Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Information Security: Components and Techniques

Aniruddha Singh* MS in (Cyber Law & Information Security) (Indian Institute of Information Technology,Allahabad), India

Abhishek Vaish Associate Professor MS/MBA Department, (Indian Institute of Information Technology,Allahabad), India

Pankaj Kumar Keserwani Assistant Professor (Computer Science & Engg. Department) NIT , Sikkim, India

Abstract: Institutions of all sizes collect and store huge volumes of confidential information. Most of this information is collected, processed and stored on computers and transmitted across networks to other computers. The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. Information security means protecting information and information systems from unauthorized access, use, disruption, or destruction. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks. The paper undertakes the concepts of information security and also review the current technologies related to information security.

Keywords: Information Security, Protecting Information,Physical Security,International Terrorism.

1. INTRODUCTION

Information security means protecting information and information systems from unauthorized access,use,disruption, or destruction. The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing,or transit, and against denial of service to authorized users.information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.Information security is more than just computer security. It also includes a wide range of physical security measures such as protecting your information assets against natural disasters or theft, and social engineering attacks such as someone tricking you into giving out sensitive information.

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure,destruction,modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review. This makes information security an indispensable part of all the business operations across different domains.

2. THE HISTORY OF INFORMATION SECURITY

The need for computer security, or the need to secure the physical location of hardware from outside threats, began almost immediately after the first mainframes were developed. Groups developing code-breaking computations during World War II created the first modern computer. Badges, keys, and facial recognition of authorized personnel controlled access to sensitive military locations.In contrast,information security during these early years was rudimentary and mainly composed of simple document classification schemes. There were no application classification projects for computers or operating systems at this time, because the primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage.

The 1960s : During the 1960s, the Department of Defense's Advanced Research Procurement Agency (ARPA) began examining the feasibility of a redundant networked communications system designed to support the military's need to exchange information. Larry Roberts, known as the Founder of the Internet, developed the project from its inception.

The 1970s and 80s : During the next decade, the ARPANET grew in popularity and use, and so did its potential for misuse. In December of 1973, Robert M. Metcalfe, indicated that there were fundamental problems with ARPANET security. Individual remote users' sites did not have sufficient controls and safeguards to protect data against unauthorized remote users. There were no safety procedures for dial-up connections to the ARPANET. User identification and authorization to the system were nonexistent. Phone numbers were widely distributed and openly publicized on the walls of rest rooms and phone booths, giving hackers easy access to ARPANET. Much of the focus for research on computer security centered on a system called MULTICS (Multiplexed Information and Computing Service). In mid-1969, not long after the restructuring of the MULTICS project, several of the key players created a new operating system called UNIX.While the MULTICS system had planned security with multiple security levels, and passwords, the UNIX system did not. In the late 1970s the microprocessor brought in a new age of computing capabilities and security threats as these microprocessors were networked.

3. THE PAPER THAT STARTED THE STUDY OF COMPUTER SECURITY

It began with Rand Report R-609, which attempted to define multiple controls and mechanisms necessary for the protection of a multi-level computer system. The scope of computer security grew from physical security to include Safety of the data itself, limiting of random and unauthorized access to that data, involvement of personnel from multiple levels of the organization. At this stage, the concept of computer security evolved into the more sophisticated system we call information security.

The 1990s : At the close to the 20th century, as networks of computers became more common. This gave rise to the Internet, the first manifestation of a global network of networks. There has been a price for the phenomenal growth of the Internet. As the requirement for networked computers became the dominant style of computing, the ability to physically secure that physical computer was lost, and the stored information became more exposed to security threats.

The Present : Today, the Internet has brought millions of unsecured computer networks into communication with each other. Our ability to secure each computer's stored information is now influenced by the security on each computer to which it is connected. The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit.

Governments, military, corporations, financial institutions, hospitals, and private Businesses collect and store huge volumes of confidential information. The information may be about employees, customers, research, products or financial operations. Most of this information is collected, processed and stored on computers and transmitted across networks to other computers. If this information fell into the wrong hands, it could lead to lost business, law suits, identity theft or even bankruptcy of the business. With cybercrime on the rise, protecting your corporate information and assets is vital. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

What Is Security? In general, security is "the quality or state of being secure that is to be free from danger." It means to be protected from adversaries from those who would do harm, intentionally or otherwise. A successful organization should have the following multiple layers of security in place for the protection of its operations.

a) *Physical Security :* To protect the physical items, objects, or areas of an organization from unauthorized , access and misuse.
b) *Personal Security :* To protect the individual or group of individuals who are authorized to access the organization and its operations.
c) *Operations Security :* To protect the details of a particular operation or series of activities.
d) *Communications Security :* To protect an organization's communications media, technology, and content.
e) *Network Security :* To protect networking components,connections, and contents.
f) Information Security *:* To protect of information and its critical elements, including the systems and hardware.

4. COMPONENTS OF AN INFORMATION SYSTEM

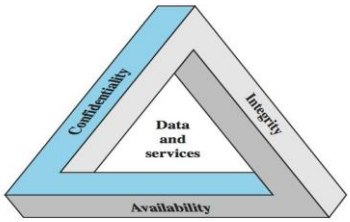
To fully understand the importance of information security, it is necessary to briefly review the elements of an information system. An Information System is much more than computer hardware. It is the entire set of software, hardware, data, people, and procedures necessary to use information as a resource within and outside the organization. To protect the information and its related systems from danger, tools, such as policy, awareness, training, education, and technology are necessary.

Securing the Components : When considering the security of information systems components, it is important to understand the concept of the computer as the subject of an attack as opposed to the computer as the object of an attack. When a computer is the subject of an attack, it is used as an active tool to conduct the attack. When a computer is the object of an attack, it is the entity being attacked.

Security and Access Balancing : When considering information security, it is important to realize that it is impossible to obtain perfect security. Security is not an absolute; it is a process not a goal. Security should be considered a balance between protection and availability. To achieve balance the level of security must allow reasonable access, yet protect against threats. Where information is exempted from disclosure, it implies that security measures will apply in full. Information security in today's enterprise is a "wellinformed sense of assurance that the information risks and controls are in balance."

5. COMPONENTS OF INFORMATION SECURITY

The C.I.A. triangle has been considered the industry standard for security since the development of the mainframe. It was solely based on three characteristics that described the utility of information: confidentiality, integrity, and availability. The interpretations of these three aspects vary, as do the contexts in which they arise.



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.

Confidentiality : Confidentiality is the concealment of information or resources. Confidentiality means making sure that information is only seen by people who have the right to see it. Keeping information secret from unauthorized access is probably the most common aspect of information security. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity : Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity i.e. the content of the information and origin integrity i.e. the source of the data. Integrity means ensuring that information remains intact and unaltered. This means watching out for alterations through malicious action, natural disaster, or even a simple innocent mistake. Integrity includes both the correctness and the trustworthiness of the data.

Availability : Availability refers to the ability to use the information or resource desired. Availability means having access to your information when you need it. In other words, it means making sure no person or event is able to block legitimate or timely access to information. The information created and stored by an organization needs to be available to authorized users and applications. Information is useless if it is not available. In some cases information needs to be changed constantly, which means that it must be accessible to those authorized to access it. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable.

Two additional objectives:

a) ***Authenticity :*** Authenticity means being genuine and able to be verified or trust. In computing, e Business, and information security, it is necessary to ensure that the data, transactions, communications or documents are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be.

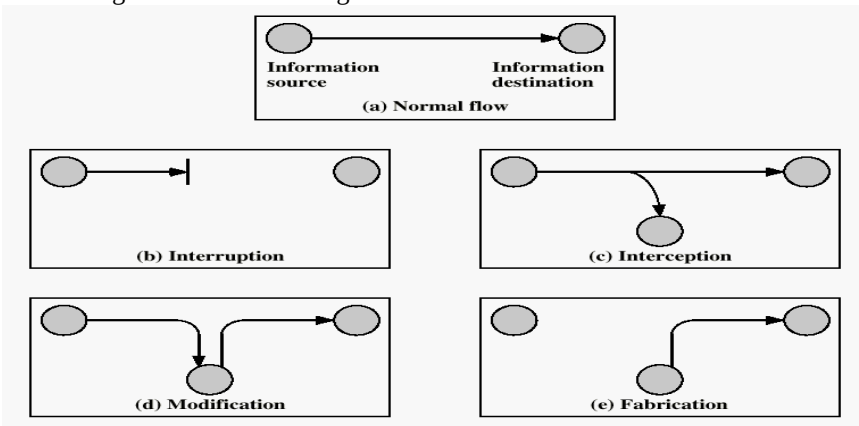
b) ***Accountability :*** Accountability involves actions of an entity can be traced uniquely to that entity, supports nonrepudiation, deterrence, fault isolation, intrusion, detection and prevention. Non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

6. SOME COMMON SECURITY ATTACKS

Attacks Threatening Confidentiality : In general, two types of attack threaten the confidentiality of information: snooping and traffic analysis. Snooping refers to unauthorized access to or interception of data. Traffic analysis refers other types of information collected by an intruder by monitoring online traffic.

Attacks Threatening Integrity : The integrity of data can be threatened by several kinds of attack: modification, masquerading, replaying and repudiation.

Attacks Threatening Availability : Denial of service (DOS) attacks may slow down or totally interrupt the service of a system. The attacker can use several strategies to achieve this. They might make the system so busy that it collapses, or they might intercept messages sent in one direction and make the sending system believe that one of the parties involved in the communication or message has lost the message and that it should be resent.



Interruption: This is an attack on availability

- Disrupting traffic
- Physically breaking communication line

Interception: This is an attack on confidentiality

- Overhearing, eavesdropping over a communication line

Modification: This is an attack on integrity

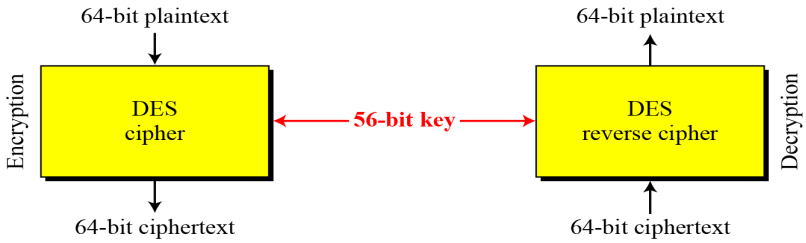
- Corrupting transmitted data or tampering with it before it reaches its destination

Fabrication: This is an attack on authenticity

- Faking data as if it were created by a legitimate and authentic party

7. TECHNIQUES OF INFORMATION SECURITY

Cryptography : Cryptography, a word with Greek origins, means "secret writing". Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit and while information is in storage 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. The original message is referred to as plaintext and the message that is sent through the channel is referred to as the cipher text. Information that has been encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption.



Traditional Ciphers : Traditional ciphers used two techniques for hiding information from an intruder: *substitution* and *transposition*.

Substitution Ciphers : A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another.

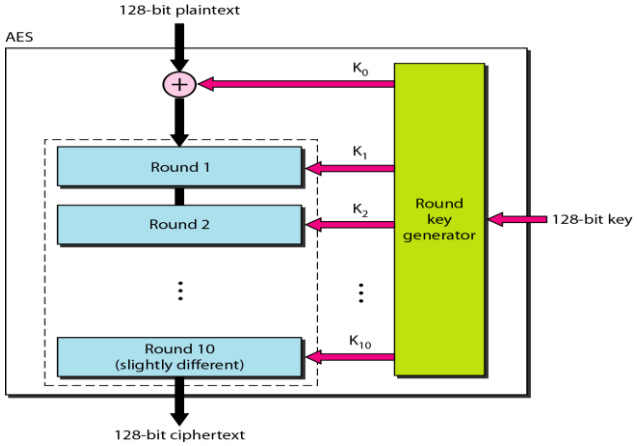
Transposition Ciphers : A transposition cipher does not substitute one symbol for another; instead it changes the location of the symbols. A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext, while a symbol in the eighth position in the plaintext may appear in the first position of the ciphertext. In other words, a transposition cipher reorders (transposes) the symbols.

Modern symmetric-key ciphers:-Since traditional ciphers are no longer secure, modern symmetric-key ciphers have been developed. Modern ciphers normally use a combination of substitution, transposition and some other complex transformations to create a cipher text from a plaintext. Modern ciphers are bit-oriented (instead of character-oriented). The plaintext, cipher text and the key are strings of bits.

Two modern symmetric-key ciphers are DES and AES:

DES (Data Encryption Standard) : The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977.it uses 56-bit symmetric key, 64-bit plaintext input. DES has been the most widely used symmetric-key block cipher since its publication.

AES : (Advanced Encryption Standard) : The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the US National Institute of Standards and Technology (NIST) in 2001 in response to the shortcoming of DES. It processes data in 128 bit blocks and128, 192, or 256 bit keys.



Asymmetric-Key Cryptography : Asymmetric-key cryptography is used for confidentiality. Unlike symmetrickey cryptography, there are distinctive keys in asymmetrickey cryptography, a private key and a public key. If encryption and decryption are thought of as locking and unlocking padlocks with keys, then the padlock that is locked with a public key can be unlocked only with the corresponding private key. Both symmetric-key and asymmetric-key cryptography will continue to exist in parallel. The conceptual differences between the two systems are based on how these systems keep a secret. In symmetric-key cryptography, the secret token must be shared between two parties. In asymmetrickey cryptography, the token is unshared each party creates its own token. It is believed that both are complements ofeach other. The advantages of one can compensate for the disadvantages of the other.

Message Integrity : Hash Function : There are occasions on which we may not even need secrecy, but instead must have integrity. One way to preserve the integrity of a document was traditionally through the use of a fingerprint. The electronic equivalents of the document and fingerprint pair are the message and digest pair. To preserve the integrity of a message, the message is passed through an algorithm called a cryptographic hash function. The function creates a compressed image of the message that can be used like a fingerprint. To check the integrity of a message or document, we run the cryptographic hash function again and compare the new message digest with the previous one. If both are the same, we are sure that the original message has not been changed.

Digital Signatures : We are familiar with the concept of a signature. Digital signature is a Cryptographic technique analogous to hand-written signatures. A person signs a document to show that it originated from him/her or was approved by him/her. The signature is proof to the recipient that the document comes from the correct entity. In other words, a signature on a document, when verified, is a sign of authentication—the document is authentic. An electronic signature can prove the authenticity of the sender of the message. We refer to this type of signature as a digital signature.
In Digital signature process the sender uses a signing algorithm to sign the message. The message and the signature are sent to the recipient. The recipient receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted, otherwise it is rejected.
A digital signature needs a public-key system. The signer signs with her private key, the verifier verifies with the signer's public key. A cryptosystem uses the private and public keys of the recipient; a digital signature uses the private and public keys of the sender.

8. WEB SECURITY

Basic Authentication : Basic Authentication is a simple user ID and password-based authentication scheme, and provides to identify which user is accessing the server and to limit users to accessing specific pages.
Secure Socket Layer (SSL) : Netscape Inc. originally created the SSL protocol, but now it is implemented in World Wide Web browsers and servers from many vendors. SSL provides the Confidentiality through an encrypted connection based on symmetric keys and authentication using public key identification and verification, connection reliability through integrity checking.
There are two parts to SSL standard, the SSL Handshake which is a protocol for initial authentication and transfer of encryption keys and the SSL Record protocol is a protocol for transferring encrypted data.
The client sends a message to the Web server, and the server responds with a copy of its digital certificate. The client decrypts the server's public key using the well-known public key of the Certificate Authority. The client generates two random numbers that will be used for symmetric key encryption, one number for the receiving channel and one for the sending channel. These keys are encrypted using the server's public key and then transmitted to the server. The client issues a challenge (some text encrypted with the send key) to the server using the send symmetric key and waits for a response from the server that is using the receiver's symmetric key. Server authenticates client and data is exchanged across the secure channel.
Distributed Authentication: KERBEROS : Kerberos is a network authentication protocol which Provides
authentication for client-server applications, and data integrity and confidentiality. It relies entirely on symmetric cryptography . In this when Client wants service from a particular server an Authentication Server allows access based on tickets. Ticket specifies that a particular client (authenticated by the Authentication Server) has the right to obtain service from a specified server. In this the network is under the control of an Authentication Server.
This uses two types of tickets with two different lifetimes. One ticket grants to right to ask for service which performed once per login session Ticket. For each type of service, use a ticket that grants the right to use that particular service Ticket. Every time that service is needed, the ticket is used.
Protecting IP: IPSEC : IPSEC is an Internet standard for ensuring secure private communication over IP networks, and it was developed by IPSEC working group of IETF. It implements network layer security by facilitating direct IP connectivity between sensitive hosts through untrusted networks.
In this a relationship between a sender and a receiver is identified by three parameters
(I) Security Parameter Index (SPI)
(II) IP Destination address (IP of the destination SA, can be a host, a firewall or a router)
(III) Security Protocol Identifier (ESP or AH) SPI + IP destination address uniquely identifies a particular Security Association.
Authentication Header (AH) provides integrity and authentication without confidentiality. In Transport Mode AH authenticates the IP payload and selected portions of the IP header while in Tunnel Mode AH authenticates the entire inner IP packet and selected portions of the outer IP header.
Encapsulating Security Payload (ESP) provides confidentiality and can also provide integrity and authentication. In Transport Mode ESP encrypts and optionally authenticates the IP payload (data), but not the IP header while in Tunnel Mode ESP encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.
Access Control : Firewalls : Firewall isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others. A firewall is used to control traffic flow between networks.
Firewall uses the following techniques:
Packet Filters : It is the commonly used firewall technique which Operates at IP level, Checks each IP packet against the filter rules before passing (or not passing) it on to its destination.

In this internal network connected to Internet via router firewall that filters packet-by-packet, decision to forward/drop packet based on source IP address, destination IP address, TCP/UDP source and destination port numbers, ICMP message type, TCP SYN and ACK bits. It is Very fast than other firewall techniques but Hard to configure.

Application Gateways : Application gateways Filters packets on application data as well as on IP/TCP/UDP fields and allow select internal users to telnet outside. In this all telnet users require to telnet through gateway, for authorized users, gateway sets up telnet connection to destination host and Gateway relays data between 2 connections. Router filter blocks all telnet connections not originating from gateway.

9. CONCLUSION

With cybercrime on the rise the protection of data (information security) is the most important. The protection of networks is important to prevent loss of server resourcesas well as to protect the network from being used for illegal purposes. Information security is an ongoing and never ending process. Each information security technique has its unique features and applicability. To ensure information security the best that can be done is to implement a wide variety of solutions and more closely monitor who has access to what network resources and information.

REFERENCES

[1] Sattarova Feruza Y. and Prof.Tao-hoon Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security", International Journal of Multimedia and Ubiquitous Engineering, Vol. 2, No. 2, April, 2007

[2] Manas Paul and Jyotsna Kumar Mandal, "A Universal Session Based Bit Level Symmetric Key Cryptographic Technique to Enhance the Information Security", (IJNSA), Vol.4, No.4, July 2012

[3] Overview of Network Security: Mohamed Sharif

[4] Network Security: J.F Kurose and K.W. Ross

[5] Networks Fall 2002: Justin Weisz

[6] Information Security: Cristina Nita-Rotaru

[7] Information Security: Principles and Practice, Mark Stamp Second Edition

[8] http://www.vsrdjournals.com/CSIT/Issue/2013_04_April/Web/4_Kapil_Kumar_Sharma_1612_Review_Article_VSRDIJCSIT_April_2013..pdf

[9] Information Security: Cristina Nita-Rotaru

[10] Information Security: Principles and Practice, Mark Stamp Second Edition

