Information security

Introduction

The requirements of information security with in an organization have undergone major changes in the past and present times. In the earlier times physical means is used to provide security to data. With the advent of computers in every field, the need for software tools for protecting files and other information stored on the computer became important. The important tool designed to protect data and thwart illegal users is computer security.

With the introduction and revolution in communications, one more change that affected security is the introduction of distributed systems which requires carrying of data between terminal user and among a set of computers. Network security measures are needed to protect data during their transmission. The mechanisms used to meet the requirements like authentication and confidentiality are observed to be quite complex. One must always consider potential counter measures while developing a particular mechanism. It is also important to identify implementations to adopt these mechanisms. Security mechanisms usually involve more than a particular algorithm or protocol. It means that participants be in possession of some secret information, which raises doubts about their creation, distribution and protection of that secret information. Thus a model has to be developed within which security services and mechanisms can be viewed.

To identify the security needs of an organization at its effective level, the manager needs a systematic way. One approach is to consider three aspects of information security that is Security attack, Security mechanism and Security services. Security attack identifies different modes by which intruder tries to get unauthorized information and the services are intended

to counter security attacks, and they make use of one or more security mechanisms to provide the service.

As information systems become ever more active and important to the conduct of activities, electronic information takes on many of the roles earlier being done on papers. Few information integrity functions that the security mechanism has to support are security and confidentiality of the data to be transmitted and authentication of users.

There is no single mechanism that will provide all the services specified. But we can see that one particular element that specifies most of the security mechanisms in use: cryptographic techniques. Encryption or encryption like transformations of information is the most common means of providing security. A model for much of what we will be discussing is captured in general terms.

Encryption Model

This general model shows that there are four basic tasks in designing a particular security service.

1. Design an algorithm for performing encryption & decryption process.
2. Generate the secret information with the help of algorithm of step 1.
3. Identify methods for the distribution and sharing of secret information.
4. Identify rules to be used by both the participating parties that makes use of security algorithm and the secret information to achieve a particular security service.

A crypto system is an algorithm, plus all possible plain texts, cipher texts and keys. There are two general types of key based algorithms: symmetric and

public key. With most symmetric algorithms, the same key is used for both encryption and decryption.

Symmetric-key encryption

Execution of symmetric-key encryption can be highly useful, so that users do not experience any significant time delay because of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages specify a meaningful sense.

Symmetric-key encryption will be successful only if the symmetric key is kept secured by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. The success of a symmetric algorithm rests in the key, divulging the key means that any one could encrypt and decrypt messages. As long as the communication needs to remain secure, the key must be protected between the participating parties.

Encryption and decryption with a symmetric algorithm are denoted by

$E_K(M) = C$

$D_K(M) = P$

Symmetric algorithms can be divided into two categories. Some operate on the plain text a single bit or byte at a time, these are called stream

algorithms or stream ciphers. Others operate on group of bits or characters. Such algorithms are called block algorithms.

Public algorithms are designed so that the key used for encryption is different from the key used for decryption. The algorithms are called public key because the encryption key be made public. It involves a pair of keys–a *public key* and a *private key* –associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Further more the decryption key cannot be calculated from the encryption key. Each public key is published, and the corresponding private key is kept secret. Data encrypted with ones public key can be decrypted only with his private key. shows a simplified view of the way public-key encryption works.

Public-key encryption

Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, it’s possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol. This provides Authentication, Integrity & Confidentiality of Information at low computing power. Nevertheless, private-key encryption is useful, because it means you can use your private key to sign data with your digital signature–an important requirement for electronic commerce and other commercial applications of cryptography. Encryption and decryption can be represented in a public key scheme is

$E_{Kpu}(M) = C$

$D_{Kpr}(C) = M$

Where Kpu is the public key and Kpr is the private key.

In public key encryption there is always a possibility of some information being leaked out. A crypto analyst tries to get some information based on ones public key. Not a whole of information is to be gained here, but there are potential problems with allowing a crypto analyst to encrypt random messages with public key. Some information is leaked out every time to the crypto analyst, he encrypts a message. In probabilistic Encryption, multiple cipher texts are generated for one plain text, a cryptanalyst can not generate any information by chosen plain text and chosen cipher text attacks.

Probabilistic encryption

Security Analysis of algorithms: Different algorithms offers different degrees of security, it depends on how hard they are to break. If the cost required to break an algorithm is greater than the value of the encrypted data, then we are probably safe. If the time required to break an algorithm is longer than the time that the encrypted data must remain secret, then we are probably safe. If the amount of data encrypted with a single key is less than the amount of data necessary to break the algorithm, then we are probably safe.

An algorithm is unconditionally secure if, no matter how much cipher text a crypto analyst has, there is not enough information to recover the plain text. In point of fact, only a one time pad is unbreakable in a cipher text only attack, simply by trying every possible key one by one and by checking whether the resulting plain text is meaningful. This is called a brute force

attack. Cryptography is more concerned with crypto systems that are computationally infeasible to break. Any algorithm is considered computationally secure if it cannot be broken with available resources.

The complexity of an attack can be measured as Data Complexity, the amount of data needed as input to the attack, Processing complexity, the time needed to perform the attack and storage requirements which are the amount of memory needed to do the attack which is space complexity.

As a thumb rule, the complexity of an attack is taken to be minimum of these three factors. Another classification of complexities is by complexity of the algorithm by its construction and complexity of the algorithm by its strength. By its construction, the time complexity of the algorithm can be calculated by executing through the steps of the algorithm, which will be referred as O(n). Complexities can also be expressed as orders of magnitude. If the length of the key is k, then the processing complexity is given by 2k . It means that 2 k operations are required to break the algorithm. Then the complexity of the algorithm is said to be exponential in nature.

A desirable property of any encryption algorithm is that a small change in plain text or the key should produce significant change in cipher text. Such an effect is known as avalanche effect. The more the avalanche affects of the algorithm, the better the security. Crypto analysis is the study of recovering the plain text with out access to the key. It may also find weakness in a crypto system that eventually leads to previous results.

An attempted crypto analysis is called an attack. There are five types of attack. Each of them assumes that the crypto analyst has complete knowledge of the encryption algorithm used.

1. Cipher text only attack: Here the crypto is in hold of cipher text only. The crypto analyst has cipher text of several messages, all of which have been encrypted using the same encryption algorithm. The crypto analyst’s job is to recover the plain text of as many messages as possible, or better yet to deduce the key used to encrypt the messages, in order to decrypt other messages encrypted with the same keys.
2. Known Plaintext attack: The crypto analyst is in hold of not only to the cipher text of several messages, but also to the plain text of those messages. His job is to get the key used to encrypt the messages or an algorithm to decrypt any messages encrypted with the same key.
3. Chosen Plaintext Attack (CPA): Here the crypto analyst is in hold of not only cipher text but also parts of chosen plain text. If the analyst is able to insert into the system a message chosen by the analyst, then such an attack is known as chosen plain text attack. Differential crypto analysis is an example of this mode.
4. Chosen cipher text attack (CCA): Under the CCA model, an adversary has access to an encryption and a decryption machine and must perform the same task of distinguishing encryptions of two messages of its choice. First, the adversary is allowed to interact with the encryption and decryption services and choose the pair of messages.

After it has chosen the messages, however, it only has access to an encryption machine.

5. Chosen text: In this model, the analyst posses the encryption algorithm, Cipher text to be decoded, plain text message chosen by the crypto analyst and purported cipher text chosen by the crypto analyst.

Present work:

In this work an attempt has been made to generate a set of algorithms which provides security to data transmitted. The first algorithm considers a random matrix key which on execution by a series of steps generates a sequence. This sequence is used a sub key to build three different encryption models. Each model can be used for encryption of data. The second algorithm considers not only the key but also initialization vector and a time stamp to generate sub keys which are used for encryption process. And also a mechanism has been discussed which identifies any garbled key while transmitted from the Key Distribution Centre.

In this work both the algorithms are discussed in terms of computational security, computational complexity and computational overhead. Both the algorithms are studied for their strengths and limitations. A crypto analytical study of the algorithms with emphasis on probabilistic encryption is also considered in this study.

The encryption algorithms are compared with standard algorithms like RC4 and DES. The algorithms are also discussed in terms of its applications and also about their advantages and limitations in network security environment.