncontrollability of core chip and key technology, low security level of open operating systems, unreliable login to the sensor network, unsafe storage of data, software programming bug, illegal outreach, all kinds of invisible ports and visible peripherals, removable storage medium, virus, Trojan [38], misconduct of end users and so on. If the information flowed out of a sensor network, the controllability of the sensor network related to the information would change. For example, files in sensor network for storing user name and password having been stolen by Trojan, the control ability of the user to this file would decline or absolutely be lost. Another example, if the sensor network was invaded by an attacker and the user name and password were modified, the user won't be able to use the sensor network and lost his control ability to the sensor network.

In order to give an abstract description of the controllability of a sensor network, we collectively refer the processes, files, heap, stack, memory, hard drives, gateways and other elements of a sensor network. In this way, the discussion on the controllability of a sensor network can be substituted by the discussion on its elements. A sensitive sensor network is considered to have boundaries, for example, input and output, switches and routers, import and export gateways to form the layered borders of a wireless sensor network. Elements in a sensitive sensor network and all paths between them within the network are defined as a connected closed set, which are called the controllable region of the system. The probability that sensitive information elements leave the controllable region can be used to describe the controllability of the sensor network.

The allowance of or the rejection to a particular piece of information's flowing out can be considered as a response that the sensor network makes to the outside operation requests. For a particular kind of information elements, if an operation request is judged legitimate, the corresponding information can be allowed to flow out. On the other hand, if an operation request is judged illegal, the corresponding flowing out will be rejected. As a result, the probability that sensitive information elements could leave the controllable region can be regarded as the probability that the sensor network could make a correct identification on the outstanding operation request.

There are four cases:

- Case 1: A legal request is judged legitimate and the corresponding information is allowed to flow out;
- Case 2: A legal request is judged illegitimate and the corresponding information is rejected to flow out;
- Case 3: An illegal request is judged legitimate and the corresponding information is allowed to flow out;
- Case 4: An illegal request is judged illegitimate and the corresponding information is rejected to flow out.

According to the definition of controllability, case 1 and case 4, which reflect a system's controllability, are what we want. Case 2 and case 3 reduce the controllability of a sensor network. Quantitative model for computing controllability in sensitive sensor network is given in Figure 2.

All controllable elements can be classified into kinds according to their flowing-out nature. Controllability here is the probability that the sensor network can make a correct identification on operation requests to these kinds of elements.

For the kind of specific element, the system sets indexes to answer whether an operation request is legitimate, with the word "Yes" or "No". If the sensor network is able to give clear answers to all the indexes according to the information acquired by analyzing operation requests, the probability that the sensor network can make a correct identification on this operation request for this kind of element is 1; If the sensor network cannot give even one clear answer to these indexes, the probability is 0.5 (Because the sensor network doesn't obtain any useful information by analyzing these operation requests, the judgment whether the operation request is legitimate or not is completely random and there are only two kinds of possibilities: legal or illegal. If the request is judged to be legal, the information will be allowed to flow out; if illegal, the information will be rejected to go out. So there are only two kinds of possibility and one of them must be correct).

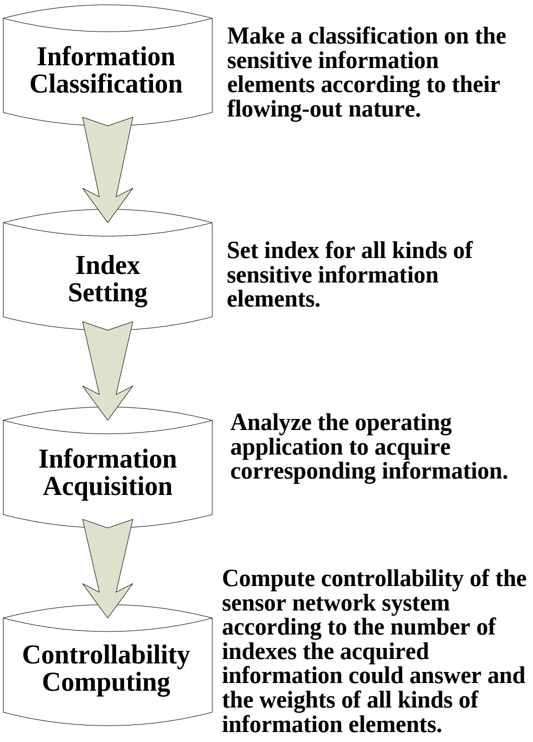
Information Classification
Make a classification on the sensitive information elements according to their flowing-out nature.
Index Setting
Set index for all kinds of sensitive information elements.
Information Acquisition
Analyze the operating application to acquire corresponding information.
Controllability Computing
Compute controllability of the sensor network system according to the number of indexes the acquired information could answer and the weights of all kinds of information elements.

Figure 2. A Controllability Model

Suppose there are l_i kinds of operation requests for the $i-th$ kind of element, and the sensor network could answer $\rho_{ij}\ (j=1,2\ldots,l_i)$ indexes clearly and correctly among the m_i ones after making an analysis, so the probability that the sensor network could give a correct identification on this request is

$$\frac{\rho_{ij}}{m_i}+0.5\left(1-\frac{\rho_{ij}}{m_i}\right),\ (j=1,2\ldots,l_i).$$

$\frac{\rho_{ij}}{m_i}$ is the probability that the sensor network could make a correct identification with the help of the index information acquired through analysis. $0.5\left(1-\frac{\rho_{ij}}{m_i}\right)$ is the probability that the sensor network could make a correct identification with useless information, though they are yet acquired through analysis. So the probability that the sensor network could make a correct identification on all kinds of operation requests for $i-th$ element is

$$f_i=\sum_{j=0}^{l_i}\left(\frac{\rho_{ij}}{m_i}+\frac{1}{2}\left(1-\frac{\rho_{ij}}{m_i}\right)\right)p_{ij}=\frac{1}{2}\sum_{j=0}^{l_i}\left(\frac{\rho_{ij}}{m_i}+1\right)p_{ij}.$$

p_{ij} is the probability that the $j-th$ kind of operation request appears among all requests for the $i-th$ kind of elements.

A sensitive sensor network includes different kinds of elements and the flowing out of different information couldn’t produce the same degree of impact. For the confidential nets, which are physically isolated from the outside, controllability loss caused by the interaction of people and systems brings a higher risk, so a higher weight should be configured to this; while for general individual users, especially the ones followed by specific institutions, controllability loss caused by Trojan is of a higher risk, so it should be configured with a higher weight.

According to different levels of impact caused by the flowing out of different kinds of information, a corresponding weight is configured. Set the weight of the $i-th$ kind of element in the sensor network w_i $(i=1,2\cdots n$, $\sum_{i=1}^{n} w_i = 1)$ the controllability is denoted by P_{ctrl}

$$P_{ctrl} = \sum_{i=1}^{n} f_i w_i = \frac{1}{2}\sum_{i=1}^{n}\sum_{j=0}^{l_i}\left(\frac{\rho_{ij}}{m_i}+1\right)p_{ij}w_i$$

Example: Consider such a sensitive sensor network: all elements share the same nature of flowing out. In other words, there is only one kind of element ($n=1$). There are four kinds of operation request to this kind of element: browsing, copying, inserting and deleting ($l_1 = 4$). The sensor network sets 3 indexes ($m_1 = 3$). Try to compute the controllability of this sensitive information system.

Specific indexes are as follows:

Table 1. Specific Indexes for Controllability Quantization

	Yes (legal)	No (illegal)	Unable to determine
Address Legitimacy	Sensor network is able to get a user's real address and it is in the domain.	Sensor network is able to get a user's real address but it is outside the domain.	Sensor network can't obtain users' identities accurately.
Input Legitimacy	What input is consistent with the white list	What input is consistent with the black list	What input is not consistent with both black and white list
Token Legitimacy	Sensor network requires users to present a valid token and the key is the same as the one given by the server.	Sensor network requires users to present a valid token but the key given by a user is different with the one given by the server.	A token is not necessary, that is there is no need for tokens.

We can make the following what-if analysis:

The information acquired from the browsing request:

Table 2. Browsing Request

	Able to answer "Yes" or ”No"	Unable to determine

Address Legitimacy		√
Input Legitimacy		√
Token Legitimacy		√

In this case, the acquired information couldn't give any clear answer to the 3 indexes set by the sensor network, that is $\rho_{11}=0$. So the probability that the sensor network could make a correct identification on the legitimacy of this browsing request is:

$$\begin{aligned}&\frac{\rho_{ij}}{m_i}+0.5\left(1-\frac{\rho_{ij}}{m_i}\right)\\&=\frac{\rho_{11}}{m_1}+0.5\left(1-\frac{\rho_{11}}{m_1}\right)\\&=\frac{0}{3}+0.5\left(1-\frac{0}{3}\right)\\&=0.5\end{aligned}$$

The information acquired from the copying request:

Table 3. Copying Request-1

	Able to answer "Yes" or "No"	Unable to determine
Address Legitimacy	√	
Input Legitimacy		√
Token Legitimacy		√

Or

Table 4. Copying Request-2

	Able to answer "Yes" or "No"	Unable to determine
Address Legitimacy		√
Input Legitimacy	√	
Token Legitimacy		√

Or

Table 5. Copying Request-3

	Able to answer "Yes" or "No"	Unable to determine

Address Legitimacy		√
Input Legitimacy		√
Token Legitimacy	√	

In this case, the acquired information could give 1 clear answer to the 3 indexes set by the sensor network, that is $\rho_{12}=1$. So the probability that the sensor network could make a correct identification on the legitimacy of this copying request is:

$$\begin{aligned}\frac{\rho_{ij}}{m_i}+0.5\left(1-\frac{\rho_{ij}}{m_i}\right)&=\frac{\rho_{12}}{m_1}+0.5\left(1-\frac{\rho_{12}}{m_1}\right)\\&=\frac{1}{3}+0.5\left(1-\frac{1}{3}\right)\\&=\frac{2}{3}\end{aligned}$$

The information acquired from the inserting request:

Table 6. Inserting Request-1

	Able to answer “Yes” or ”No”	Unable to determine
Address Legitimacy		√
Input Legitimacy	√	
Token Legitimacy	√	

Or

Table 7. Inserting Request-2

	Able to answer “Yes” or ”No”	Unable to determine
Address Legitimacy	√	
Input Legitimacy		√
Token Legitimacy	√	

Or

Table 8. Inserting Request-3

	Able to answer “Yes” or ”No”	Unable to

		determine
Address Legitimacy	√	
Input Legitimacy	√	
Token Legitimacy		√

$$\begin{aligned}&\frac{\rho_{ij}}{m_i}+0.5\left(1-\frac{\rho_{ij}}{m_i}\right)\\&=\frac{\rho_{13}}{m_1}+0.5\left(1-\frac{\rho_{13}}{m_1}\right)\\&=\frac{2}{3}+0.5\left(1-\frac{2}{3}\right)\\&=\frac{5}{6}\end{aligned}$$

Table 9. Deleting Request

	Able to answer "Yes" or "No"	Unable to determine
Address Legitimacy	√	
Input Legitimacy	√	
Token Legitimacy	√	

In this case, the acquired information could give 3 clear answers to the 3 indexes set by the sensor network, that is $\rho_{14}=3$. So the probability that the sensor network could make a correct identification on the legitimacy of this deleting request is:

$$\begin{aligned}&=\frac{\rho_4}{m_1}+0.5\left(1-\frac{\rho_{14}}{m_1}\right)\\&=\frac{3}{3}+0.5\left(1-\frac{3}{3}\right)\\&=1\end{aligned}$$

The probabilities that each operation request appears are:

$$p_{1j}=\frac{1}{l_1}=\frac{1}{4},(j=1,2,3,4)$$

As there is only one kind of element in this sensor network, its weight is: $w_1=1$

$$
\begin{aligned}
&= \frac{1}{2}\sum_{i=1}^{n}\sum_{j=0}^{l_i}\left(\frac{\rho_{ij}}{m_i}+1\right)p_{ij}w_i \\
&= \frac{1}{2}\sum_{i=1}^{1}\sum_{j=1}^{4}\left(\frac{\rho_{ij}}{m_i}+1\right)p_{ij}w_i \\
P_{ctrl} = \sum_{i=1}^{n} f_i w_i &= \frac{1}{2}\sum_{j=1}^{4}\left(\frac{\rho_{1j}}{m1}+1\right)p_{1j}w_1 \\
&= \frac{1}{4}\left(0.5+\frac{2}{3}+\frac{5}{6}+1\right) \\
&= \frac{3}{4}
\end{aligned}
$$

Now let us consider the changes of controllability, when an element moves from one controllable region to another. Just as shown in Figure 3, element e moves from Set A to Set B via Path e_{AB}. So $C=\{e_{AB}\}\cup A\cup B$ is a new connected set. As a result, the corresponding controllable region has changed.

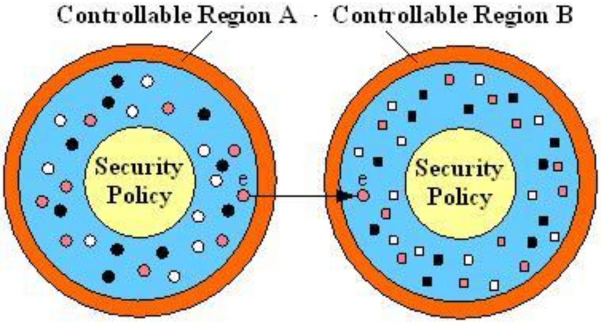

Figure 3. Expansion of Controllable Region

What should be noted is that the controllability of the sensitive sensor network is an inherent nature, which only depends on the logical structure of the sensor network and has nothing to do with the elements and the operation requests. What we have done is just making a rough quantification on the controllability with the help of elements and requests. According to this, we can draw the following conclusions: the controllability is still P_{ctrl_A} for controllable Region A though element e is flowing out; the controllability is still P_{ctrl_B} for controllable Region B though element e is flowing in; for the new controllable Region C, the controllability is. $P_{ctrl_C}=\min\{P_{ctrl_A},P_{ctrl_B}\}$

5. Conclusion

The connotation and denotation of information security are constantly deepened and expanded and the issue of information security has become increasingly prominent, thus leading to some undesirable outcomes, for example, the demarcation of virtual network space border and national physical border, the proliferation of pornographic information, the spread of malicious code, the violation of network personal privacy, the abuse of intellectual property, the cyber terrorism (including the network propagated psychological warfare on the battlefield of Internet) and other issues. With the development of sensor network and internet, the cyber world and the physical world is gradually fusing into a whole. Cyberspace security has become an international problem. The research on sensitive information system security model is being improved with the development of information security technology. Throughout the development of information security technology, we can see that the development of security practice always precede the development of the security model, resulting in the unparalleled of them two. That is to say there lack proper security model to guide the development of information security technology, especially in the cyberspace security where there is no recognized description. The description of cyberspace and information security and the three-dimension model PDRL that proposed by this paper, ensure the security of sensitive information in every phase of system lifecycle, and emphasize on the thought of seeking the system security assurance to the source of system development. Nowadays, quantitative description of the information security attributes using the concept of probability is a mainstream approach. However, security failures are usually caused by malicious attack, unlike random failures, it is hard to describe. As for the controllability attribute in PDRL security model, we proposed one probability calculation method and show how to calculate the controllability of sensor network as an example. Information security has been regarded as a dynamic process. How to dynamically portray the security attributes will be our next step.

ACKNOWLEDGMENTS

This work is supported by the following programs: the National Natural Science Foundation of China under Grant No.61170273; the China Scholarship Council under Grant No.[2013]3050; Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (NO. CAAC-ITRB-201201);2010 Information Security Program of China National Development and Reform Commission with the title “Testing Usability and Security of Network Service Software”.

References

[1] J. Symanzik, K. H. Choi, G. S. Mun and J. Y. Aen, “Sensitivity of Interview Chart for Medical Diagnoses of Primary Headaches”, International Journal of Innovative Computing, Information and Control, vol. 8, no.10(B), **(2012)**, pp.7133-7142.

[2] D. Bell and L.Padula, “Security Computing Systems: Mathematical Foundation and Model”, MITRE Report, Bedbord, MA, **(1975)**.

[3] K. J. Biba, “Integrity Considerations for Secure Computer Systems”, MTR-3153, The Mitre Corporation, **(1977)** April.

[4] D. D. Clark and D. R. Wilson, “A Comparison of Commercial and Military Computer Security Policies”, Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), Oakland, CA, IEEE Press, **(1987)** May, pp. 184–193.

[5] Y.-C. Hsiao and G.-H. Hwang, “Chinese Wall Security Model for Workflow Management System with Dynamic Security Policy”, Journal of Information Science and Engineering, **(2011)**.

[6] B. Y. C. J. R. McCumber and J. Staff, “Information System Security: A Comprehensive Model”, Proceedings 14th National Computer Security Conference, National Institute of Standards and Technology, **(1991)**.

[7] P. Wang, Y. Xiang and S. Zhang, “A Novel Reliability Assurance Method for Cyberphysical System Components Substitution”, International Journal of Distributed Sensor Networks, vol. 2012, Article ID 242654, **(2012)**.

[8] Y. Pan, Y. Yu and L. Yan, “An Improved Trust Model Based on Interactive Ant Algorithms and Its Applications in Wireless Sensor Networks”, International Journal of Distributed Sensor Networks, vol. 2013, Article ID 764064, **(2013)**.

[9] C. E. Shannon, “Communication in the Presence of Noise”, PROC IRE, **(1949)**.

[10] “U.S. Department of Defense Standard”, Department of Defense Trusted Computer System Evaluation Criteria(Orange Book), DoD 5200.28-STD, Library No. S225,711, **(1985)** December.

[11] “National Security Agency Information Assurance Solutions Technical Directors”, Information Assurance Technical Framework, Release 3.0, **(2000)** September.

[12] D. Denyer, E. Kutsch, E. Lee-Kelley and M. Hall, “Exploring reliability in information systems programmes”, International Journal of Project Management, vol. 29, Issue 4, **(2011)** May, pp. 442-454.

[13] J. P. G. Sterbenz, D. Hutchison, E. K. Cetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller and P. Smith, “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines”, The Journal of Computer Networks, Elsevier B.V., **(2010)**.

[14] “Department of Defense of United States”, Department of Defense Strategy for Operating in Cyberspace, **(2011)** July.

[15] B. X. Fang, Y. C. Guo and Y. Zhou, “Information content security on the Internet: the control model and its evaluation”, Science in China Series F: Information Sciences, vol. 53, Issue 1, **(2010)**, pp. 30-49.

[16] ISO/IEC International Standards (IS) 15408-1:1999, 15408-2:1999, and 15408-3:1999, “Common Criteria for Information Technology Security Evaluation: Part 1-Introduction and General Model, Part 2-Security Functional Requirements, and Part 3-Security Assurance Requirements”, CCIMB-99-031, CCIMB-99-032, and CCIMB-99-033, Version 2.1, **(1999)** August.

[17] National Security Agency, “The Information Systems Security Engineering Process”, Information Assurance Technical Framework, **(2002).**

[18] International Telecommunications Union, “Security Architecture for Open Systems Interconnection for CCITT Applications”, ITU X.800, **(1991)** March.

[19] M. E. Whitman and H. J. Mattord, “Principles of Information Security”, 4 edition, Course Technology-Cengage Learning, **(2011)** January.

[20] M. S. Fujii, “A comparison of software assurance methods”, Proceedings of the 1st Annual Software Quality Assurance Workshop on Functional and Performance Issues, ACM, New York, USA, **(1978)**, pp. 27-32.

[21] President’s Information Technology Advisory Committee, “Cyber Security: A Crisis of Prioritization”, Report to the President, published by the National Coordination Office for Information Technology Research and Development, **(2005)** February, http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[22] “National Science and Technology Council”, Federal Plan for Cyber Security and Information Assurance Research and Development, **(2006)**, http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf.

[23] “Committee on National Security Systems”, National Information Assurance (IA) Glossary, CNSS Instruction no. 4009, **(2006)** April.

[24] “National Defense Industrial Association System Assurance Committee”, Engineering for System Assurance, Version 1.0, Guidebook, NDIA, **(2008)** October, http://www.acq.osd.mil/sse/ssa/guidance.html.

[25] P. R. Croll, “Engineering for Systems Assurance - A State of the Practice Report”, Proceedings of 1st Annual IEEE System Conference, **(2007)** April, Waikiki Beach, Honolulu, Havaii, USA.

[26] “Department of Defense”, Information Assurance(IA), no. 8500.01E, **(2012)** October.

[27] D. B. Parker, “Fighting Computer Crime: A New Framework for Protecting Information”, ISBN:0471163783, Wiley Computer Publishing, **(1998)**, New York.

[28] S. Bosworth and M. E. Kabay, “Computer security handbook, Fourth Edition”, ISBN:978-0-471-26975-5, John Wiley & Sons, INC, **(2002)** October.

[29] W. Xianping, “Security Architecture for Sensitive Information Systems”, PHD Thesis, Monash University, **(2009)**.

[30] Y. Cherdantseva and J. Hilton, “A Reference Model of Information Assurance & Security”, Proceedings of Availability, Reliability and Security (ARES), IEEE, **(2013)** September, pp. 546-555.

[31] H. J. Kim, “Security and Vulnerability of SCADA Systems over IP-Based wireless Sensor Networks”, International Journal of Distributed Sensor Networks, vol. 2012, Article ID 268478, **(2012)**.

[32] M. R. Clarkson, “Quantification and Formalization Security”, A Dissertation Presented to the Faculty of the Graduate School of Cornell University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy, **(2010)** February.

[33] M. R. Clarkson and F. B. Schneider, “Quantification of Integrity”, Proceedings of 23rd IEEE Computer Security Foundations Symposium, ISBN: 978-0-7695-4082-5, **(2010)** July.

[34] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan and K. S. Trivedi, “A method for modeling and quantifying the security attributes of intrusion tolerant systems”, Performance Evaluation, vol. 56, **(2004)**, pp. 167–186.

[35] M. Enev, J. Jung, L. Bo, X. Ren and T. Kohno, “SensorSift: Balancing Sensor Data Privacy and Utility in Automated Face Understanding”, Proceedings of Annual Computer Security Applications Conference (ACSAC), **(2012)**, pp. 149-158.

[36] A. Kumar, “Using Automated Model Analysis for Reasoning about Security of Web Protocols”, Proceedings of Annual Computer Security Applications Conference (ACSAC), **(2012)**, pp. 289–298.

[37] N. Cai, J. Xi, Y. Zhong and H. Ma, “Controllability Improvement for Linear Time-Invariant Dynamical Multi-Agent Systems”, International Journal of Innovative Computing, Information and Control, vol. 8, no. 5(A), **(2012)** May, pp. 3315-3328.

[38] S. Whattam, “Situational Crime Prevention: Modern Society’s Trojan Horse”, International Journal of Criminology, **(2011)**.

Authors

Tian-Bo Lu, was born in Guizhou Province, China, 1977. He received his PH.D Degree in computer science from the Institute of Computing Technology of the Chinese Academy of Sciences in 2006. He is an Associate professor in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information security, computer network and Privacy Enhancing Technologies.

Xiaobo Guo, born in Hebei Province, China, 1990. She is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her technical interests include Cyber-Physical System and Privacy Enhancing Technologies .

Ling-Ling Zhao, is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her technical interests include Cyber-Physical System and P2P network.

Yang Li, was born in Hunan Province, China, 1978. He is a PhD and his technical interests include information security, distributed computing and P2P network.

Peng Lin, is a professor in Beijing University of Posts and Telecommunications, China. His technical interests include computer network and cyber security.

Binxing Fang, is an academician of china engineering academy, a professor in Beijing University of Posts and Telecommunications, China. His technical interests include computer network, cyber security and Privacy Enhancing Technologies.