International Journal of Multimedia and Ubiquitous Engineering
Vol. 2, No. 2, April, 2007

IT Security Review: Privacy, Protection, Access Control, Assurance and System Security

Sattarova Feruza Y. and Prof.Tao-hoon Kim

Hannam University, Department of Multimedia Engineering, 306 791
mymail6585@gmail.com, taihoonn@empal.com

Abstract

Computer security is a branch of technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. There are many elements that are disrupting computer security. In this paper, we review the current strategies and methods related to IT security.

Keywords: *IT Security, Privacy, Access Control, Information Assurance*

1. Introduction

Information Systems are decomposed in three main portions, hardware, software and communications with the purpose to identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: Physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators)how to use products to ensure information security within the organizations.[2] In the following sections of this paper, we review elements related to IT security and finally we review the current technologies related to IT Security

2. IT Security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.[1]

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

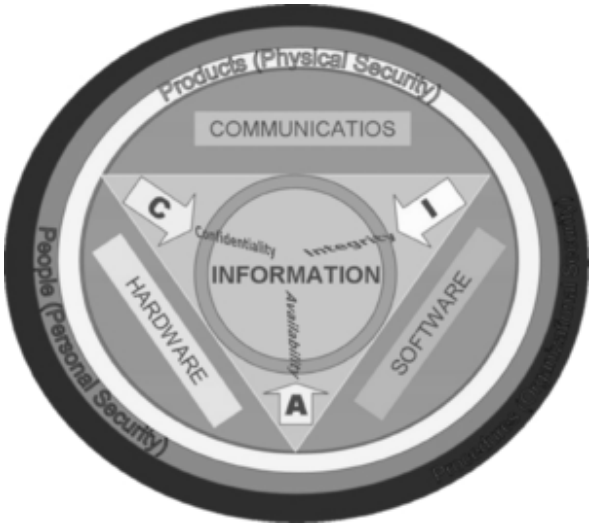

Figure 1. Information Security Components: or qualities, Confidentiality, Integrity and Availability (CIA).

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of gaining entry into the field. It offers many areas for specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, to name a few. This article presents a general review of information security and its core concepts.

3. Basic Principles

3.1 Key concepts

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) as the core principles of information security. Many information security professionals firmly believe that Accountability should be added as a core principle of information security.

3.2 Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

3.3 Integrity

In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mis-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

3.4 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware

failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

3.5 Authenticity

In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

3.6 Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

3.7 Risk management

A comprehensive treatment of the topic of risk management is beyond the scope of this article. We will however, provide a useful definition of risk management, outline a commonly used process for risk management, and define some basic terminology.

The CISA Review Manual 2006 provides the following definition of risk management: "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."[2]

There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerability emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man made or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of

information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called residual risk.

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis. The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

- security policy,
- organization of information security,
- asset management,
- human resources security,
- physical and environmental security,
- communications and operations management,
- access control,
- information systems acquisition, development and maintenance,
- information security incident management,
- business continuity management, and
- regulatory compliance.

4. Controls

When Management chooses to mitigate a risk, they will do so by implementing one or more of three different types of controls.

4.1 Administrative controls

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed - the Payment Card Industry (PCI) Data Security Standard required by Visa and Master Card is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

4.2 Logical controls

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read Email and surf the Web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

4.3 Physical controls

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

An important physical control that is frequently overlooked is the separation of duties. Separation of duties ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator - these roles and responsibilities must be separated from one another.[3]

5. Cryptography

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.[4]

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure application such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using the WPA or WEP protocols. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GNUPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. PKI solutions address many of the problems that surround key management.

6. Informational Privacy

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data is collected, stored, and associated. In other cases the issue is who is given access to information. Other issues include whether an individual has any ownership rights to data about them, and/or the right to view, verify, and challenge that information.

Various types of personal information often come under privacy concerns. For various reasons, individuals may not wish for personal information such as their religion, sexual orientation, political affiliations, or personal activities to be revealed. This may be to avoid discrimination, personal embarrassment, or damage to one's professional reputation.

Financial privacy, in which information about a person's financial transactions is guarded, is important for the avoidance of fraud or identity theft. Information about a person's purchases can also reveal a great deal about that person's history, such as places they have visited, whom they have had contact with, products they use, their activities and habits, or medications they have used.

Internet privacy is the ability to control what information one reveals about oneself over the Internet, and to control who can access that information. These concerns include whether email can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited collect, store, and possibly share personally identifiable information about users.

Medical privacy allows a person to keep their medical records from being revealed to others. This may be because they have concern that it might affect their insurance coverage or employment. Or it may be because they would not wish for others to know

about medical or psychological conditions or treatment which would be embarrassing. Revealing medical data could also reveal other details about one's personal life (such as about one's sexual activity for example).

Sexual privacy prevents a person from being forced to carry a pregnancy to term and enables individuals to acquire and use contraceptives and safe sex supplies and information without community or legal review.

Political privacy has been a concern since voting systems emerged in ancient times. The secret ballot is the simplest and most widespread measure to ensure that political views are not known to anyone other than the original voter — it is nearly universal in modern democracy, and considered a basic right of citizenship. In fact even where other rights of privacy do not exist, this type of privacy very often does.

7. Protection: Defense in depth

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its life time, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defence in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in- depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people as the outer layer of the onion, and network security, host-based security and application security forming the inner layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

8. Access Control

Access control is the traditional center of gravity of computer security. It is where security engineering meets computer science. Its function is to control which principals (persons, processes, machines, etc) have access to which resources in the system which files they can read, which programs they can execute, how they share data with other principals, and so on. Access control works at a number of levels, as shown in Figure 2, and described in the following:

1. The access control mechanisms, which the user sees at the application level, may express a very rich and complex security policy. A modern online business could assign staff to one of dozens of different roles, each of which could initiate some subset of several hundred possible transactions in the system. Some of these (such as credit card transactions with customers) might require online authorization from a third party while others (such as refunds) might require dual control.
2. The applications may be written on top of middleware, such as a database management system or bookkeeping package, which enforces a number of protection properties. For example, bookkeeping software may ensure that a transaction that debits one ledger for a certain amount must credit another ledger for the same amount.
3. The middleware will use facilities provided by the underlying operating system. As this constructs resources such as files and communications ports from lower-level components, it acquires the responsibility for providing ways to control access to them.
4. Finally, the operating system access controls will usually rely on hardware features provided by the processor or by associated memory management hardware. These control which memory addresses a given process can access.

As we work up from the hardware through the operating system and middleware to the application layer, the controls become progressively more complex and less reliable. Most actual computer frauds involve staff accidentally discovering features of the application code that they can exploit in an opportunistic way, or just abusing features of the application that they were trusted not to. But in this chapter, we will focus on the fundamentals: access control at the hardware and operating system level.

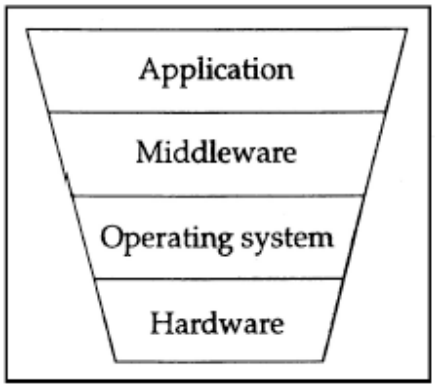

Figure 2. Access controls at different levels in a system.

As with the other building blocks discussed so far, access control makes sense only in the context of a protection goal, typically expressed as a security policy. This puts us at a slight disadvantage when discussing PCs running single-user operating systems such as DOS and Win95/98, which have no overt security policy: any process can modify any data. People do have implicit protection goals, though; you don’t expect a shrink-wrap program to trash your hard disk. So an explicit security policy

is a good idea, especially when products support some features that appear to provide protection, such as login IDs. [6]

9. Current Technologies Related to IT Security

9.1 Key Management Systems for Multilevel Security

Secret data should be managed for access to authorized people only. In order to do so, secret keys must be distributed solely to those with access to the pertaining information. However, this is not a simple problem to solve. [7]

9.1.1 KMS Using a One-Way (Cryptographic) Hash Function. Since Akl and Taylor's KMS for multilevel security uses exponentiation, the overload of computation of keys is high. However, we can compute keys faster than Akl and Taylor's method as shown below if we use a one-way hash function.

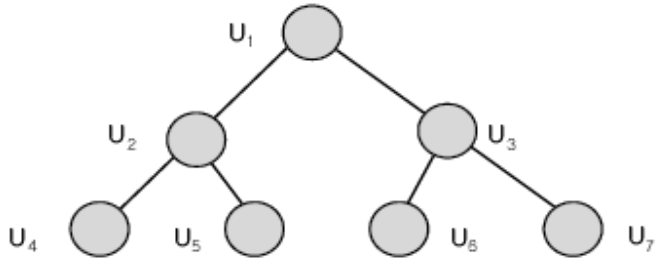

Figure 2. A lower tree

Once again, if there is no top class, we add a top class. Then the CA assigns a name to each class as in Fig. 2. Note that, in a lower tree, there is a unique class, denoted by *c(Uk)*, which covers a class *Uk* of a lower tree with top class

Table 1. Distribution of multilevel security keys for a lower tree using a hash function

Class	Keys
U_1	$K_{U_1} = K$
U_2	$K_{U_2} = H(U_2, K_{U_1})$
U_3	$K_{U_3} = H(U_3, K_{U_1})$
U_4	$K_{U_4} = H(U_4, K_{U_2})$
U_5	$K_{U_5} = H(U_5, K_{U_2})$
U_6	$K_{U_6} = H(U_6, K_{U_3})$
U_7	$K_{U_7} = H(U_7, K_{U_3})$

Now the *CA* selects a key *K* belonging to the top class and a one-way hash function *H*. The *CA* computes *KUk = H(Uk,Kc(Uk))* and distributes it together with *H* to each class *Uk*.

Then the users in an upper class can compute all keys belonging to the classes lower than theirs using their keys, hash function *H*, and names of lower classes. (See Table 1.) Because of the one-wayness of the hash function, a user in *Uk* can not compute others' keys belonging to upper classes.

9.2 Cooperative Security Management Enhancing Survivability Against DDoS Attacks

Mechanisms to Enhance Survivability are in two categories. One for intra-domain, and the other is for inter-domain.[8]

9.2.1 Management within a Domain. Since the number of network nodes is confined in a domain, it is relatively easy to treat DoS attacks. Therefore, it is necessary to monitor outbound traffics generated in a domain. The objectives of the monitoring are to detect abnormal outbound traffic flows and to provide essential services in the domain with enough bandwidth. A domain manager collects packet headers periodically. From this information, it can detect IP spoofing and service port access violation. Statistics based on traffic flows also can be obtain in the process.

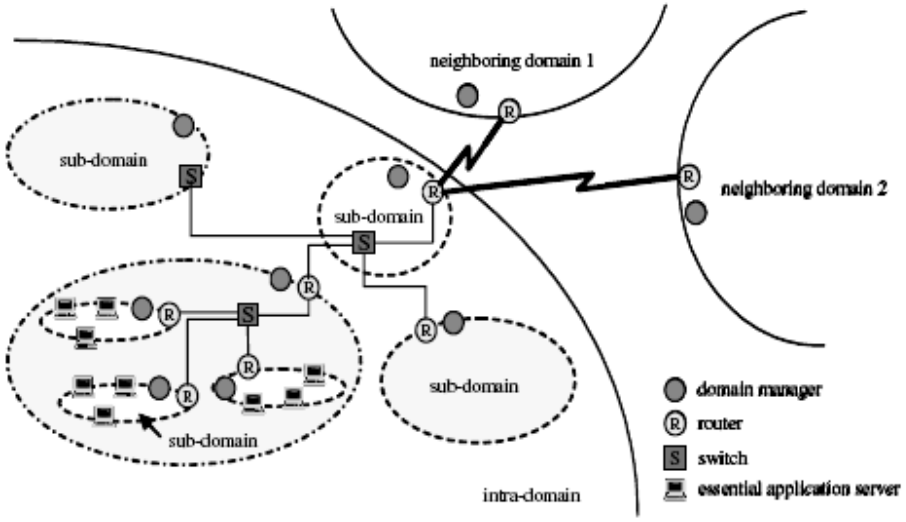

Figure 3. Intra-Domain Architecture

9.2.2 Inter-domain Cooperative Management. Inter-domain cooperation should be based on trust. Messages exchanged among domain managers are authenticated. In order not to be revealed to any attacker, the messages are encrypted and handled by the domain managers. For this purpose, domain managers conduct inbound traffic monitoring. It is to detect abnormal traffics and to control bandwidth for essential services. There are two types of messages exchanged among domain managers. One is the pushback message to cut off the traffic toward a certain victim node. The other is the feedback message. The feedback message is to increase the survivability as much as possible. Once an attack is controlled successfully by the virtue of the pushback message, the domain manager issues the feedback message back to the origin

of the pushback message. Other domain managers receiving the feedback message cease the rate limit and return to the status before the corresponding pushback message was generated.

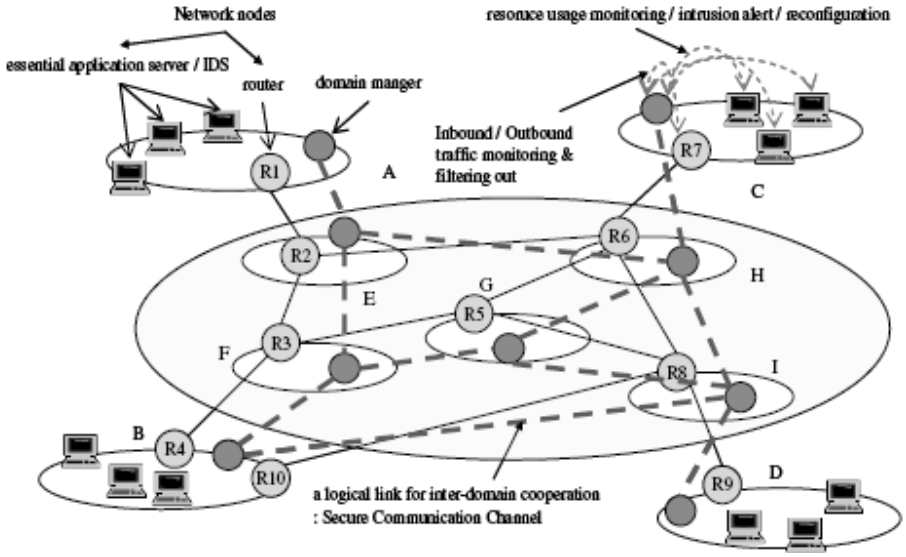

Figure 4. Inter-Domain Architecture

9.3 Frameworks for Assuring Security in Components

CSA(Component Security Assurance provides a schematic representation of the some inter models such as component security requirements model, assuring security model and modeling component security assurance. It shows the relationship between e-business domain and security model-based framework. Component domain requirements, security requirements model and CBD workbench/security architecture model apply in this paper context in any of the delivery tracks.

However, as we'll see a little later, de-scoping may occur at regular points through the lifecycle, resulting in hybrid projects. So, for example, a solution assembly project could branch into separate smaller assembly, provisioning and integration projects. Also software requirements techniques may also be used within a e-business domain services. They are especially useful in conjunction with prototyping, as a means of scouting ahead to explore different designs.

9.3.1 Component Security Requirement Model. One of the most important aspects of any security architecture model is the ability to manage/maintain an accurate and consistent level of component security controls. An integrated risk management program is critical in securing business objectives requiring the enforcement of confidentiality, integrity, availability, and accountability.

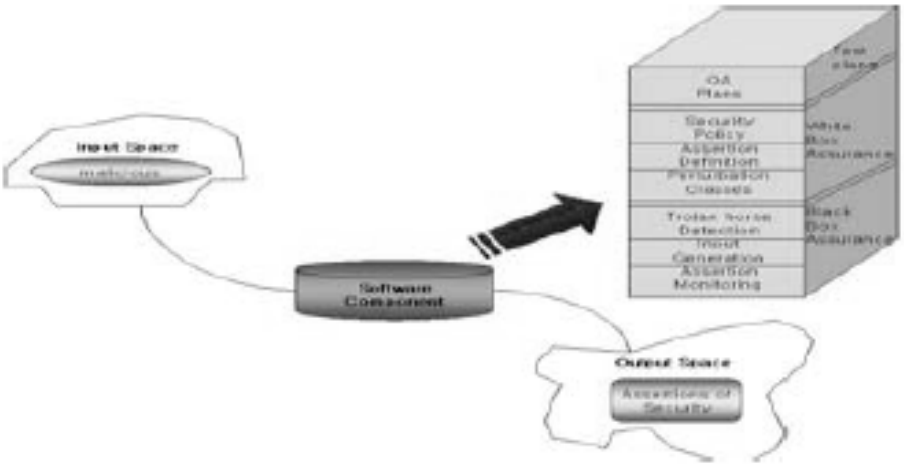

Figure 5. Component Security Assuring Dimension

Confidentiality ensures the protection of component from unauthorized access throughout an organization's information architecture, which extends to all component directly associated with the architecture's applications, component stores, communication links and/or processes. Integrity ensures that component, services, and other controlled resources are not altered and/or destroyed in an unauthorized manner. Integrity based controls provide safeguards against accidental, unauthorized, or malicious actions that could result in the alteration of security protection mechanisms, security classification levels, addressing or routing information, and/or audit information. Because of increasing information sharing and the cost of securing information, it is important to classify information correctly. Under-classification of sensitive information can have serious consequences.

The security requirements for each classification level are defined, based on the organization's particular application of the technology. The model includes categories for security, and the criteria by which the information is to be secured. Categories relate to both business processes (applications and component) and information technologies (hardware, software and services) that support that environment. The categories define a comprehensive structure for IT risk management issues and represent the components of the information systems environment.

9.3.2 Assuring Security Model in Component. The proposed approach for assuring security in components is illustrated by the Component Security Assurance (CSA) dimension as in Figure 5. The CSA dimension is an architecture for providing security-oriented testing processes to a software component. The dimension consists of several processes including the construction of test plans, analysis using white- box testing techniques, black-box testing techniques, and the stamping with a digital signature of the relative security rating based on the metrics evaluated through the testing. The processes are broken out into sub-pipes of test plans, white-box testing, and black-box testing. The first stage to component certification is the development of a test plan. The application in which the JavaBean component will be used will influence the security policy, test suites, assertions, and fault perturbations used in both whitebox and black-box testing processes.

Based on the security policy, input generation will make use of test suites delivered from the applicant for certification as well as malicious inputs d signed to violate the security policy. The definition of the security policy is used to code security assertions that dynamically monitor component vulnerability during security analyses. Finally, perturbation classes are generated for white-box fault injection analysis according to the application in which the component will be used.

9.4 Privacy Protection Model for ID Management System

9.4.1 Identity Management Privacy Protection (IDMP) Model. Privacy-enhancing technologies usually use purpose or policy to keep privacy that is set by users. For example, a P3P policy describes a website's privacy practices. When users and webservers want to maintain privacy, they automatically exchange policies in P3P. In the same way, the main purpose of privacy policies is to maintain privacy of IMS.

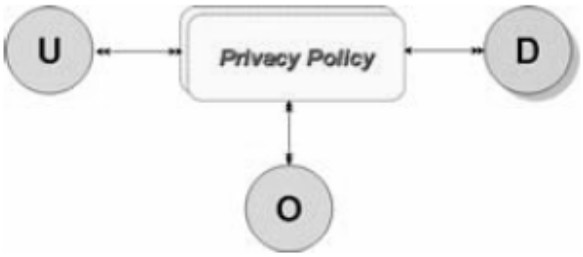

Figure 6. IDMP Basic Concept

In IMS, privacy policies are merely divided into information permission policy and information request policy. Figure 6 shows that only users can access objects (personal information) when information permission policy and information request policy are agreed on properly.

10. Conclusion

The protection of data (information security) is the most important. The protection of networks is important to prevent loss of server resources as well as to protect the network from being used for illegal purposes. The protection of computing power is relevant only to expensive machines such as large supercomputers. In this paper, we review the elements regarding IT security. We also review the current technologies related to IT security.

References

[1] U.S. Code collection http://www.law.cornell.edu/uscode/44/3542.html
[2] Wikepedia – IT Security http://en.wikipedia.org/wiki/Information_security
[3]"Segregation of Duties Control matrix". ISACA http://www.isaca.org/AMTemplate.cfm?Section=CISA1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=40835
[4] Wikepedia – Cryptgraphy http://en.wikipedia.org/wiki/Cryptography
[5] Wikepedia – Informational Privacy http://en.wikipedia.org/wiki/Privacy

[6] Security Engineering: A Guide to Building Dependable Distributed Systems
http://www.cl.cam.ac.uk/~rja14/Papers/SE-04.pdf
[7] Hwankoo Kim, Bongjoo Park, JaeCheol Ha, Byoungcheon Lee, DongGook Park, "New Key Management Systems for Multilevel Security", O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481
[8] Sung Ki Kim, Byoung Joon Min, Jin Chul Jung, and Seung Hwan Yoo, "Cooperative Security Management Enhancing Survivability Against DDoS Attacks", O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481
[9] Gu-Beom Jeong and Guk-Boh Kim, "A Framework for Security Assurance in Component Based Development" , O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481
[10] Hyang-Chang Choi, Yong-Hoon Yi, Jae-Hyun Seo, Bong-Nam Noh, and Hyung-Hyo Lee, "A Privacy Protection Model in ID Management Using Access Control", O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481