Using Information Technology Security to Protect the Network Models

Abeer Salim Jamil
Al- Mansour University College

Huda A. Alle AlAmwee
Al - Mustanserah University

Abstract :

This paper discuss how to use the principles of information technology security with models , the principles of information security : confidentiality , integrity , availability, accountability, and assurance are used to protection of information systems against unauthorized access to or modification of information, whether in storage , processing or transit, and against the denial of service to authorized users or provision of service to authorized users, including those measures necessary to detects , document and counter such threats .

This paper present how can implement the principles of information technology security on the Network Model (Intranet models) and we make the analysis the result and conclude this principles is very important to increase the protection of models in net.

1-Introduction [1, 2]

Information security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated 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. the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. Information security covers not just information but all infrastructures that facilitate its use processes, systems, services, technology.

2- Security Goal and Objectives [2,3,4,5]

v Security Goal

The goal of information technology security is to enable an organization to meet all of its mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners and customers.

v Security Objectives

The security goal can be met through the following security objectives:

A. Availability (of systems and data for intended use only)

Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users. This objective protects against:

1• Intentional or accidental attempts to either:

− perform unauthorized deletion of data or

− otherwise cause a denial of service or data.

2• Attempts to use system or data for unauthorized purposes.

Availability is frequently an organization's foremost security objective.

B. Integrity (of system and data)

Integrity has two facets:

1• Data integrity (the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit) or

2• System integrity (the quality that a system has when performing the intended function in an Unimpaired manner, free from unauthorized manipulation).

Integrity is commonly an organization's most important security objective after availability

C. Confidentiality (of data and system information)

Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.

For many organizations, confidentiality is frequently behind availability and integrity in terms of importance. Yet for some systems and for specific types of data in most systems (e.g., authenticators), confidentiality is extremely important.

D. Accountability (to the individual level)

Accountability is the requirement that actions of an entity may be traced uniquely to that entity. Accountability is often an organizational policy requirement and directly supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

E. Assurance

Assurance is the basis for confidence that the security measures, both technical and operational, work as intended to protect the system and the information it processes. The other four security objectives (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation when:

• required functionality is present and correctly implemented.

• there is sufficient protection against unintentional errors (by users or software),

and

• there is sufficient resistance to intentional penetration o r by - pass.

Assurance is essential; without it the other objectives are not met. However, assurance is a continuum; the amount of assurance needed varies between systems.

3.Security Objective Inter- dependencies [4,5,6,7]

The five security objectives are interdependent. Achieving one objective without consideration of the others is seldom possible. This is depicted in Figure (1) [5] and discussed below.

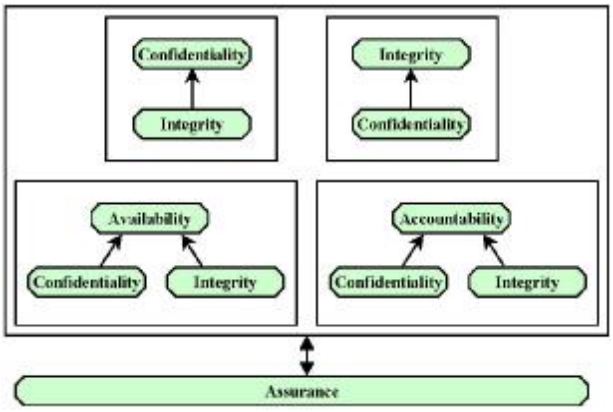

Figure (1) Security Objective Dependencies

A-Confidentiality is dependent on Integrity, in that if the integrity of the system is lost, then there is no longer a reasonable expectation that the confidentiality mechanisms are still valid.

B-Integrity is dependent on Confidentiality, in that if the confidentiality of certain information is lost (e.g., the super user password), then the integrity mechanisms are likely to be by-passed.

C-Availability and Accountability are dependent on Confidentiality and Integrity, in that:

• if confidentiality is lost for certain information (e.g., super user password), the mechanisms implementing these objectives are easily by passable; and

• if system integrity is lost, then confidence in the validity of the mechanisms implementing these objectives is also lost.

All of these objectives are interdependent with Assurance. When designing a system, an architect or engineer establishes an assurance level as a target. This target is achieved by both defining and meeting the functionality requirements in each of the other four objectives and doing so with sufficient 'quality'. Assurance highlights the fact that for a system to be secure, it must not only provide the intended functionality, but also ensure that undesired actions do not occur.

4. Security Model [6,7,8,9]

The technical security model is depicted in Figure (2)[4] which shows the primary services and supporting elements used in implementing an information technology security capability, along with their primary relationships. The model also classifies the services according to their primary purpose as follows:

A-Support:- These services are generic and underlie most information technology security capabilities. The supporting services are :-

1. Densification (and naming):- This service provides the capability to uniquely identify users, processes, and information resources.

2. Cryptographic key management Cryptographic keys must be securely

managed when cryptographic functions are implemented in various other services.

3. Security administration The security features of the system need to be administered in order to meet the needs of a specific installation and to account for changes in the operational environment.

4. A system protection underlying the various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from both the perspective of the design processes used and the manner in which the implementation was accomplished. Some examples of system protections are: residual information protection (also known as object reuse), least privilege, process separation, modularity, layering, and minimization of what needs to be trusted.

B-Prevent:- These services focus on preventing a security breach from occurring .

1. Protected communications In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications service ensures the integrity, availability, and confidentiality of information while in transit. In most situations all three elements are essential requirements, with confidentiality being needed at least for authentication information.

2. Authentication Ensuring that a claimed identity is valid is extremely important. The

authentication service provides the means to verify the identity of a subject.

3.Authorization The authorization service enables specification and subsequent management of the allowed actions for a given system.

4. Access control enforcement when the subject requesting access has been validated for access to particular processes, enforcing the defined security policy s still necessary. The access control enforcement service provides this enforcement, and frequently the enforcement mechanisms are distributed throughout the system. It is not only the correctness of the access control decision, but also the strength of the access control enforcement that determines the level of security obtained.

Checking identity and requested access against access control lists is a common access control enforcement mechanism. File encryption is another example of an access control enforcement mechanism.

5. Non-repudiation System accountability depends upon the ability to ensure that senders cannot deny sending information and that receiver cannot deny receiving it. Non-repudiation is a service that spans prevention and detection. This service has been placed into the prevention category because the mechanisms implemented prevent the ability to successfully repudiate an action. As a result, this service is typically performed at the point of transmission or reception. .

6. Transaction privacy Both government and private systems are increasingly required to maintain the privacy of individuals using these systems. The transaction privacy service protects against loss of privacy with respect to transactions being performed by an individual.

C-<u>Recover:-</u> The services in this category focus on the detection and recovery from a security breach.

1. <u>Audit</u> The auditing of security relevant events is a key element for after-the-fact detection of and recovery from security breaches.

2. Intrusion detection and containment A Detecting insecure situation is essential in order to respond in a timely manner. Also, detecting a security breach is of little use if no effective response can be initiated. The intrusion detection and containment service provides these two capabilities.

3. Proof of Wholeness In order to determine that integrity has been compromised, the ability must exist to detect when information or system state is potentially corrupted. The proof of wholeness service provides this ability.

4. Restore 'secure' state when a security breach occurs, the system must be able to return to a state that is known to be secure. That is the purpose for this service.

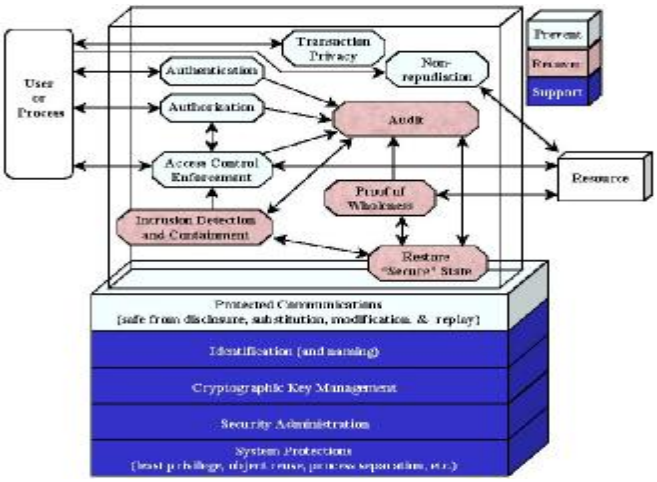

Figure (2) Security Model

The primary availability services are those that directly impact the ability of the system to maintain operational effectiveness. One aspect of maintaining effectiveness is protection from unauthorized changes or deletions by defining

authorized access and enforcing this definition. Mission effectiveness is also maintained by detecting intrusions, detecting a loss of wholeness, and providing the means of returning to a secure state. Show the Figure (3).[8]

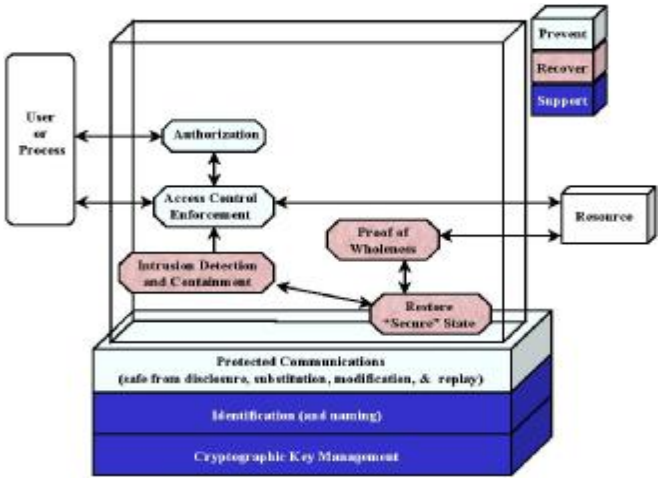

Figure (3) Primary Availability

The services that provide for availability also provide for integrity. This is because maintaining or restoring integrity is an essential part of maintaining availability. Although availability is only concerned with changes (or deletions) that impact mission availability, the practical reality is that the applicable security mechanisms do not differentiate between purposes for the unauthorized access nor between impacts of loss of wholeness. Show the Figure(4).

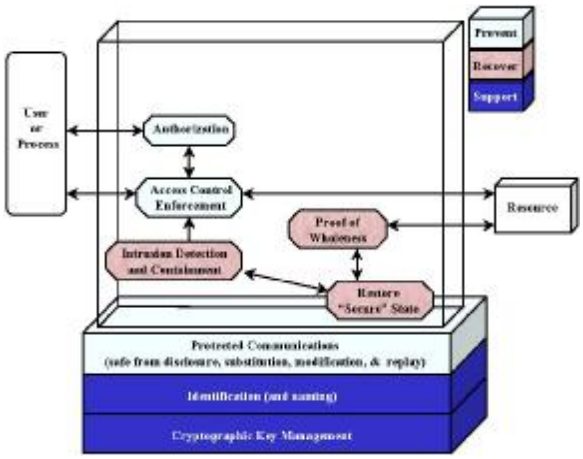

Figure (4) Primary Integrity Services

Once lost, confidentiality cannot be restored. Therefore, the detection and recovery services that can play an important role in maintaining availability and

integrity do not apply to confidentiality. The protection of communications from disclosure, the enforcement of authorized read accesses, and the capability for privacy provide for confidentiality. Show the Figure(5).

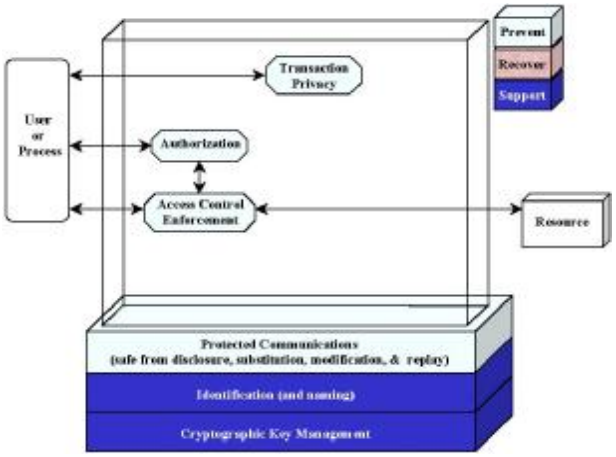

Figure (5) Primary Confidentiality Services

Maintaining accountability for user actions is performed primarily by the audit and non-repudiation services. Access control enforcement is also included as the primary generator of records of user actions.
Show the Figure(6).

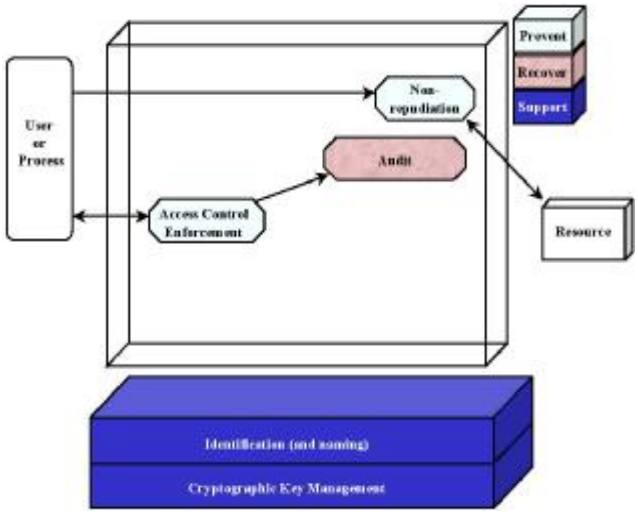

Figure (6) Primary accountability Services

Assurance is grounds for confidence that the security objectives are met and, encompasses both correct and sufficient security capabilities. Show the Figure(7).

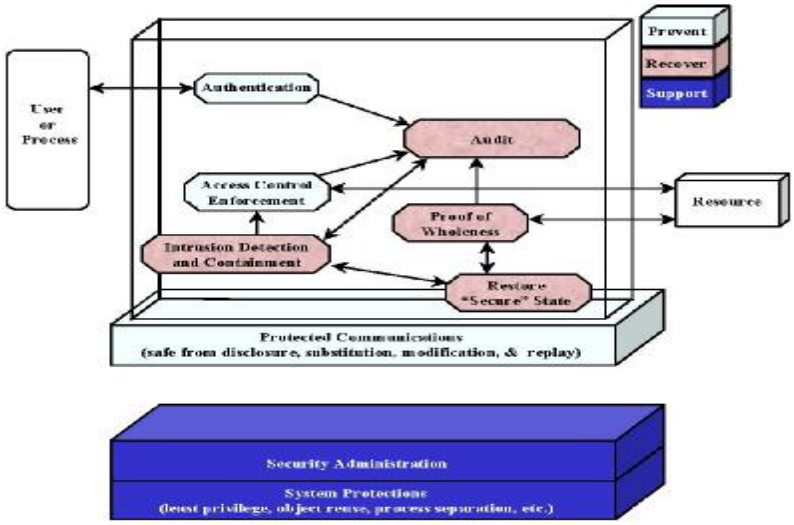

Figure (7) Primary Assurance Services

5. Proposal using Information Technology Security

This paper suggests applying the principles of information security with model to calculate the degree of security model, this is explaining in the general algorithm:

Step 1 : Input Model.

Step 2 : Availability method Implementation to check the system and data are work.

Step 3 : Integrity method Implementation to check the system and data are not change by unauthorized .

Step 4 : Confidentiality method Implementation after applied the availability and integrity methods , Confidentiality protection applies to data in storage during processing.

Step 5 : Accountability method Implementation.

Step 6 : Assurance method Calculation.

Step 7 : Analysis Results and Display the degree of security model.

Step 8 : End.

An important advantage of applying the principles of Information Technology to fond the degree of security of model , then the result is a good guide to show the relation between the principles of IT (Information Technology) and models .

6. Execution Information Technology Security

In Figure (8), the principles of information technology security applied on the network model to determine the degree of security of models and show the relation between information technology security and network models, then discuss and display the result . This operation involves performing the following tasks:-

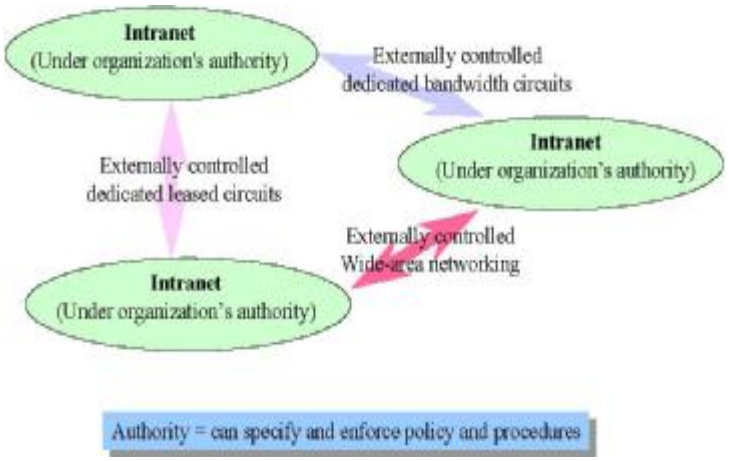

Figure (8) Network Model (Intranet)

1. Build Data

In this step the network models should be design and the principles of information technology security should be specified before the operation is begin.

2. Execute the principles of information Technology Security

There are many methods of principles of information technology security an over the network model. These methods are :-

1- Availability method.

2- Integrity method.

3- Confidentiality method.

4- Accountability method.

5- Assurance method .

3. Analysis the Result

After ending from application process of the information security technology principle at the net work models, the result must have been analyzed, so it will observe that relation between the technology principle of information security & network models , whereas not allowed of access to these information or make any modifying on theses movable or storage info.

For unauthorized at the net. So that has been reached these important principles to increase the activity on info. Production & gave a high level of security to the models at this networks. The executing of principles information technology on the network models (intranet) are illustrated in Figure (9) :-

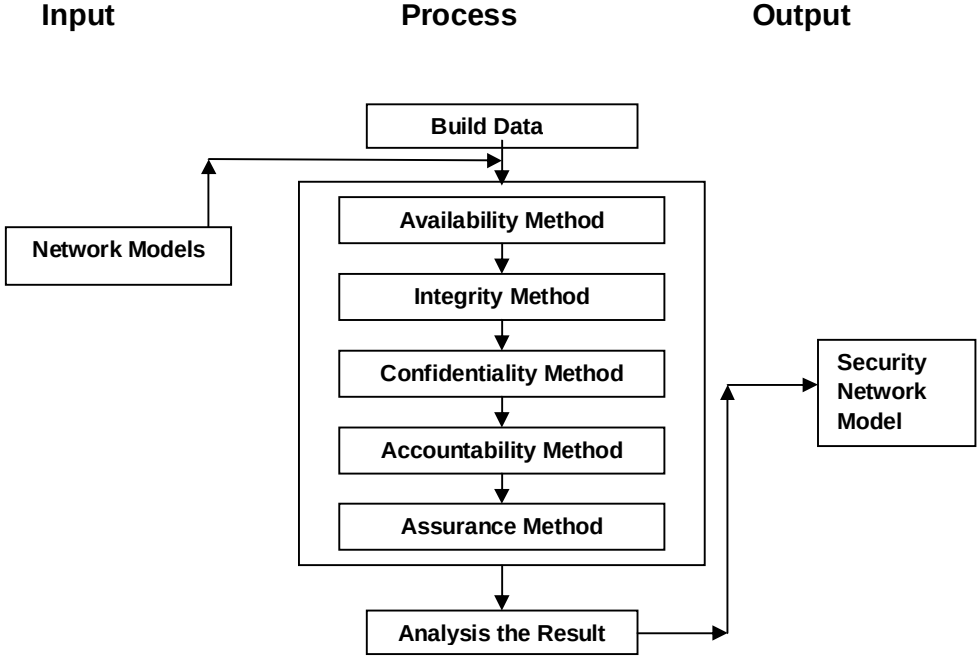

Figure (9) Diagram Execution of apply Principles information

Technology Security on Network Models

7. Conclusion

when the technology principle applied theory of information security , a network models (intranet) it noticed that principles have a relationship between each ether that the confidently can not apply before getting integrity & availability, after the end of each of them , it will achieve confidently & then we can make accountability that leading as to make the Assurance which make it in case of getting availability , integrity, confidently & Accountability , on these way , making the full security to the information witch be special by model & also not allowed the unauthorized to reach or modifying the moveable storage information in the network, as well as giving the complete availability for authorized reaching the information and making the necessary modify, these process makes the complete security to information and upraise high level of information security to net .

8. Reference

[1] Cobit Guidelines, 'Information Security Audit and Control Association", 2000.

[2] C. Stacey Sawyer , k. Briank Williams , " *Using Information Technology* ",

MC- Graw –Hill, USA, 2001.

[3] J. Yoder and J. Barcalow, "Architectural patterns for enabling application security", 2001.

Available at : http://jerry.cs.uiuc.edu/~plop

[4] Layton , Timothy P. , " Information Security :Design ,Implementation,, Measurement and Compliance ", USA , 2007.

[5] M. Leonard Jessup, S. Joseph Valacich, "Information Systems Today", Prentice Hall , UAS , 2003

[6] N. Harrison, B. Foote, and H. Rohnert, Eds , "Pattern Languages of Program Design and Security", Addison-Wesley, 2000.

[7] Peltier , Thomas R . " Information Security Risk Analysis ", USA, 2001

[8]Peltier, Thomas R. ," Information Security Policies, Procedures, and Standards: guidelines for effective information security management", USA, 2002.

[9] Turban E., Rainer R. Kelly, E. Richard Potter, "Introduction to Information Technology", Second Edition, Jon Wiley &Sons, Inc, USA, 2003.

استخدام امنية تكنولوجيا المعلومات لحماية نماذج الشبكة

م. عبير سالم جميل
كلية المنصور الجامعة

م.م. هدى عبد العال
الجامعة المستنصرية

المستخلص :

نناقش في هذا البحث كيفية استخدام اسس تكنولوجيا امنية المعلومات مع النماذج وهذه الاسس تتمثل بـ (السريّة، السلامة، توفير البيانات، المسؤولية،التأمين) حيث انها تستخدم لحماية المعلومات من الاختراق من قبل الغير مخولين في الوصول الى المعلومات وخاصة المعلومات المخزونة او القابلة للتنقل عبرالشبكة وايضا تم حماية المعلومات من الغير المخولين من اجراء التعديلات على الملفات الخاصة بالنموذج عبر الشبكة , مما يؤدي في هذه الحالة الى السرية الكاملة لجميع المعلومات الموجودة ضمن النموذج ويسمح فقط للمخولين من الوصول الى المعلومات الخاصة بالنموذج واجراء التعديلات اللازمة على النموذج عبر الشبكة .

في هذا البحث سوف نقوم بتنفيذ اسس تكنولوجيا امنية المعلومات على Network Model (Intranet) وبعدها نقوم بعملية تحليل النتائج والوصول الى ان هذه الاسس مهمة جدا لزيادة في حماية المعلومات واعطاء درجة عالية من الامنية لـ Network Model عبر الشبكة .