Security Issues in Information System: User's Perspective

Dr. R. D. Kumbhar[#1]
KBPIMSR, Satara
rdk14@rediffmail.com

Mrs. Arati Nimgaonkar[#2]
Fergusson College, Pune
arati.nimgaonkar@fergusson.edu

Abstract-
Information Systems security is one of the biggest challenges in today's digital age. Digitalization of the systems has changed, and will continue to change, our cyber world. Information Systems have become an integral part of everyday life in the home, businesses, government, and organizations. It has changed the way that people live their lives, conduct business, even run the government. Current generation has become very dependent on Information Systems technology. So situations which actually threaten the Information Systems also threaten the everyday activities of the users. To realise these benefits, we need robust Information System security Even if users take all the required care while using the Information system still many security problems arise such as spamming, hacking, jamming, malicious software, sniffing, spoofing, and identity theft. These current problems are threatening the confidentiality, integrity, authenticity of the Information Systems. Due to these attacks on Information Systems, users of Information Systems are in the search for new techniques and new technology that will help to fix the devastating consequences. Along with new techniques and new technology fixing these problems, users of Information Systems must also protect themselves. There are certain ways that users of Information Systems can protect themselves against all of the current security problems. The future of Information Systems is somewhat unknown since it lies in the hands of the users. The main aim of the paper is to identify the vital security issues pertaining to Information Systems and to present some solutions to these issues which arise during using Information System Securely.

Keywords- spamming, hacking, jamming, malicious software, sniffing, spoofing, identity theft, confidentiality, integrity, non-repudiation, DoS

I. Introduction

Cyber security tools and techniques are one of the foundations for trust that information will be protected, such as that trade secrets will be safeguarded or that personal information will be kept confidential. As people conduct more of their daily lives online, opportunities to acquire and misuse financial, medical, sexual, and other forms of personal information are multiplying. Furthermore, the continued development and spread of computer and communications technologies are creating new ways for companies, governments, and criminals to gain access to information that people would rather keep to themselves. And once data have been generated and exist somewhere, disclosure of those data creates the potential for harm. A particular challenge is that even if disclosure of some data is not likely to cause harm, aggregation of those data with other data may be harmful. Researchers have explored potential technical solutions to some aspects of this problem, such as differential privacy, but these work at best in limited circumstances, and the general challenge persists.

Individuals have many preferences about their privacy, and those preferences are not fixed. They are dynamic, informed by context, shaped by relationships with other people and institutions, and constantly under negotiation. Sometimes these preferences coalesce socially into expectations, norms, or conventions that are associated with particular contexts. And also they don't know how to use these security measures. At the same time, governments, communities, social networks, and businesses have legitimate interests in acquiring, analyzing, and using data about individuals. These interests may be commercial, governmental, or social, but they all create a desire or a need for personal information. So basically there is need of establishing secure information system.

II. The Security Perspective

Information Security perspective can be divided in three related categories:

i) ***The Security Expert's Perspective-*** These focus on the technical details of security of the component system such as cryptography, threats and security policies.
ii) ***The software composer's perspective-*** It covers implemented security properties and their impact on the composite system.
iii) ***The end-user's perspective-*** The ultimate security goals which are achieved in association with a particular functionality provided by a collection of components.

III. Information Security Goals

A security goal is the ultimate security objective of a security property [1]. It is achieved as a result of the implemented security properties in the software. For example, a security goal could be defined as the integrity of an object or a piece of data, confidentiality of a message, authentication of an entity or user,

authorization for an operation on certain object or data, or non repudiation of a message etc [4].

Confidentiality – The designed system should provide privacy to the information which travelling through a communication media. It is nothing but provide confidentiality to your data i.e. only the intended recipient other than you can access that data.[2]

Integrity – The system should provide Integrity to your information. Security should restrict other users from altering or modifying the data apart from intended recipient.[2]

Availability – System should avail all the information related assets, resources in terms of hardware or software and made available to authorized users at any time.[2]

Non-repudiation- The designed system should not allow the sender of the information to refuse or to claim the denial for sent information.[2]

IV. Issues Concerning Information Systems Security

The current technological generation has become very much dependent upon Information Systems. The intricate role that Information Systems plays in daily activities has been developed near to perfection by implementing security goals, but still there are many current problems such as spamming, hacking, jamming, malicious software, sniffing, spoofing, and identity theft. These current problems are threatening the reliability and security of Information Systems.

These problems can be broadly divided into two categories. First one is computer crime or computer abuse and secondly vulnerability in the information system software.

Computer crime or computer abuse- Computer crime and computer abuse is widely becoming a widespread problem since technology can help accomplish almost any illegal or unethical task. There is a difference between computer crime and computer abuse, though; computer crime is when a person uses a computer to commit an illegal act, while computer abuse is when a person uses a computer to commit an unethical but not always illegal act. Some of the current computer crime and abuse problems threatening the future of Information Systems are,

Spamming - Spamming can be defined as "the practice of sending unsolicited e-mail and other electronic communication." [4]

Hacking - Hacking is when an illegal user tries to access private information that they are not entitled to access. This illegal access is done either by using Trojan horses, logic bombs, and many other types of software that can very easily be hidden.

DoS – In Denial of Service, intruder flood a network server or Web server with many thousands of false communications or requests in order to jam the communication network. [4] Once the lines are tied up, then legitimate visitors can not access the site, therefore, the lines are "jammed" with illegal users.

Malicious software- When computer viruses are sent through a means, usually the Internet and these computer viruses "infect" the computer, often disabling programs or maybe even causing the computer to "crash," become inoperable.

Sniffing – It can let unauthorized users to access private information about an individual because a piece of software can be used to cross the lines between an Internet user and a web site so the "sniffer" can intercept sensitive data.

Spoofing – Also known as phishing. It involves the making a false web site geared to collect personal information from an Internet user to use it in criminal or unethical acts. Identity theft is the side effect of spoofing.

Vulnerability in the information system software – According to Bruce Schneier – *"People are the weakest link in the security."* The fact is that in the IT world, these security and privacy features make unreasonable demands on users, system administrators and developers. To secure a system's or users' personal information, involves an increasing amount of complexity. Due to this complexity, users avoid interacting with the available security and privacy features on websites and applications which makes system vulnerable.

So while designing the system, developers should take care of the security implications of their design decisions because they are the ones left with the responsibility for making security decisions and designs for these new web applications.

The field that investigates the complexities users experience when interacting with security is usable security. It embraces the fact that most web applications have security features that users should interact with. However, due to their lack of usability, users often avoid and even ignore their security responsibilities (Furnell, Jusoh and Katsabas, 2006). The non-usable design of security has contributed to the fact that the human is regarded as the most common cause behind security configuration errors, which undermine the overall security. It is evident that there is a problem in the interaction between the human element and the technology i.e. design of the interface.

V. Solution

These technological issues that have arisen pose many hindrances to the flow of meaningful information as well as security of information being sent. In spite of these impediments there are solutions to these problems. Some solutions come in the form of counter programming, others as legislation passed by various governing bodies. There is not, however, a single solution that solves or circumvents the issues the plague information systems and their security, each unique problem necessitates an equally unique solution.

To resolve the issue of junk e-mail or spamming, currently many internet service providers offer policies against spamming and/or some sort of application that attempts to curb the amount

of spam in user's mailboxes. Along with this a central security monitoring centre should be set up which would monitor all would focus on multiple communication technologies and would monitor all traffic types such as satellite, wireline, wireless, the Internet, email, VoIP, encrypted communication for de-encryption of net-based encryption methods, regulatory standards to be adopted by telecom operators and system design. Presently, the Indian Government is yet to legislate a law that directly addresses the issue of spam due to which efforts made to fight against spam would be tough.[3]

Hacking has remained a hot topic in the information security world. There are some preventative measures that can be taken by administrators or end users. On such preventative measure, a Firewall is a program used to closely monitor precisely what information passes in and out of a computer or information system. These programs can be set to keep other users out of to prevent information from leaving the computer or information system. Unfortunately, there can be no true solution because as innovative as programmers become hackers will match their innovations and skill. The key to controlling this issue is to stay one step ahead of these hackers and to continually develop new and better forms of protection.

DoS or Jamming is the most difficult attack to detect since it actually simulates web page traffic. You can't prevent being a victim of DoS attack. Firewall or Intrusion Detection Systems (IDS) works as a solution in this case but the better solution is to install Pattern Recognition web application security software. This software effectively protects against malicious behavior such as Denial of Service attacks. The patterns are regular expression-based and designed to efficiently and accurately identify a wide array of application-level attack methods.

Sniffing can take one of two forms: Software which is downloaded either knowingly or unknowingly onto a computer or system, or physical in which a sniffing device is placed on the computer. Detecting sniffing software on a computer's hard drive can be done using software designed to detect sniffing programs or they can be manually sought out by an administrator or user. As software is constantly being upgraded this can be difficult to do, though not impossible. If a physical sniffing device is used they can only be detected by a person physically checking the Ethernet connection of each individual machine.

Spoofing or phishing is the most commonly used technique of attack. You should be alert enough to get rid of such types of attack. Always use secure web sites for communication. Don't reply to any unknown email asking for your private account 6.

information. Use of access control list to deny private IP addresses on your downstream interface can help you from becoming the victim of spoofing. Also by enabling encryption sessions on your router so that trusted hosts that are outside your network can securely communicate with your local hosts.

Vulnerability in the information system software can be reduced by implementing usable security approach while designing a secure system. The usable security is the field that investigates the complexities users experience when interacting with security. So while designing any security system, developer should take into account the factors such as speed, efficiency, learnability and memorability of the implemented security. Security system designed considering these factors may lead to minimise vulnerability in the system.

VI. Conclusion

Internet security is like a game of cat and mouse. Cyber attackers try to find new ways to breach networks and businesses employ better safeguards to stop them. So as a user, by using these safeguards techniques one can protect your network from such attacks. Best practice for incorporating security in an information system is to think and work it very early in development phases. The outcome of every phase should be checked for security concerns. Since the major work for information systems focus on the data management and retrieval, therefore it is recommended to use one of the security techniques, depending upon the usage requirements, so as to make every transaction a secure one.

REFERENCE

1. Alvi, A.K.; Zulkernine, M.; , "A Natural Classification Scheme for Software Security Patterns," Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on , vol., no., pp.113-120, 12-14 Dec. 2011.
2. Atul Kahate, 2003,"Cryptography and Network Security", New Delhi, Tata McGraw Hill Eductaion Private limited, Page 7-10.
3. https://blog.ipleaders.in/overview-laws-spamming-india/
4. Laudon, Jane P., and Laundon, Kenneth C., Management Information Systems. New Jersey: Pearson Education, Inc., 2004.
5. Leitner, M.; , "Security Policies in Adaptive ProcessAware Information Systems: Existing Approaches and Challenges," Availability, Reliability and Security (ARES), 2011 Sixth International Conference on , vol., no., pp.686- 691, 22-26 Aug. 2011.