Standardization and Security in Network Based Information System

Dr. Kuntalkumar P. Patel
Lecturer, Institute of Technology
Nirma University, Ahmedabad – 382481, Gujarat, India.
E-mail: kuntal_78@yahoo.com

ABSTRACT

The success of today's business in competitive world depends on how successfully and effectively they are using networked based information system. Such information systems are used with the main objective to make "paper-less office". Also, use of the Internet becomes more central among such networked based information system in governmental agencies, corporate businesses and among individuals. To stay safe over the network lots of national and international level standards are available giving guidelines for network security improvement, in this paper how one can accept and use such standards for improving network security is discussed. Also, with the procedure for standards implementation, general security improvement guidelines are given in this paper.

I. Role of Network Based Information System for Today's Businesses

The success of businesses today and in future depends on their capability to operate globally. The business environment gets changed because of globalization. The businesses have to provide global delivery systems for their products and services to their customers or business partners. They have to maintain their products and services standards in world market competition.

An Information system can be defined technically as a set of interrelated components that collect, process, store, and distribute information to support decision making and control in an organization. In addition to supporting decision making, coordination and control, information system may also help to the managers and workers to analyze the problems.

Use of the Information System is the way that provides power to the businesses for conducting trade and managing businesses on a global market. Controlling the global corporation, communicating with dealer and distributors, operating 24 hours and 7 days a week in different nations, servicing local and global reporting needs – is a major business challenge that requires powerful use of Information System.

From the business point of view information system can be defined as series of activities for acquiring, transforming and distributing information that mangers can use to improve decision making, enhance organizational performance, and ultimately increase profit of the business.

Today's information system used by the organizations becomes more powerful and productive because of computer network technology. Through special communication and information technology standards, any computer can communicate with any other computers connected to the computer network willing to share their information. They are able to communicate information using ordinary telephones lines.

Companies and individuals can use this computer network facility to exchange business transactions, text messages, and images, audio and video files.

By using various forms of Information and communications technologies, management can increase organizations flexibility. Use of desktop computers, computer-aided designing software, computer based management system, and computer controlled machine tools provide the precision, speed, and quality in the organizational activities. Immediate information access can eliminates the need for research staff and business libraries. Any level of manager (Top, Middle or Bottom) can easily access information they need to manage large numbers of employees in widely scattered locations. Massive customer database record can be analyzed so that large companies can know their customer's needs.

II. The Internet for Network Based Information System

The Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location.

The WORLD INTERNET USERS STATISTICS given by www.internetworldstats.com, indicates that in last five years, the number of the Internet users increases rapidly, which is also one of the reason behind the popularity of network based information system. The Internet provides backbone for implementing computer networked based information systems for today's businesses. Some of the functionality provided by the Internet are: Communications, Searching, Public / Private Discussion Groups, Public and Private Information Sharing, Entertainment, Business Transactions and File Transfer. Also using the Internet, an Electronic Commerce applications, three major categories [01]: B2B (Business to Business), B2C (Business to Customer) and C2C (Customer to Customer) becomes very much popular.

III. Types of Threats Over Computer Network

Since many of the ICT applications are Internet based, they are very much vulnerable to the unauthorized access of the ICT system. Hence, in case of automated systems, we must recognize the vulnerability of these systems and the importance of taking appropriate security measures from accidental and intentional threats to confidentiality, integrity, and availability. Vulnerabilities are not only found in the technical nature of the infrastructure but also in the users themselves. The greater the number of users of information systems, the greater the number of system failures due to human errors.

A network threats is an intended or unintended illegal activity, an unavoidable or accidental event that could lead to unpredictable, unintended and adverse consequences on an ICT system resources. Following are the widely known and recent network attacks[02]:

- IP spoofing, Password attacks

- Distribution of sensitive internal information to external sources
- Fraud E-mail attacks
- CPU –intensive attacks, DNS poisoning
- Denial-of-service (DoS)
- Spy ware, Trojan Horses, Viruses, Worms
- Exploitation of Code, Internet Infrastructure Attacks, Scan
- Phishing, Malicious Websites, Key Logger

The various attacks on the internet can be divided into two major categories: Active Attack and Passive Attack.

Active attack is one in which unauthorized user not only reads the data / information but also modifies / inserts / deletes data / information available over the networks.

Passive attack is one in which unauthorized user just read the data / information available on network / local machine.

In case of active attack, legal user can easily identify the attack as data / information is updated. But in case of passive attack it is very difficult to track the attack as there is no change in the data / information. There is no perfect mechanism that can provide 100% guarantee about the system security. The only way to improve the security is to go for standardization.

IV. The Standards Implementation Procedure

When any individual / company / government of country want to implement new standard for their networked based system, following figure 1 will help them by illustrating the steps to be followed while implementing new national / international level standard.

Step 1: New Standard implementation procedure starts when any individual, industry, company or country's government realize the need for standardization to improve the network based application system satisfy or improve services efficiency.

Step 2: Define exact requirements and scope of standard implementation in organization / company / any other interested area for which standardization is needed. Here defining scope means, we are finalizing that whether standard is to be needed for the product or for service or for environment or for the safety purpose.

Step 3: Search for any readily available national or compatible international standards, which can satisfy your needs. The compatible international standard means, international standard that can be applied directly or with minor modification, to satisfy your needs.

Step 4: Purchase suitable national or compatible international standard from national or international standards developing organizations and accept it.

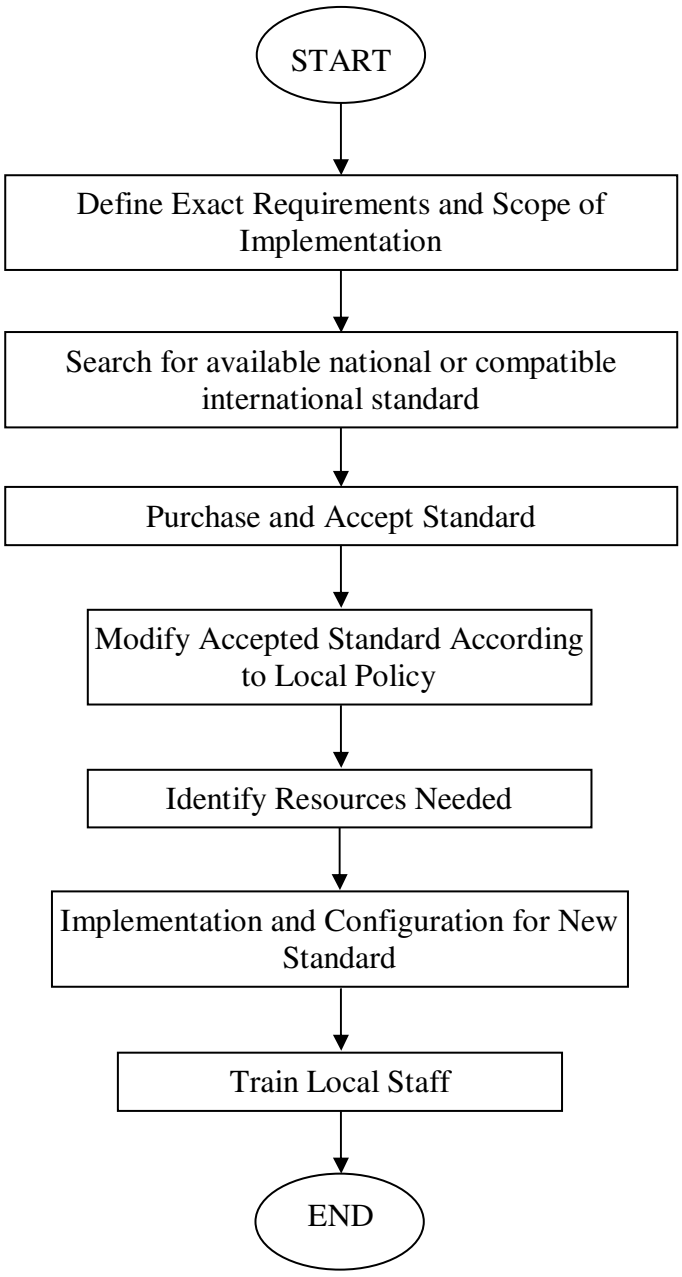

Figure 1. - Implementation Procedure for New Standard

Step 5: Modify accepted national or compatible international standard according to local security policies or any administrative policies defined by the organization.

Step 6: Identify hardware, software, technology and any other resources needed for implementing new standard.

Step 7: Implement and configure new standard.

Step 8: Train local staff to efficiently follow new standard guidelines.

Step 9: Implementation Process End: Eventually revise / retire accepted standard according to company or organization policy.

V. Protection Mechanism for Network Based Information System

Following points are noticeable for the network based information system protection.

- **Data integrity mechanism** – Some mechanism have been created to guarantee the integrity of messages against intentional change. The MAC (Message Authentication Code) methods encode transmitted data with a MAC, which an attacker can not break. Typical scheme use cryptographic hashing mechanisms.
- **Encryption and Confidentiality –** To ensure that the content of a message remains confidential, message must be encrypted. Someone who intercepts a copy of am encrypted message will not be able to extract information. Several techniques exist for encryption. One of most popular category is Single Key (Private Key) Cryptography techniques.
- **Firewall Concept –** Although encryption technology helps lot, but one more technology is equally important, that is Firewall. The technology helps the organization to protect organization's computer and network resources from unwanted Internet traffics / intruders / hackers. A firewall is placed between an organization and rest of the Internet. Firewalls are the most important tool used to handle network connections between two organizations that do not trust each other for all transactions.
- **Intrusion Detection System (IDS) –** This is a type of system that monitors all packets arriving at organization's network, and notifies the site administrator if a security violation is detected. Ready made IDS are available in the market that one can use for protecting network.
- **Secure Socket Layer (SSL) –** SSL is a technique that uses encryption to provide authentication and confidentiality. SSL protocol encrypts the data before sending it on the network transmission line. SSL is used in a transaction over web, to allow users to conduct financial transaction safely.
- **IP Security (IPSec) –** This is a security standard used with IP datagrams. The IPSec also uses cryptographic techniques.

Readymade Recovery Tools

- Many of the incident recovery tools are freely / publicly available security technology that can be downloaded from the Internet. Most of the tools and applications described below can be found in one of the following archive sites[03]:
    - CERT Coordination Center, URL: ftp://info.cert.org:/pub/tools
    - DFN-CERT, URL:ftp://ftp.cert.dfn.de/pub/tools/
    - Computer Operations, Audit, and Security Tools (COAST), URL: coast.cs.purdue.edu:/pub/tools

VI. Conclusion

It is important that standards developing organizations and researchers related to network based information system; develop a good quality of Standards to provide better

security mechanisms for the system. By developing such standards guidelines in cooperation with trained professionals, we can achieve great improvements in performance of the existing network based information system. This research work is one of the steps from my side towards improvement in ICT based system.

VII. References

[01] K. Laudon, J. Laudon, *Management Information System Managing the Digital Firm*, 8th ed., Prentice-Hall India, pp. 118

[02] J. Rittinghouse, W. Hancock, *Cybersecurity Operations Handbook,* Elsevier, 2005

[03] RFC 2196 - Site Security Handbook, page 60